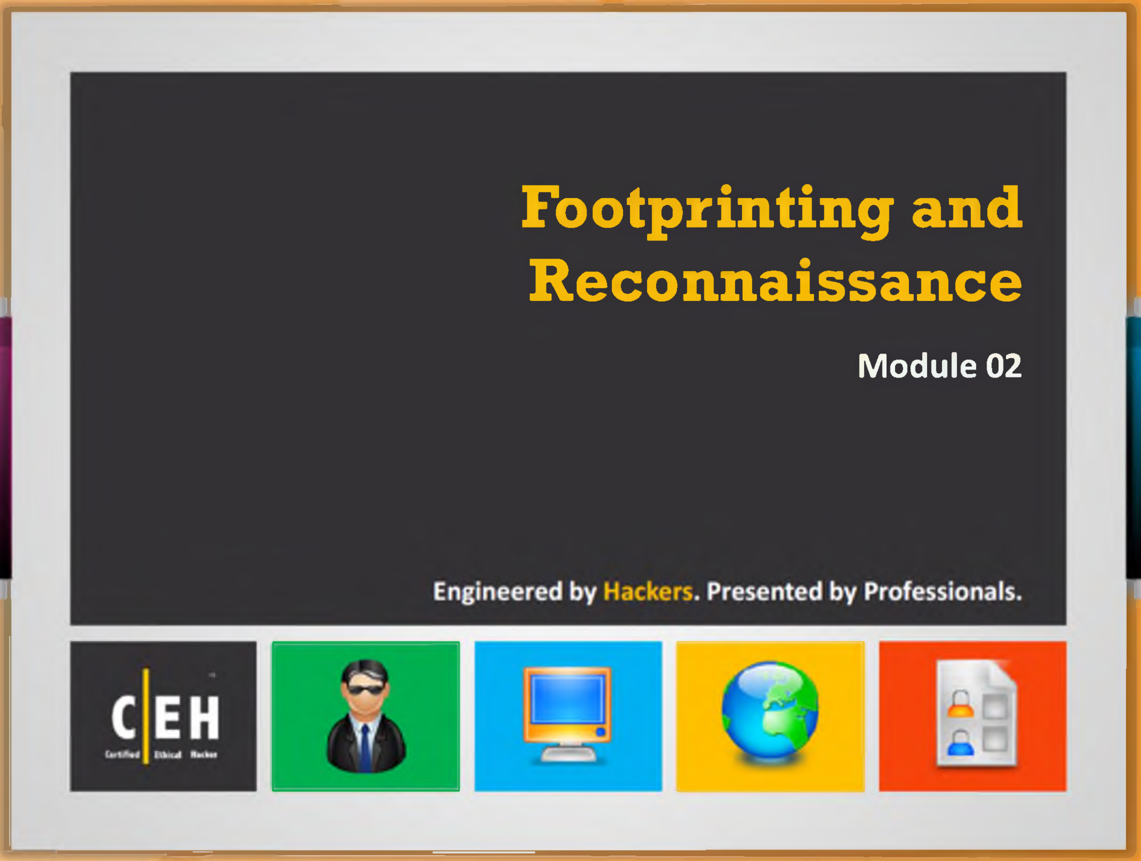
Footprinting and Reconnaissance

Module 02



Footprinting and Reconnaissance

Module 02

Engineered by Hackers. Presented by Professionals.

Ethical Hacking and Countermeasures v8

Module 02: Footprinting and Reconnaissance

Exam 312-50

Security News

Facebook a 'treasure trove' of Personally Identifiable Information

April 10, 2012

Facebook contains a "treasure trove" of personally identifiable information that hackers manage to get their hands on.

A report by Imperva revealed that users' "general personal information" can often include a date of birth, home address and sometimes mother's maiden name, allowing hackers to access this and other websites and applications and create targeted spearphishing campaigns.

It detailed a concept I call "friend-mapping", where an attacker can get further knowledge of a user's circle of friends; having accessed their account and posing as a trusted friend, they can cause mayhem. This can include requesting the transfer of funds and extortion.

Asked why Facebook is so important to hackers, Imperva senior security strategist Noa Bar-Yosef said: “People also add work friends on Facebook so a team leader can be identified and this can lead to corporate data being accessed, project work being discussed openly, while geo-location data can be detailed for military intelligence."

“Hacktivism made up 58 per cent of attacks in the Verizon Data Breach Intelligence Report, and they are going after information on Facebook that can be used to humiliate a person. All types of attackers have their own techniques.”

http://www.scmagazineuk.com

Security News

Facebook a 'treasure trove' of Personally Identifiable Information

Source: http://www.scmagazineuk.com

Facebook contains a "treasure trove" of personally identifiable information that hackers manage to get their hands on.

A report by Imperva revealed that users' "general personal information" can often include a date of birth, home address and sometimes mother's maiden name, allowing hackers to access this and other websites and applications and create targeted spearphishing campaigns.

It detailed a concept I call "friend-mapping", where an attacker can get further knowledge of a user's circle of friends; having accessed their account and posing as a trusted friend, they can cause mayhem. This can include requesting the transfer of funds and extortion.

Asked why Facebook is so important to hackers, Imperva senior security strategist Noa Bar-Yosef said: “People also add work friends on Facebook so a team leader can be identified and this can lead to corporate data being accessed, project work being discussed openly, while geo-location data can be detailed for military intelligence."

"Hacktivism made up 58 per cent of attacks in the **Verizon Data Breach Intelligence Report**, and they are going after information on Facebook that can be used to humiliate a person. All types of attackers have their own techniques."

On how attackers get a password in the first place, Imperva claimed that different **keyloggers** are used, while phishing kits that create a **fake Facebook login page** have been seen, and a more primitive method is a brute force attack, where the attacker repeatedly attempts to guess the user's password.

In more extreme cases, a **Facebook administrator's** rights can be accessed. Although it said that this requires more effort on the hacker side and is not as prevalent, it is the "**holy grail**" of attacks as it provides the hacker with data on all users.

On protection, Bar-Yosef said the roll-out of SSL across the whole website, rather than just at the login page, was effective, but users still needed to opt into this.

By Dan Raywood

http://www.scmagazine.com.au/Feature/265065,digitial-investigations-have-matured.aspx

Module Objectives

C|EH Certified Ethical Hacker

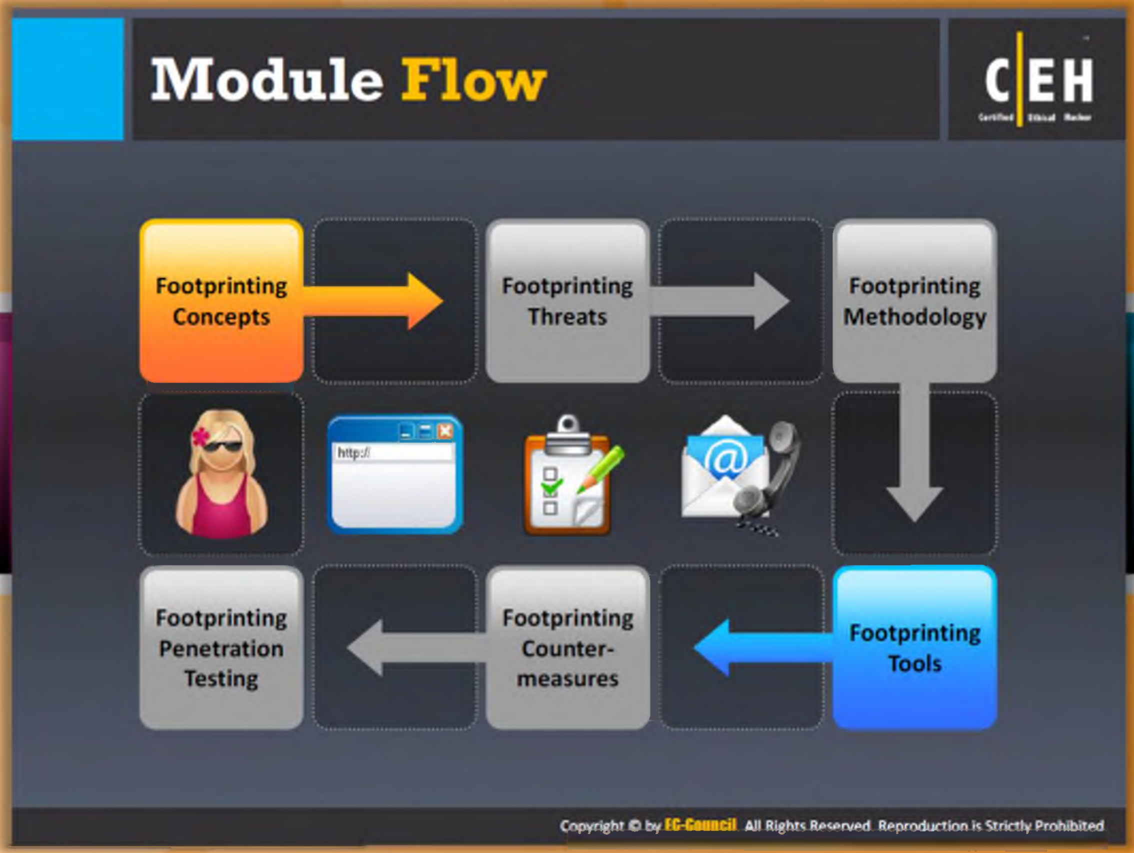
- Footprinting Terminology
- What Is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting Using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing

Module Objectives

This module will make you familiarize with the following:

- Footprinting Terminologies
- What Is Footprinting?
- Objectives of Footprinting
- Footprinting Threats
- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting Using Google
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites
- Footprinting Tools
- Footprinting Countermeasures
- Footprinting Pen Testing

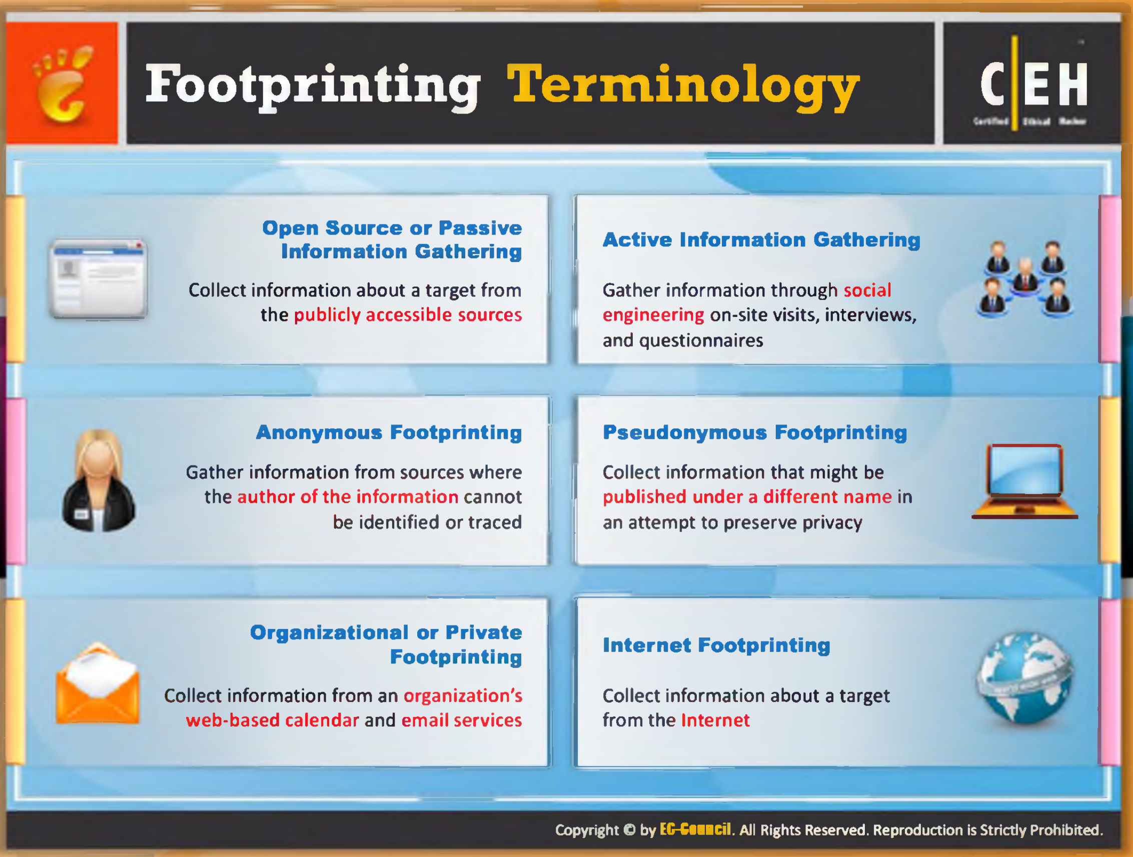

Module Flow
CEH
Certified Ethical Hacker
Footprinting Concepts
Footprinting Threats
Footprinting Methodology
http://
Footprinting Penetration Testing
Footprinting Counter-measures
Footprinting Tools
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited

Module Flow

Ethical hacking is legal hacking conducted by a penetration tester in order to evaluate the security of an IT infrastructure with the permission of an organization. The concept of ethical hacking cannot be explained or cannot be performed in a single step; therefore, it has been divided into several steps. Footprinting is the first step in ethical hacking, where an attacker tries to gather information about a target. To help you better understand footprinting, it has been distributed into various sections:

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

The **Footprinting Concepts** section familiarizes you with footprinting, footprinting terminology, why footprinting is necessary, and the objectives of footprinting.



Footprinting Terminology

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

Footprinting Terminology

Before going deep into the concept, it is important to know the basic terminology used in footprinting. These terms help you understand the concept of footprinting and its structures.

Open Source or Passive Information Gathering

Open source or passive information gathering is the easiest way to collect information about the target organization. It refers to the process of gathering information from the open sources, i.e., publicly available sources. This requires no direct contact with the target organization. Open sources may include newspapers, television, social networking sites, blogs, etc.

Using these, you can gather information such as network boundaries, IP address reachable via the Internet, operating systems, web server software used by the target network, TCP and UDP services in each system, access control mechanisms, system architecture, intrusion detection systems, and so on.

Active Information Gathering

In active information gathering, process attackers mainly focus on the employees of the target organization. Attackers try to extract information from the employees by conducting **social engineering**: on-site visits, interviews, questionnaires, etc.

Anonymous Footprinting

This refers to the process of collecting information from sources anonymously so that your efforts cannot be traced back to you.

Pseudonymous Footprinting

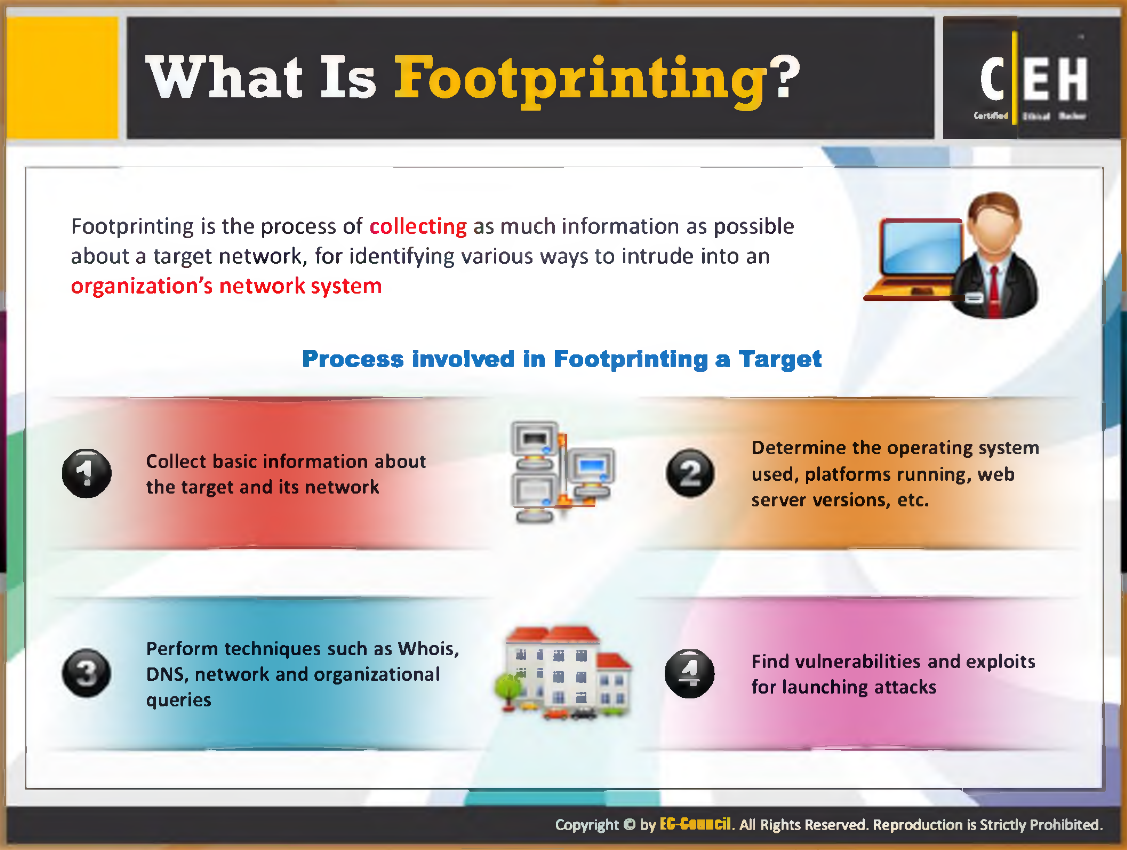
Pseudonymous footprinting refers to the process of collecting information from the sources that have been published on the Internet but is not directly linked to the **author's name**. The information may be published under a different name or the author may have a well-established pen name, or the author may be a corporate or government official and be prohibited from posting under his or her original name**.** Irrespective of the reason for hiding the author's name, collecting information from such sources is called **pseudonymous**.

Organizational or Private Footprinting

Private footprint````ing involves collecting information from an organization´s **web-based calendar** and email services.

Internet Footprinting

Internet footprinting refers to the process of collecting information of the target organization's connections to the Internet.



What Is Footprinting?

Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system

Process involved in Footprinting a Target

1. Collect basic information about the target and its network
2. Determine the operating system used, platforms running, web server versions, etc.
3. Perform techniques such as Whois, DNS, network and organizational queries
4. Find vulnerabilities and exploits for launching attacks

What Is Footprinting?

Footprinting, the first step in ethical hacking, refers to the process of collecting information about a target network and its environment. Using footprinting you can find various ways to intrude into the target organization's network system. It is considered "methodological" because critical information is sought based on a previous discovery.

Once you begin the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here the term "blueprint" is used because the result that you get at the end of footprinting refers to the unique system profile of the target organization.

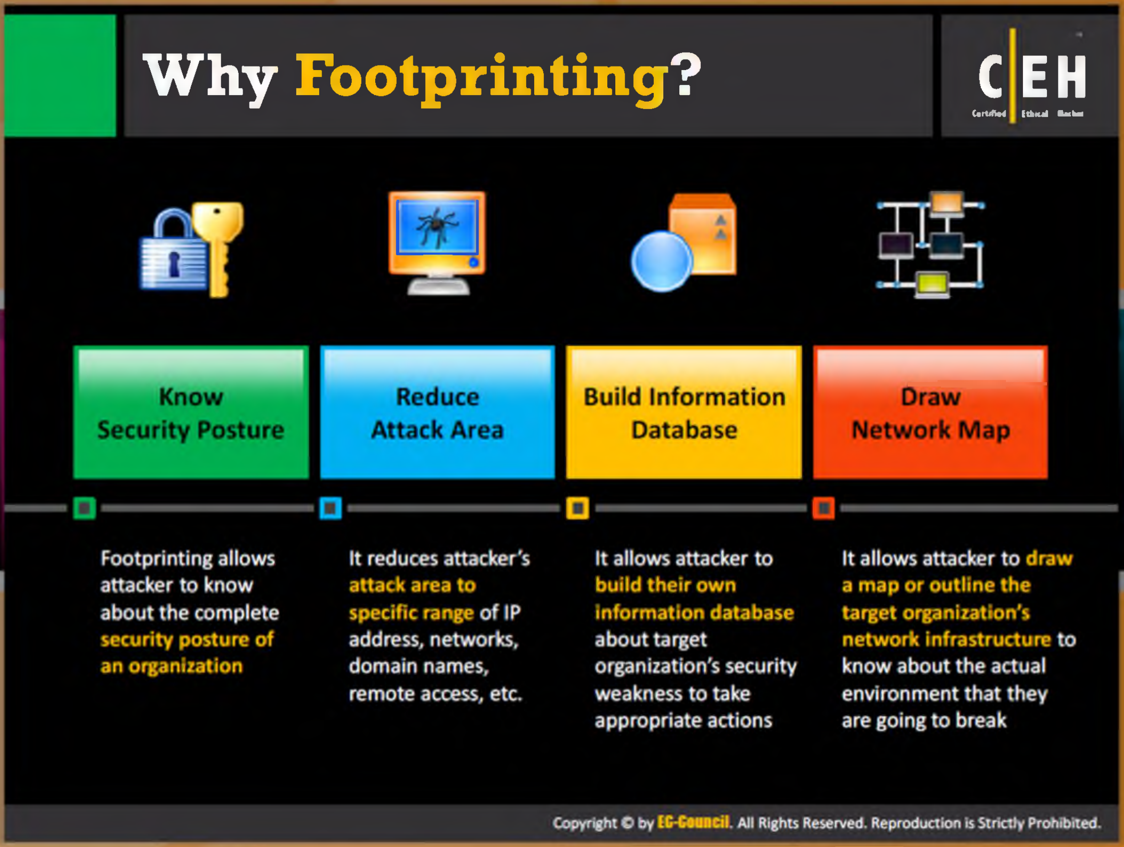
There is no single methodology for footprinting as you can trace information in several routes. However, this activity is important as all crucial information needs to be gathered before you begin hacking. Hence, you should carry out the footprinting precisely and in an organized manner.

You can collect information about the target organization through the means of footprinting in four steps:

1. Collect basic information about the target and its network
2. Determine the operating system used, platforms running, web server versions, etc.

3. Perform techniques such as Whois, DNS, network and organizational queries
4. Find vulnerabilities and exploits for launching attacks

Furthermore, we will discuss how to collect basic information, determine operating system of target computer, platforms running, and web server versions, various methods of footprinting, and how to find and **exploit vulnerabilities** in detail.



Why Footprinting?

Know Security Posture

Footprinting allows attacker to know about the complete security posture of an organization

Reduce Attack Area

It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.

Build Information Database

It allows attacker to build their own information database about target organization's security weakness to take appropriate actions

Draw Network Map

It allows attacker to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to break

Why Footprinting?

For attackers to build a hacking strategy, they need to gather information about the target organization's network, so that they can find the easiest way to break into the organization's security perimeter. As mentioned previously, footprinting is the easiest way to gather information about the target organization; this plays a vital role in the hacking process.

Footprinting helps to:

- **Know Security Posture**

  Performing footprinting on the target organization in a systematic and methodical manner gives the complete profile of the organization's security posture. You can analyze this report to figure out loopholes in the security posture of your target organization and then you can build your hacking plan accordingly.

- **Reduce Attack Area**

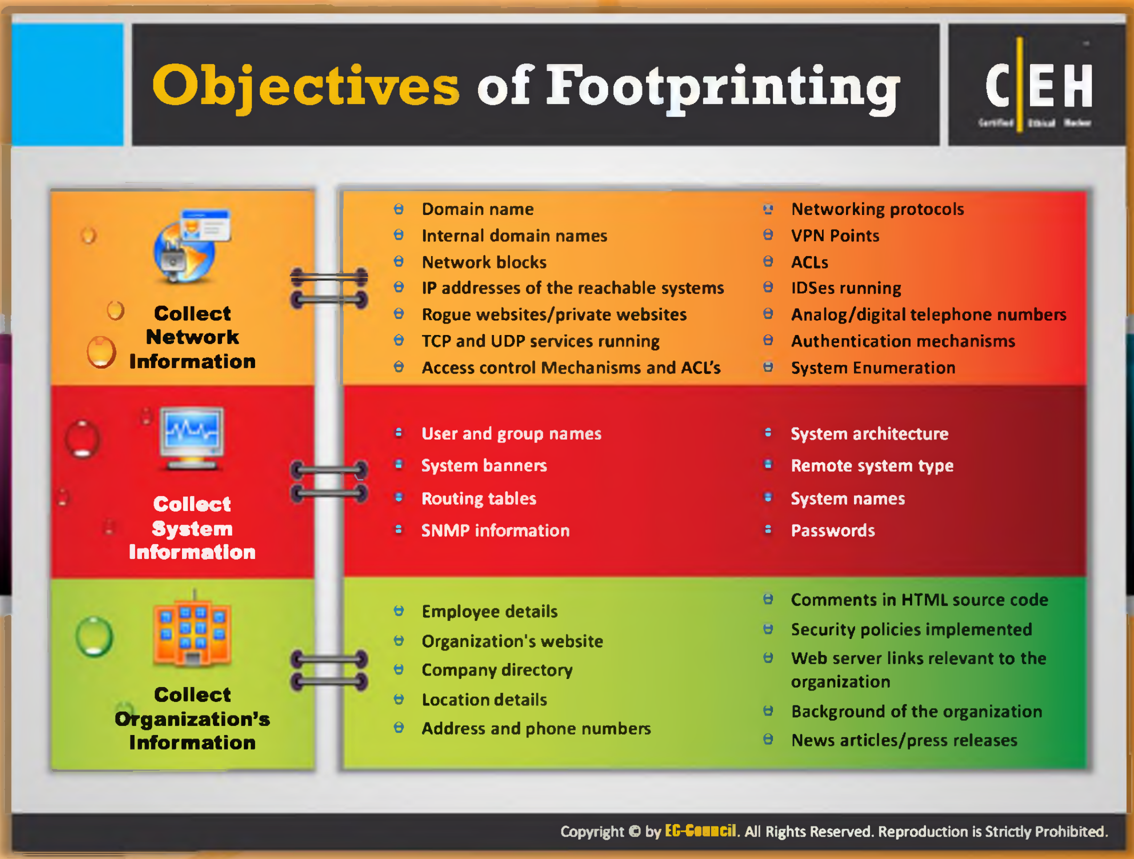
  By using a combination of tools and techniques, attackers can take an unknown entity (for example XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to its security posture.

- **Build Information Database**

A detailed footprint provides maximum information about the target organization. Attackers can build their own information database about security weakness of the target organization. This database can then be analyzed to find the easiest way to break into the organization's security perimeter.

- **Draw Network Map**

Combining footprinting techniques with tools such as Tracert allows the attacker to create network diagrams of the target organization’s network presence. This network map represents their understanding of the **target's Internet footprint**. These network diagrams can guide the attack.



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
- Access control Mechanisms and ACL's
- Networking protocols
- VPN Points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System Enumeration

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
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles/press releases

Objectives of Footprinting

The major objectives of footprinting include collecting the target's network information, system information, and the organizational information. By carrying out footprinting at various network levels, you can gain information such as: network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, and access control mechanisms. With footprinting, information such as employee names, phone numbers, contact addresses, designation, and work experience, and so on can also be obtained.

Collect Network Information

The network information can be gathered by performing a Whois database analysis, trace routing, etc. includes:

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites

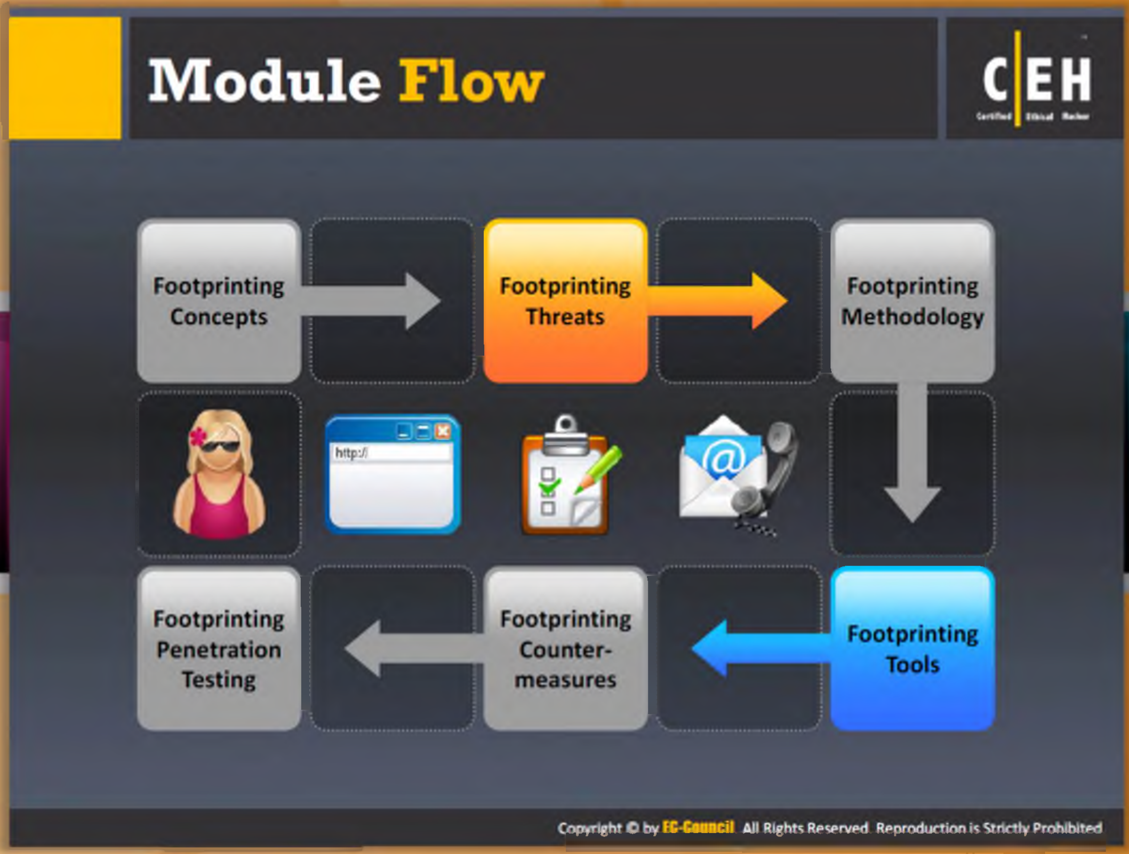
- TCP and UDP services running
- Access control mechanisms and ACLs
- Networking protocols
- VPN points
- ACLs
- IDSes running
- Analog/digital telephone numbers
- Authentication mechanisms
- System enumeration

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
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles/press releases



Module Flow

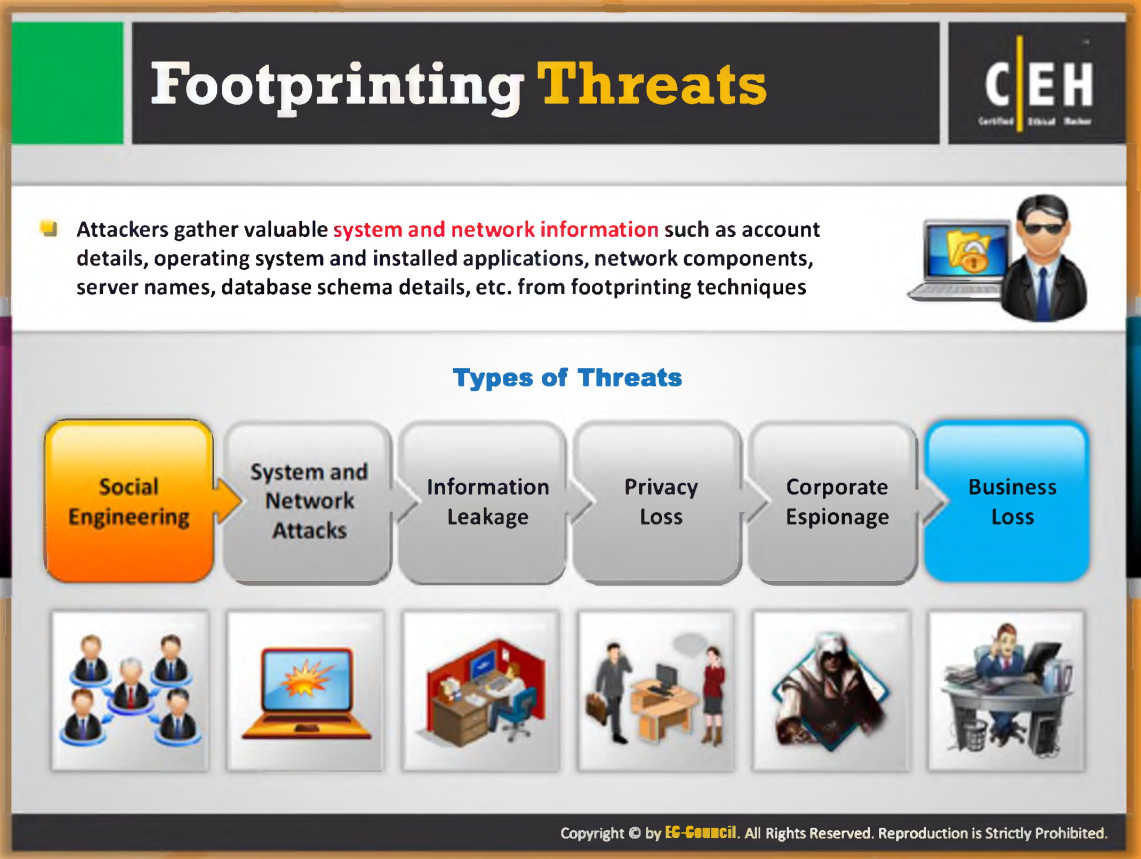
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we discussed footprinting concepts, and now we will discuss the threats associated with footprinting:

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

The Footprinting Threats section familiarizes you with the threats associated with footprinting such as social engineering, system and network attacks, corporate espionage, etc.



Footprinting Threats

- Attackers gather valuable system and network information such as account details, operating system and installed applications, network components, server names, database schema details, etc. from footprinting techniques

Types of Threats

Social Engineering → System and Network Attacks → Information Leakage → Privacy Loss → Corporate Espionage → Business Loss

Footprinting Threats

As discussed previously, attackers perform footprinting as the first step in an attempt to hack a target organization. In the footprinting phase, attackers try to collect valuable system-level information such as account details, operating system and other software versions, server names, and database schema details that will be useful in the hacking process.

The following are various threats due to footprinting:

Social Engineering

Without using any intrusion methods, hackers directly and indirectly collect information through persuasion and various other means. Here, crucial information is gathered by the hackers through employees without their consent.

System and Network Attacks

Footprinting helps an attacker to perform system and network attacks. Through footprinting, attackers can gather information related to the target organization's system configuration, operating system running on the machine, and so on. Using this information, attackers can find the vulnerabilities present in the target system and then can exploit those vulnerabilities. Thus, attackers can take control over a target system. Similarly, attackers can also take control over the entire network.

Information Leakage

Information leakage can be a great threat to any organization and is often overlooked. If sensitive organizational information falls into the hands of attackers, then they can build an attack plan based on the information, or use it for monetary benefits.

Privacy Loss

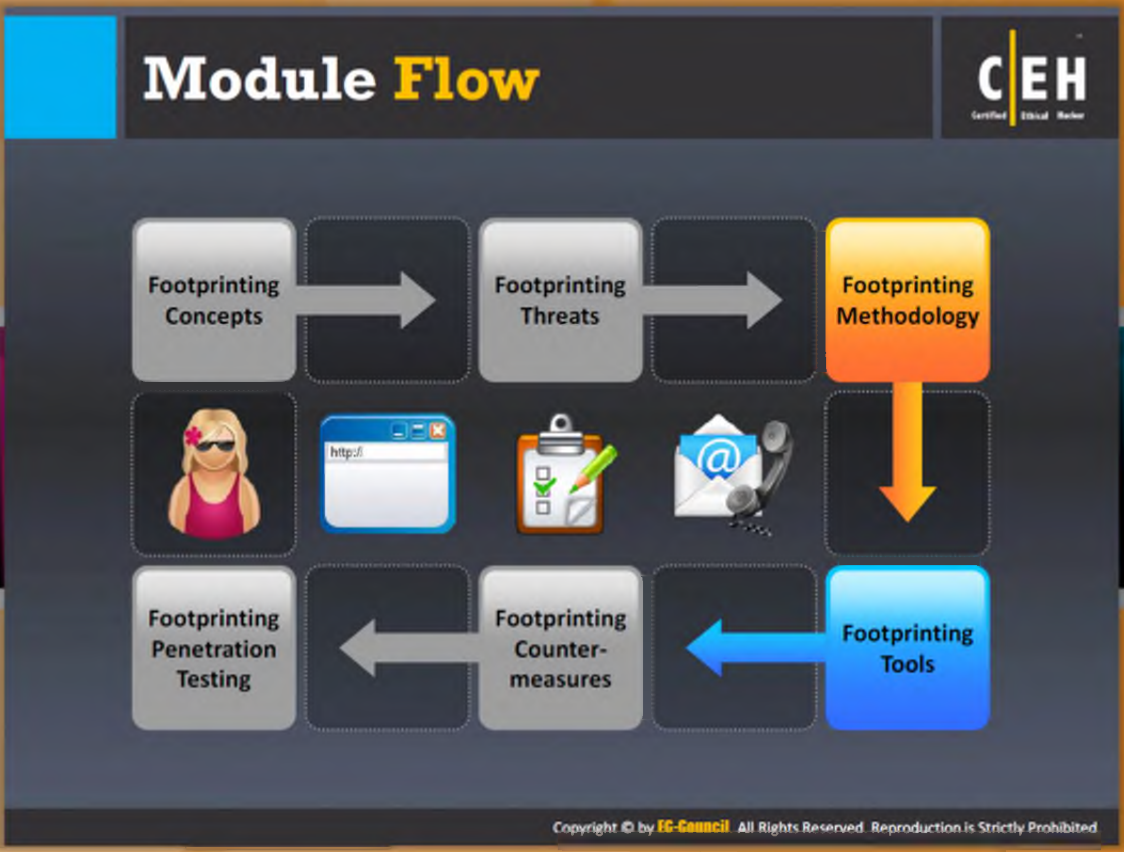
With the help of footprinting, hackers are able to access the systems and networks of the company and even escalate the privileges up to admin levels. Whatever privacy was maintained by the company is completely lost.

Corporate Espionage

Corporate espionage is one of the major threats to companies as competitors can spy and attempt to steal sensitive data through footprinting. Due to this type of espionage, competitors are able to launch similar products in the market, affecting the market position of a company.

Business Loss

Footprinting has a major effect on businesses such as online businesses and other ecommerce websites, banking and financial related businesses, etc. Billions of dollars are lost every year due to malicious attacks by hackers.



Module Flow

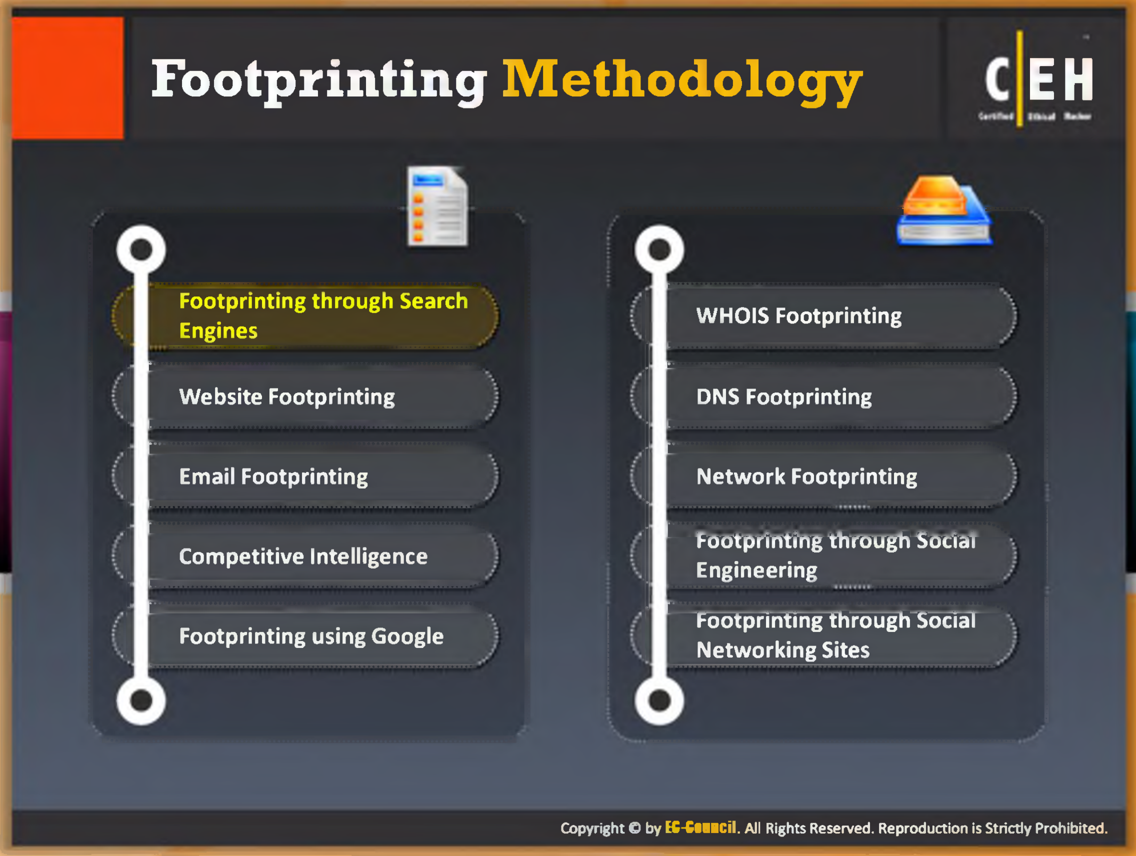
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Now that you are familiar with footprinting concepts and threats, we will discuss the footprinting methodology.

The footprinting methodology section discusses various techniques used to collect information about the **target organization** from different sources.

Footprinting Concepts	**Footprinting Tools**
Footprinting Threats	**Footprinting Countermeasures**
Footprinting Methodology	**Footprinting Penetration Testing**



Footprinting Methodology

- Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting using Google
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

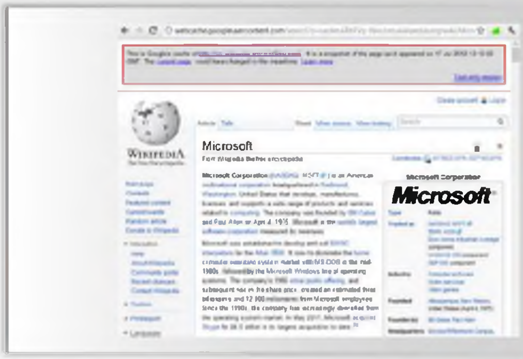
The footprinting methodology is a procedural way of collecting information about a target organization from all available sources. It deals with gathering information about a target organization, determining URL, location, establishment details, number of employees, the specific range of domain names, and contact information. This information can be gathered from various sources such as search engines, Whois databases, etc.

Search engines are the main information sources where you can find valuable information about your target organization. Therefore, first we will discuss footprinting through search engines. Here we are going to discuss how and what information we can collect through search engines.

Examples of search engines include: www.google.com, www.yahoo.com, www.bing.com

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)

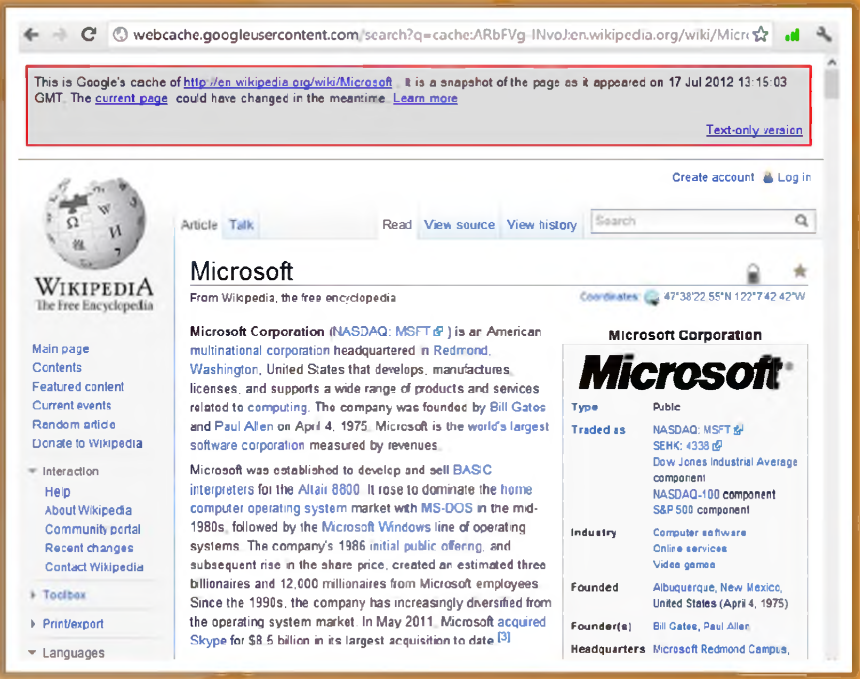


Footprinting through Search Engines

A web search engine is designed to search for information on the World Wide Web. The search results are generally presented in a line of results often referred to as search engine results pages (SERPs). In the present world, many search engines allow you to extract a target organization's information such as technology platforms, employee details, login pages, intranet portals, and so on. Using this information, an attacker may build a **hacking strategy** to break into the target organization's network and may carry out other types of advanced system attacks. A Google search could reveal submissions to forums by security personnel that reveal brands of firewalls or **antivirus software** in use at the target. Sometimes even network diagrams are found that can guide an attack.

If you want to footprint the target organization, for example XYZ pvt ltd, then type XYZ pvt ltd in the Search box of the search engine and press Enter. This will display all the search results containing the keywords "XYZ pvt ltd." You can even narrow down the results by adding a specific keyword while searching. Furthermore, we will discuss other **footprinting techniques** such as website footprinting and email Footprinting.

For example, consider an organization, perhaps Microsoft. Type Microsoft in the Search box of a search engine and press Enter; this will display all the results containing information about Microsoft. Browsing the results may provide critical information such as **physical location**, contact address, the services offered, number of employees, etc. that may prove to be a valuable source for hacking.



This is Google's cache of http://en.wikipedia.org/wiki/Microsoft. It is a snapshot of the page as it appeared on 17 Jul 2012 13:15:03 GMT. The current page could have changed in the meantime. Learn more

Text-only version

Microsoft

From Wikipedia, the free encyclopedia

Coordinates: 47°38'22.55"N 122°7'42.42"W

Microsoft Corporation (NASDAQ: MSFT) is an American multinational corporation headquartered in Redmond, Washington, United States that develops, manufactures, licenses, and supports a wide range of products and services related to computing. The company was founded by Bill Gates and Paul Allen on April 4, 1975. Microsoft is the world's largest software corporation measured by revenues.

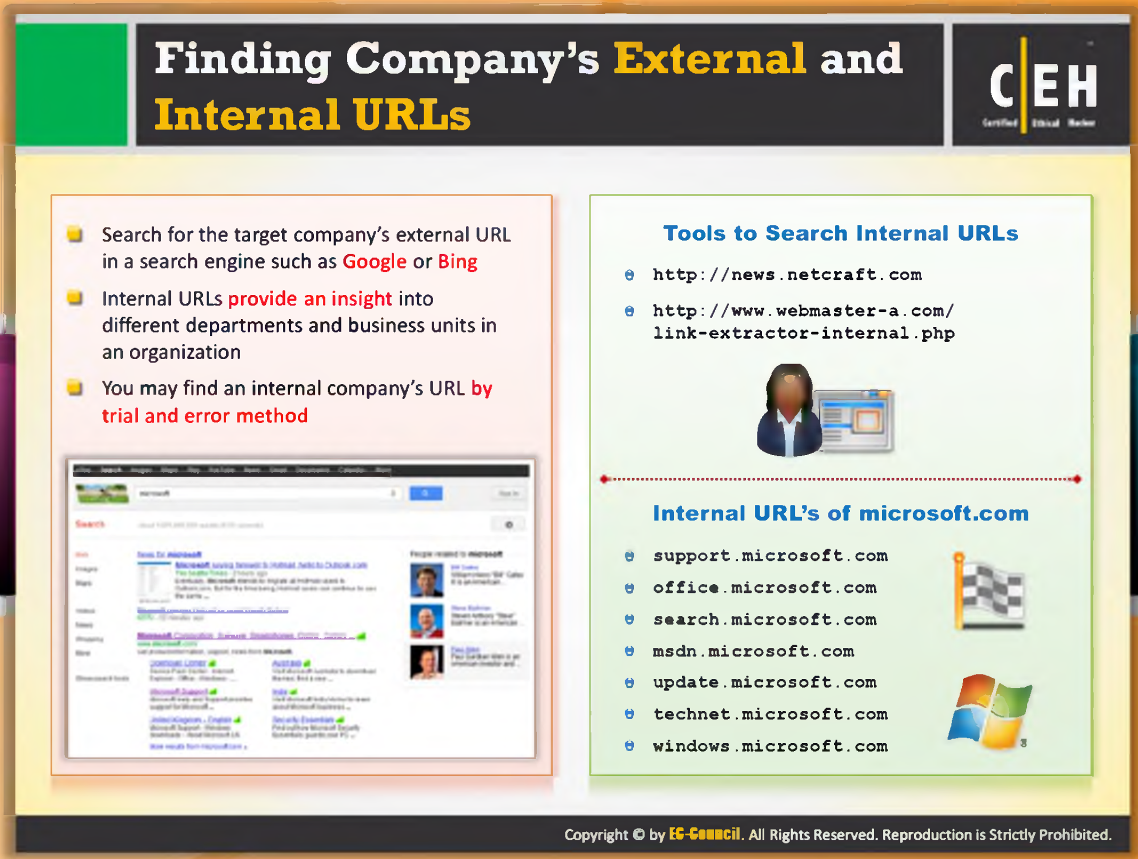
Microsoft was established to develop and sell BASIC interpreters for the Altair 8800. It rose to dominate the home computer operating system market with MS-DOS in the mid-1980s, followed by the Microsoft Windows line of operating systems. The company's 1986 initial public offering, and subsequent rise in the share price, created an estimated three billionaires and 12,000 millionaires from Microsoft employees. Since the 1990s, the company has increasingly diversified from the operating system market. In May 2011, Microsoft acquired Skype for $8.5 billion in its largest acquisition to date.[3]

Microsoft Corporation

Type	Public
Traded as	NASDAQ: MSFT SEHK: 4338 Dow Jones Industrial Average component NASDAQ-100 component S&P 500 component
Industry	Computer software Online services Video games
Founded	Albuquerque, New Mexico, United States (April 4, 1975)
Founder(s)	Bill Gates, Paul Allen
Headquarters	Microsoft Redmond Campus,

FIGURE 2.1: Screenshot showing information about Microsoft

As an ethical hacker, if you find any **sensitive information** of your company in the search engine result pages, you should remove that information. Although you remove the sensitive information, it may still be available in a search engine cache. Therefore, you should also check the search engine cache to ensure that the sensitive data is removed **permanently**.



Finding Company's External and Internal URLs

- Search for the target company's external URL in a search engine such as Google or Bing
- 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

Internal URL's of microsoft.com

- support.microsoft.com
- office.microsoft.com
- search.microsoft.com
- msdn.microsoft.com
- update.microsoft.com
- technet.microsoft.com
- windows.microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Company's External and Internal URLs

A company's external and internal URLs provide a lot of useful information to the attacker. These URLs describe the company and provide details such as the company mission and vision, history, products or services offered, etc. The URL that is used outside the corporate network for accessing the company's vault server via a firewall is called an external URL. It links directly to the company's external web page. The target company's external URL can be determined with the help of search engines such as Google or Bing.

If you want to find the external URL of a company, follow these steps:

1. Open any of the search engines, such as Google or Bing.
2. Type the name of the target company in the Search box and press Enter.

The internal URL is used for accessing the company's vault server directly inside the corporate network. The internal URL helps to access the internal functions of a company. Most companies use common formats for internal URLs. Therefore, if you know the external URL of a company, you can predict an internal URL through trial and error. These internal URLs provide insight into different departments and business units in an organization. You can also find the internal URLs of an organization using tools such as netcraft.

Tools to Search Internal URLs

Netcraft

Source: http://news.netcraft.com

Netcraft deals with web server, web **hosting market-share** analysis, and operating system detection. It provides free anti-phishing toolbar (Net craft toolbar) for Firefox as well as Internet Explorer browsers. The netcraft toolbar avoids phishing attacks and protects the Internet users from fraudsters. It checks the risk rate as well as the hosting location of the websites we visit.

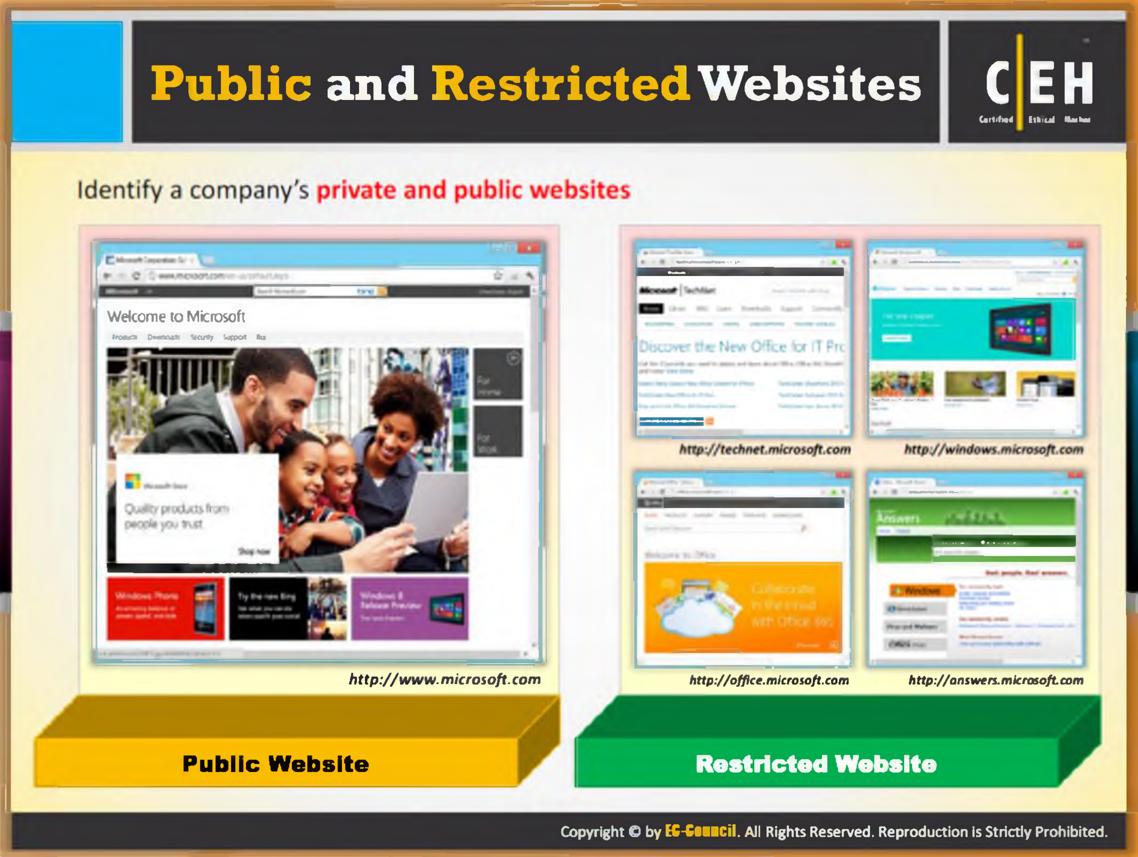
Link Extractor

Source: http://www.webmaster-a.com/link-extractor-internal.php

Link Extractor is a link extraction utility that allows you to choose between external and internal URLs, and will return a plain list of URLs linked to or an html list. You can use this utility to **competitor sites**.

Examples of internal URLs of microsoft.com:

- support.microsoft.com
- office.microsoft.com
- search.microsoft.com
- msdn.microsoft.com
- update.microsoft.com
- technet.microsoft.com
- windows.microsoft.com


Welcome to Microsoft
Quality products from people you trust
Discover the New Office for IT Pro
Answers

Public and Restricted Websites

Identify a company's private and public websites

http://www.microsoft.com

http://technet.microsoft.com

http://windows.microsoft.com

http://office.microsoft.com

http://answers.microsoft.com

Public Website

Restricted Website

Public and Restricted Websites

A public website is a website designed to show the presence of an organization on the Internet. It is designed to attract customers and partners. It contains information such as company history, services and products, and contact information of the organization.

The following screenshot is an example of a public website:

Source: http://www.microsoft.com

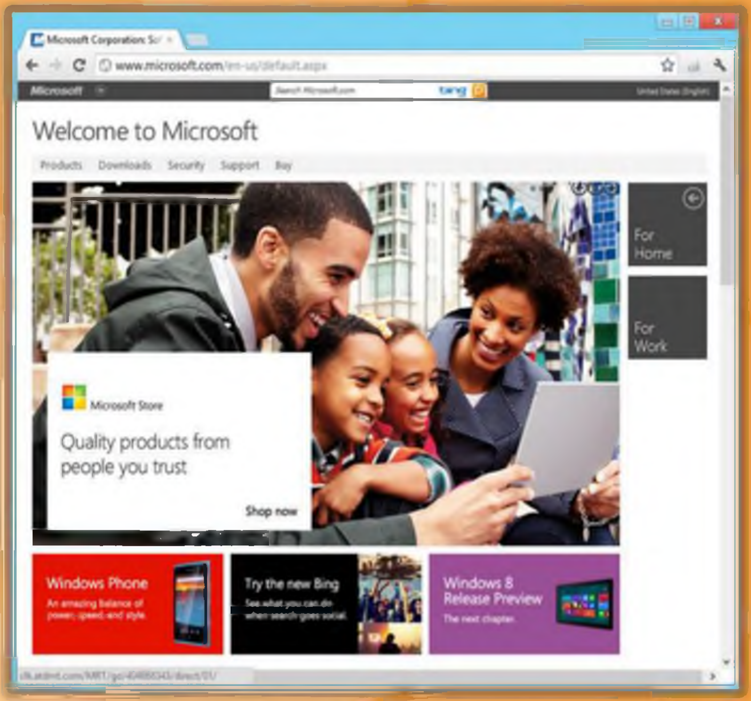

Microsoft Corporation: So
www.microsoft.com/en-us/default.aspx
Microsoft
Search Microsoft.com
bing
Welcome to Microsoft
Products Downloads Security Support Buy
For Home
For Work
Microsoft Store
Quality products from people you trust
Shop now
Windows Phone
An amazing balance of power, speed and style
Try the new Bing
See what you can do when search goes social
Windows 8 Release Preview
The next chapter

FIGURE 2.2: An example of public website

A restricted website is a website that is available to only a few people. The people may be employees of an organization, members of a department, etc. **Restrictions** can be applied based on the IP number, domain or subnet, username, and password.

Restricted or private websites of microsoft.com include: http://technet.microsoft.com, http://windows.microsoft.com, http://office.microsoft.com, and http://answers.microsoft.com.

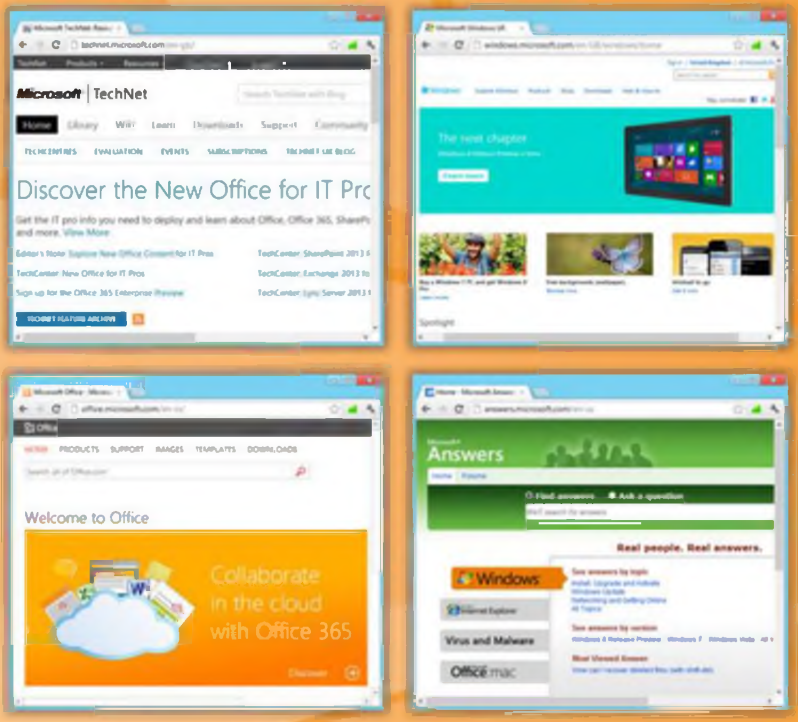
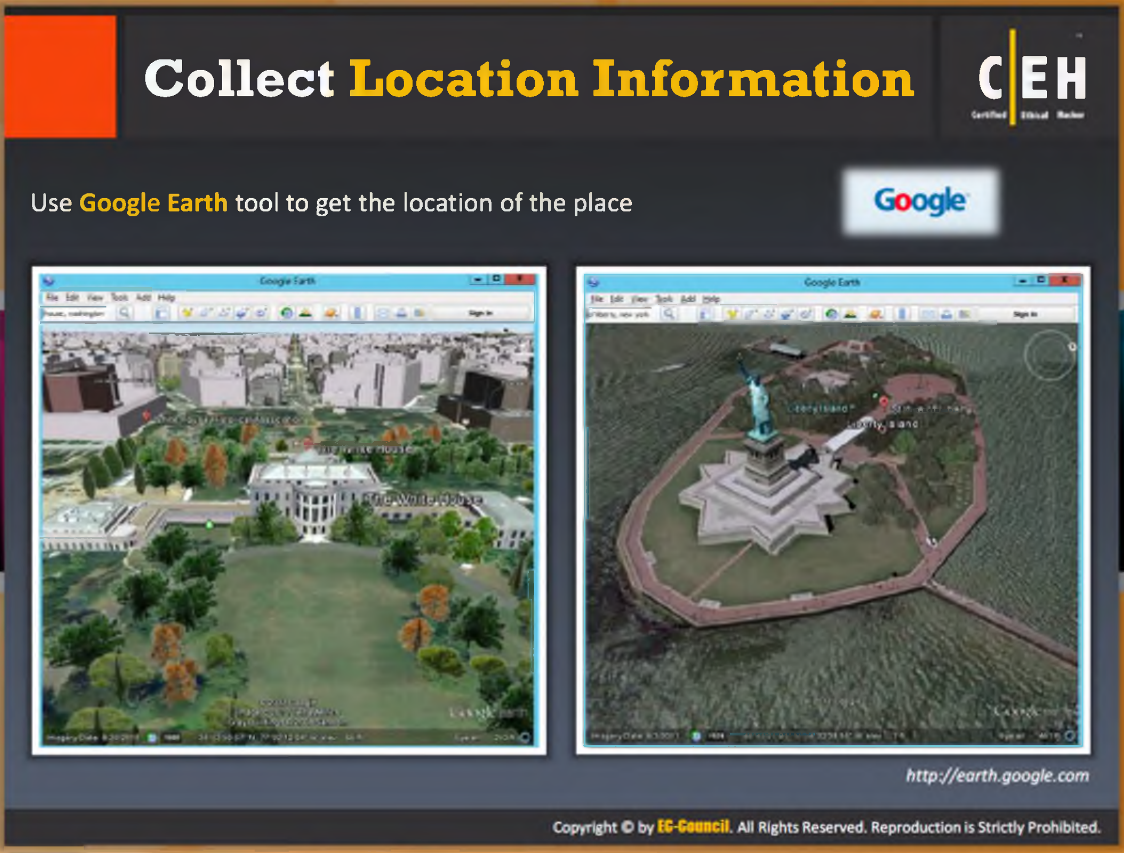


FIGURE 2.3: Examples of Public and Restricted websites



Collect Location Information

Use **Google Earth** tool to get the location of the place

http://earth.google.com

Collect Location Information

Information such as physical location of the organization plays a vital role in the hacking process. This information can be obtained using the footprinting technique. In addition to physical location, we can also collect information such as surrounding public Wi-Fi hotspots that may prove to be a way to break into the **target organization's network**.

Attackers with the knowledge of a target organization's location may attempt dumpster diving, surveillance, social engineering, and other non-technical attacks to gather much more information about the target organization. Once the location of the target is known, detailed satellite images of the location can be obtained using various sources available on the Internet such as http://www.google.com/earth and https://maps.google.com. Attackers can use this information to gain **unauthorized access** to buildings, wired and wireless networks, systems, and so on.

Example: earth.google.com

Google Earth is a valuable tool for **hacking** that allows you to find a location, point, and zoom into that location to explore. You can even **access 3D images** that depict most of the Earth in high-resolution detail.

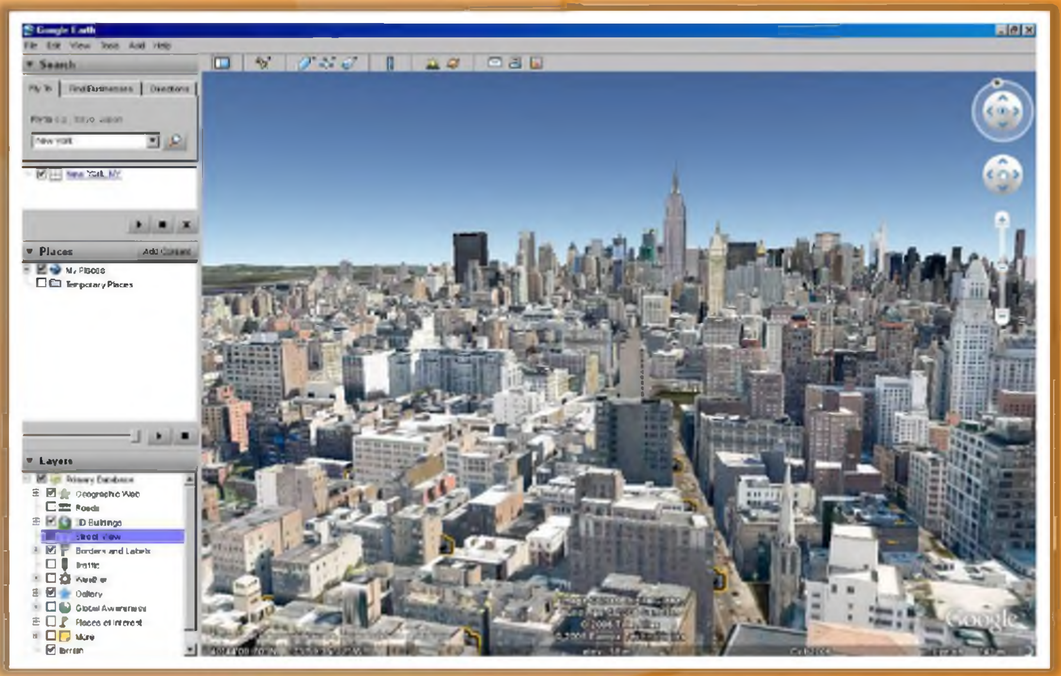


FIGURE 2.4: Google Earth showing location

Example: maps.google.com

Google Maps provides a Street View feature that provides you with a series of images of building, as well as its surroundings, including **WI-FI networks**. Attackers may use Google Maps to find or locate entrances to buildings, security cameras, gates, places to hide, weak spots in perimeter fences, and utility resources like electricity connections, to measure distance between different objects, etc.

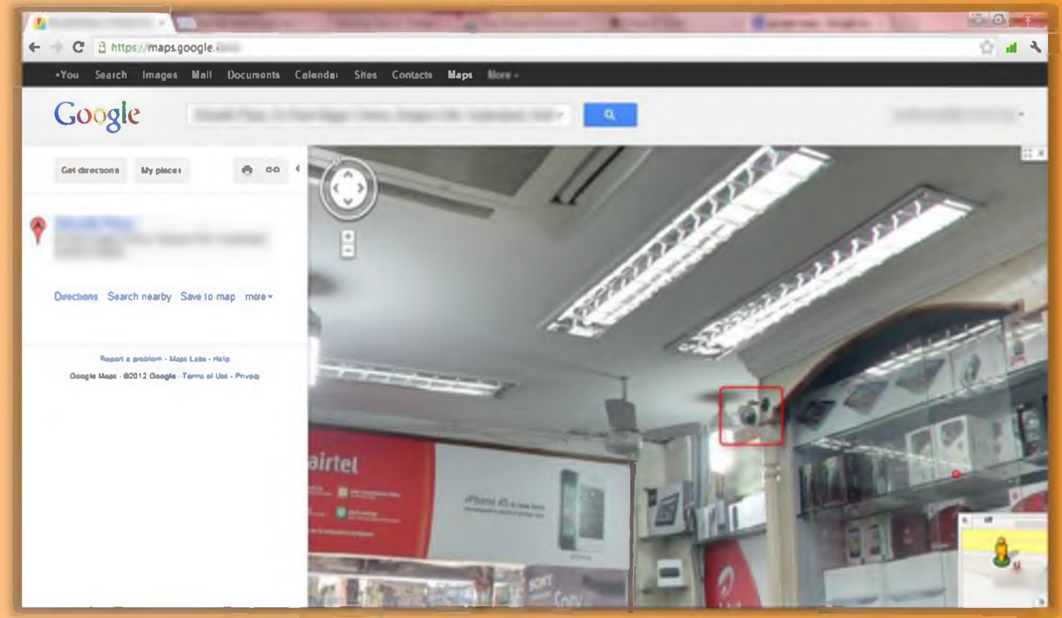
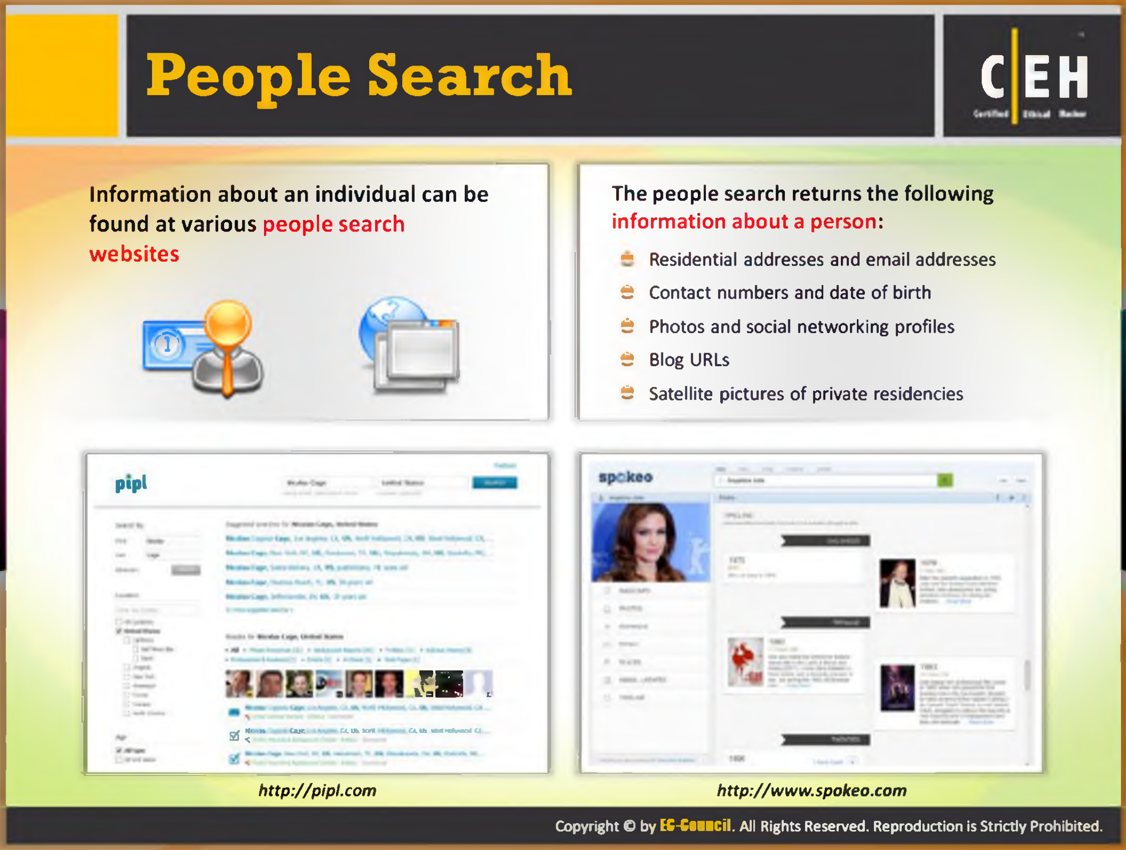


FIGURE 2.5: Google Maps showing a Street View



People Search

Information about an individual can be found at various people search websites

The people search returns the following information about a person:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residencies

http://pipl.com

http://www.spokeo.com

People Search

You can use the public record websites to find information about people's email addresses, phone numbers, house addresses, and other information. Using this information you can try to obtain bank details, credit card details, mobile numbers, past history, etc. There are many people search online services available that help find people. http://pipl.com and http://www.spokeo.com are examples of people search services that allow you to search for the people with their name, email, username, phone, or address.

These people search services may provide information such as:

- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles
- Blog URLs
- Satellite pictures of private residences

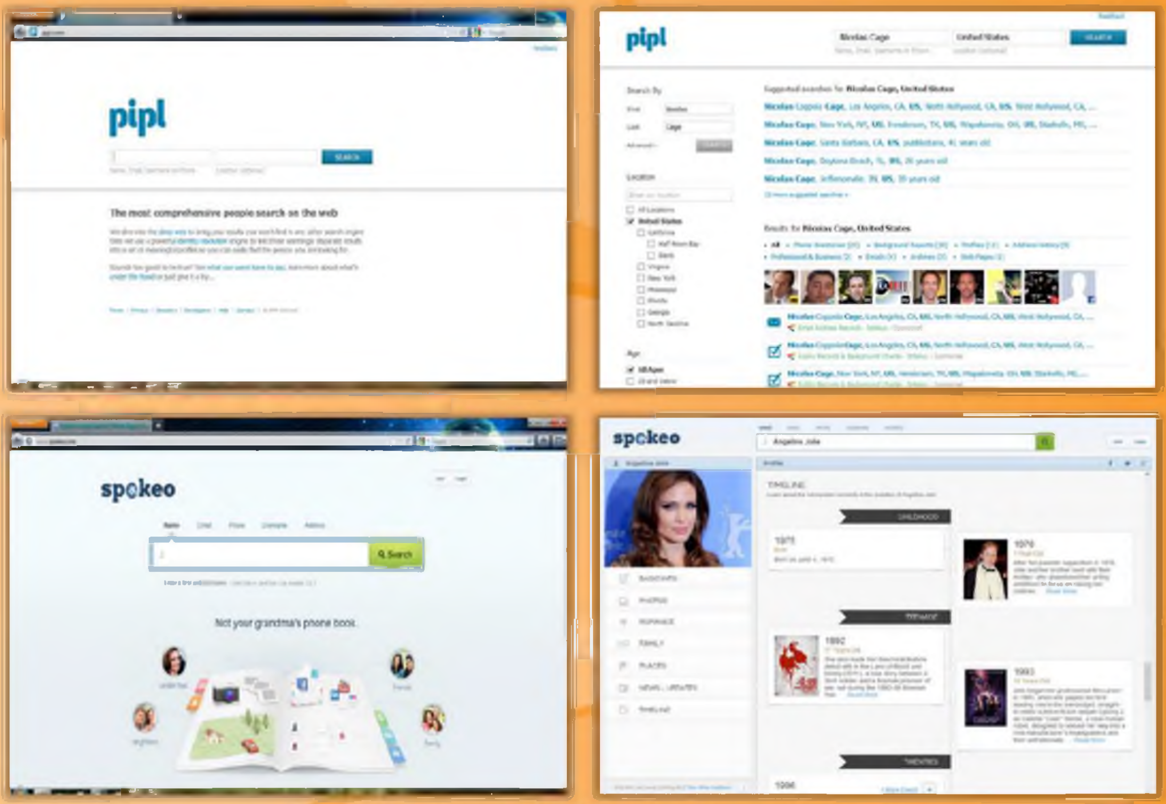
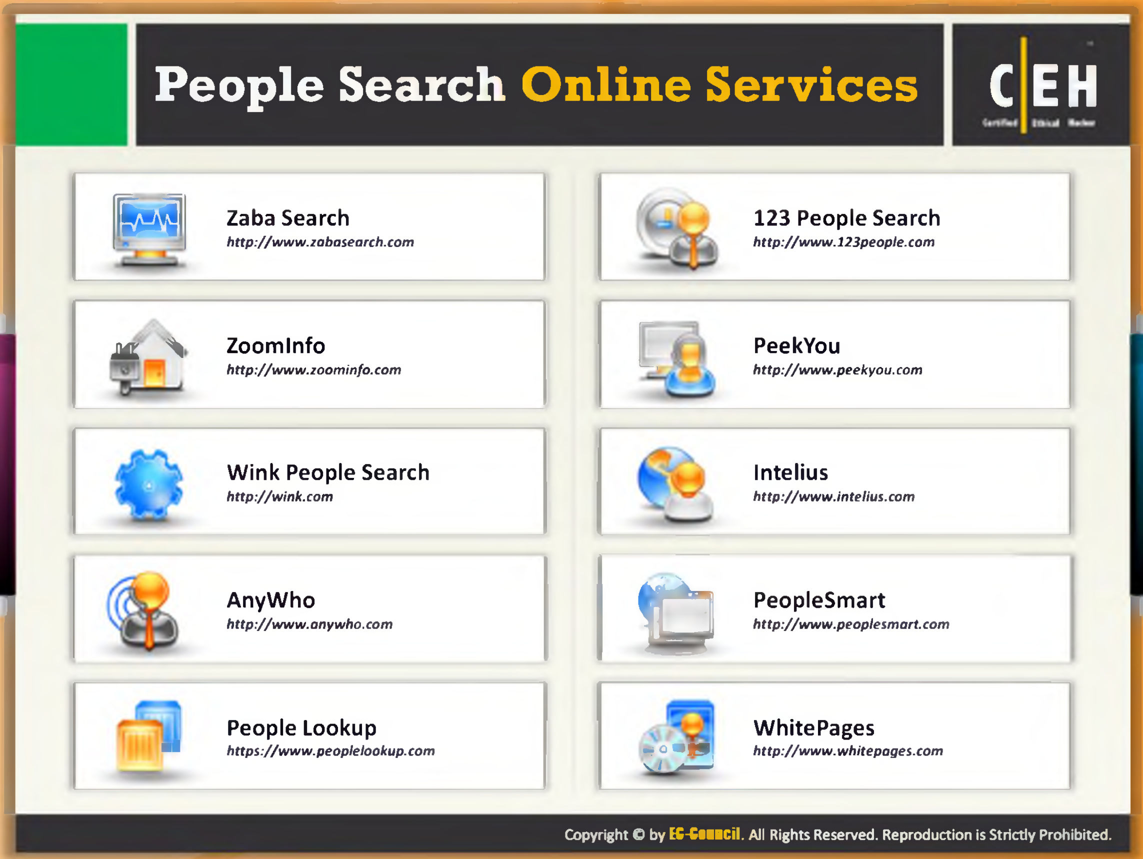


FIGURE 2.6: Examples of People search online service websites



People Search Online Services

Zaba Search
http://www.zabasearch.com

ZoomInfo
http://www.zoominfo.com

Wink People Search
http://wink.com

AnyWho
http://www.anywho.com

People Lookup
https://www.peoplelookup.com

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

PeekYou
http://www.peekyou.com

Intelius
http://www.intelius.com

PeopleSmart
http://www.peoplesmart.com

WhitePages
http://www.whitepages.com

People Search Online Services

At present, many Internet users are using people search engines to find information about other people. Most often people search engines provide **people's names, addresses, and contact details**. Some people search engines may also reveal the type of work an individual does, businesses owned by a person, contact numbers, company email addresses, mobile numbers, fax numbers, dates of birth, personal -mail addresses, etc. This information proves to be highly beneficial for attackers to launch attacks.

Some of the people search engines are listed as follows:

Zaba Search

Source: http://www.zabasearch.com

Zaba Search is a people search engine that provides information such as address, phone number, current location, etc. of people in the US. It allows you to search for people by their name.

ZoomInfo

Source: http://www.zoominfo.com

Zoom Info is a business people directory using which you can find business contacts, people's professional profiles, biographies, work histories, affiliations, links to **employee profiles** with verified contact information, and more.

Wink People Search

Source: http://wink.com

Wink People Search is a people search engine that provides information about people by name and location. It gives phone number, address, websites, photos, work, school, etc.

AnyWho

Source: http://www.anywho.com

AnyWho is a website that helps you find information about people, their businesses, and their locations online. With the help of a **phone number**, you can get all the details of an individual.

People Lookup

Source: https://www.peoplelookup.com

People Lookup is a people search engine that allows you to find, locate, and then connect with people. It also allows you to look up a phone number, search for cell numbers, find an address or phone number, and search for people in the US. This **database** uses information from **public records**.

123 People Search

Source: http://www.123people.com

123 People Search is a people search tool that allows you to find information such as public records, phone numbers, addresses, images, videos, and email addresses.

PeekYou

Source: http://www.peekyou.com

PeekYou is a people search engine that allows you to search for profiles and contact information of people in India and cities' top **employers** and **schools**. It allows you to search for the people with their names or usernames.

Intelius

Source: http://www.intelius.com

Intelius is a public records business that provides information services. It allows you to search for the people in US with their name, address, phone number, or **email address**.

PeopleSmart

Source: http://www.peoplesmart.com

People Smart is a people search service that allows you to find people's work information with their name, city, and state. In addition, it allows you to perform **reverse phone lookups,** email searches, searches by address, and county searches.

WhitePages

Source: http://www.whitepages.com

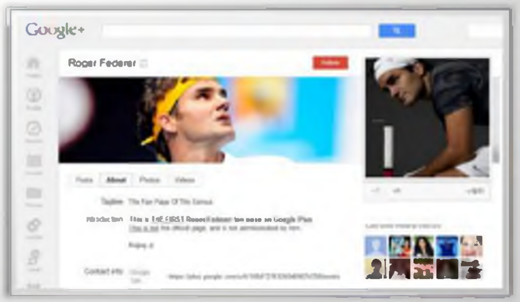
WhitePages is a people search engine that provides information about people by name and location. Using the phone number, you can find the **person's address**.

People Search on Social Networking Services

http://www.facebook.com

http://www.linkedin.com

http://twitter.com



https://plus.google.com

People Search on Social Networking Services

Searching for people on social networking websites is easy. Social networking services are the online services, platforms, or sites that focus on facilitating the building of social networks or social relations among people. These websites provide information that is provided by users. Here, people are directly or indirectly related to each other by common interest, work location, or educational communities, etc.

Social networking sites allow people to share information quickly and effectively as these sites are updated in real time. It allows updating facts about upcoming or current events, recent announcements and invitations, and so on. Therefore, social networking sites prove to be a great platform for searching people and their related information. Through people searching on social networking services, you can gather critical information that will be helpful in performing social engineering or other kinds of attacks.

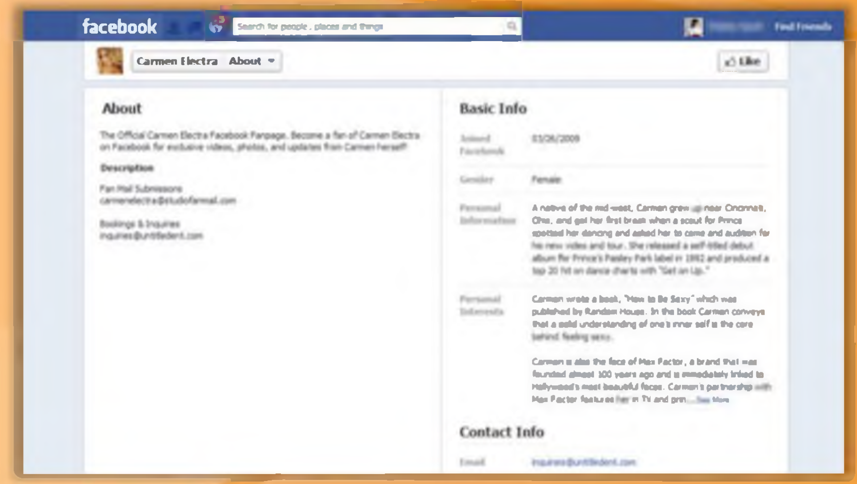
Many social networking sites allow visitors to search for people without registration; this makes people searching on social networking sites an easy task for you. You can search a person using name, email, or address. Some sites allow you to check whether an account is currently in use or not. This allows you to check the status of the person you are looking for.

Some of social networking services are as follows:

Facebook

Source: http://www.facebook.com

Facebook allows you to search for people, their **friends**, **colleagues**, and **people** living around them and others with whom they are affiliated. In addition, you can also find their professional information such as their company or business, current location, phone number, email ID, photos, videos, etc. It allows you to search for people by username or email address.



About

The Official Carmen Electra Facebook Fanpage. Become a fan of Carmen Electra on Facebook for exclusive videos, photos, and updates from Carmen herself!

Description

Fan Mail Submissions
carmenelectra@studiofanmail.com

Bookings & Inquiries
inquiries@untitledent.com

Basic Info

Joined Facebook 01/26/2009

Gender Female

Personal Information A native of the mid-west, Carmen grew up near Cincinnati, Ohio, and got her first break when a scout for Prince spotted her dancing and asked her to come and audition for his new video and tour. She released a self-titled debut album for Prince's Paisley Park label in 1992 and produced a top 20 hit on dance charts with "Get on Up."

Personal Interests Carmen wrote a book, "How to Be Sexy" which was published by Random House. In the book Carmen conveys that a solid understanding of one's inner self is the core behind feeling sexy.

Carmen is also the face of Max Factor, a brand that was founded almost 100 years ago and is immediately linked to Hollywood's most beautiful faces. Carmen's partnership with Max Factor features her in TV and prin... See More

Contact Info

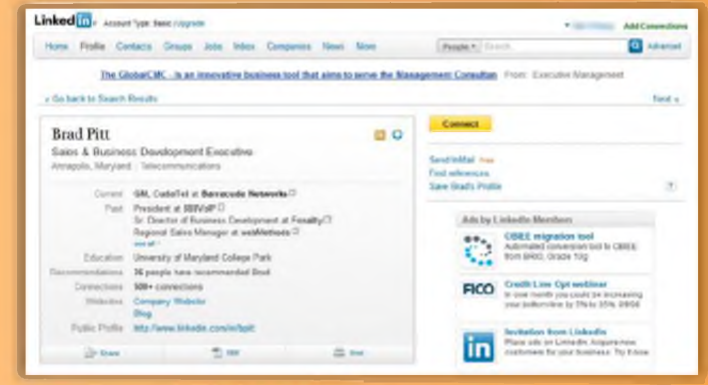
Email inquiries@untitledent.com

FIGURE 2.7: Facebook a social networking service to search for people across the world

LinkedIn

Source: http://www.linkedin.com

LinkedIn is a **social networking website** for professional people. It allows you to find people by name, keyword, company, school, etc. Searching for people on LinkedIn gives you information such as name, designation, name of company, current location, and education qualifications, but to use LinkedIn you need to be registered with the site.



The GlobalCMC - is an innovative business tool that aims to serve the Management Consultan From: Executive Management

« Go back to Search Results Next »

Brad Pitt
Sales & Business Development Executive
Annapolis, Maryland Telecommunications

Current GM, CudaTel at Barracuda Networks
Past President at [illegible]
Sr. Director of Business Development at Fonality
Regional Sales Manager at webMethods
see all
Education University of Maryland College Park
Recommendations 36 people have recommended Brad
Connections 500+ connections
Websites Company Website
Blog
Public Profile http://www.linkedin.com/in/bpitt

Send InMail
Find references
Save Brad's Profile

Ads by LinkedIn Members

CBEE migration tool
Automated conversion tool to CBEE from BRIO, Oracle 10g

FICO Credit Line Opt webinar
In one month you could be increasing your [illegible]

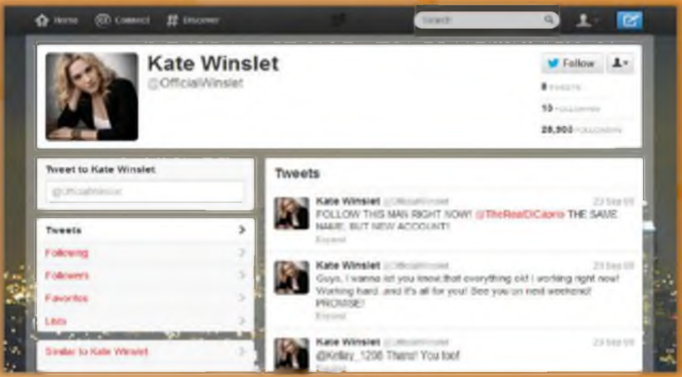
Invitation from LinkedIn
Place ads on LinkedIn. Acquire new customers for your business. Try it now

FIGURE 2.8: LinkedIn screenshot

Twitter

Source: http://twitter.com

Twitter is a social networking service that allows people to send and **read text messages** (tweets). Even unregistered users can read tweets on this site.



Kate Winslet
@OfficialWinslet

8 TWEETS
15 FOLLOWING
28,900 FOLLOWERS

Tweets

Kate Winslet @OfficialWinslet 23 Sep 09
FOLLOW THIS MAN RIGHT NOW! @TheRealDiCaprio THE SAME NAME, BUT NEW ACCOUNT!
Expand

Kate Winslet @OfficialWinslet 23 Sep 09
Guys, I wanna let you know that everything ok! I working right now! Working hard, and it's all for you! See you on next weekend! PROMISE!
Expand

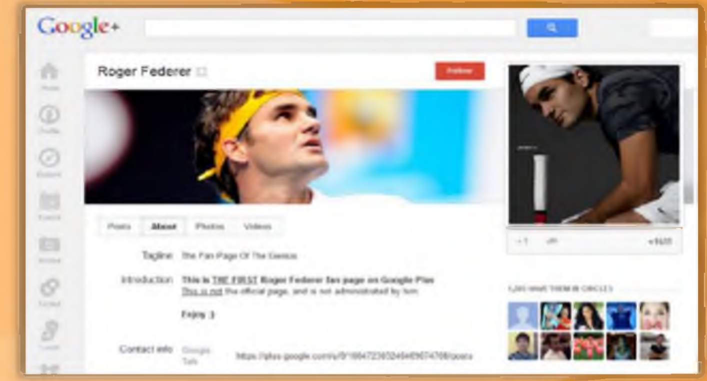
Kate Winslet @OfficialWinslet 23 Sep 09
@Kelley_1208 Thanx! You too!

FIGURE 2.9: Twitter screenshot

Google+

Source: https://plus.google.com

Google+ is a social networking site that aims to make sharing on the web more like **sharing in real life.** You can grab a lot of useful information about users from this site and use it to hack their systems.



Tagline: The Fan Page Of The Genius

Introduction: This is THE FIRST Roger Federer fan page on Google Plus
This is not the official page, and is not administrated by him.

Enjoy :)

Contact info: Google Talk [illegible]

FIGURE 2.10: Google+ screenshot

Gather Information from Financial Services

Google Finance
(http://finance.google.com/finance)

Yahoo Finance
(http://finance.yahoo.com)

Gather Information from Financial Services

Financial services such as Google Finance, Yahoo! Finance, and so on provide a lot of useful information such as the market value of a company's shares, company profile, competitor details, etc. The information offered varies from one service to the next. In order to avail themselves of services such as e-mail alerts and phone alerts, users need to register on the financial services. This gives an opportunity for an attacker to **grab useful information** for **hacking.**

Many financial firms rely on web access, performing transactions, and user access to their accounts. Attackers can obtain sensitive and private information of users using information theft, key loggers, etc. Attackers can even grab this information by implementing cybercrimes, and exploit it with the help of non-vulnerable threats (software design flaw example; breaking authentication mechanism).

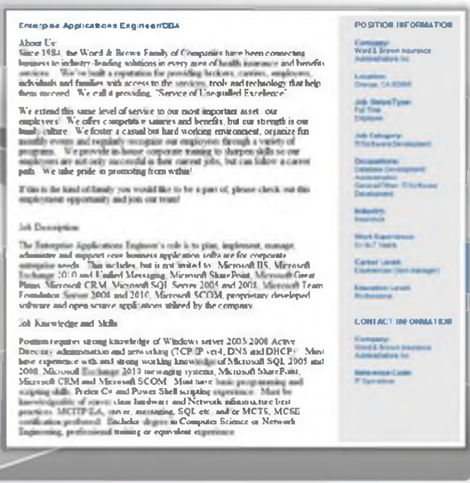
The following are some of non-vulnerable threats:

- Service flooding
- Brute force attack
- Phishing

FIGURE 2.11: Examples of financial services website for gathering information

Footprinting through Job Sites

You can gather company's infrastructure details from job postings



Enterprise Applications Engineer/DBA

About Us:
Since 1984, the Word & Brown Family of Companies have been connecting business to industry-leading solutions in every area of health insurance and benefits services. We've built a reputation for providing brokers, carriers, employers, individuals and families with access to the services, tools and technology that help them succeed. We call it providing "Service of Unequalled Excellence".

We extend this same level of service to our most important asset: our employees! We offer competitive salaries and benefits, but our strength is our family culture. We foster a casual but hard working environment, organize fun monthly events and regularly recognize our employees through a variety of programs. We provide in-house corporate training to sharpen skills so our employees are not only successful in their current jobs, but can follow a career path. We take pride in promoting from within!

If this is the kind of family you would like to be a part of, please check out this employment opportunity and join our team!

Job Description

The Enterprise Applications Engineer's role is to plan, implement, manage, administer and support core business application software for corporate enterprise needs. This includes, but is not limited to: Microsoft IIS, Microsoft Exchange 2010 and Unified Messaging, Microsoft SharePoint, Microsoft Great Plains, Microsoft CRM, Microsoft SQL Server 2005 and 2008, Microsoft Team Foundation Server 2008 and 2010, Microsoft SCOM, proprietary developed software and open source applications utilized by the company.

Job Knowledge and Skills

Position requires strong knowledge of Windows server 2003/2008 Active Directory administration and networking (TCP/IP v4, DNS and DHCP). Must have experience with and strong working knowledge of Microsoft SQL 2005 and 2008, Microsoft Exchange 2010 messaging systems, Microsoft SharePoint, Microsoft CRM and Microsoft SCOM. Must have basic programming and scripting skills. Prefer C# and Power Shell scripting experience. Must be knowledgeable of server class hardware and Network infrastructure best practices. MCITP:EA, server, messaging, SQL etc. and/or MCTS, MCSE certification preferred. Bachelor degree in Computer Science or Network Engineering, professional training or equivalent experience.

POSITION INFORMATION

Company:
Word & Brown Insurance Administrators Inc

Location:
Orange, CA [illegible]

Job Status/Type:
Full Time
Employee

Job Category:
IT/Software Development

Occupations:
Database Development/Administration
General/Other: IT/Software Development

Industry:
Insurance

Work Experience:
5+ to 7 Years

Career Level:
Experienced (Non-Manager)

Education Level:
Professional

CONTACT INFORMATION

Company:
Word & Brown Insurance Administrators Inc

Reference Code:
IT Operations

Look for these:

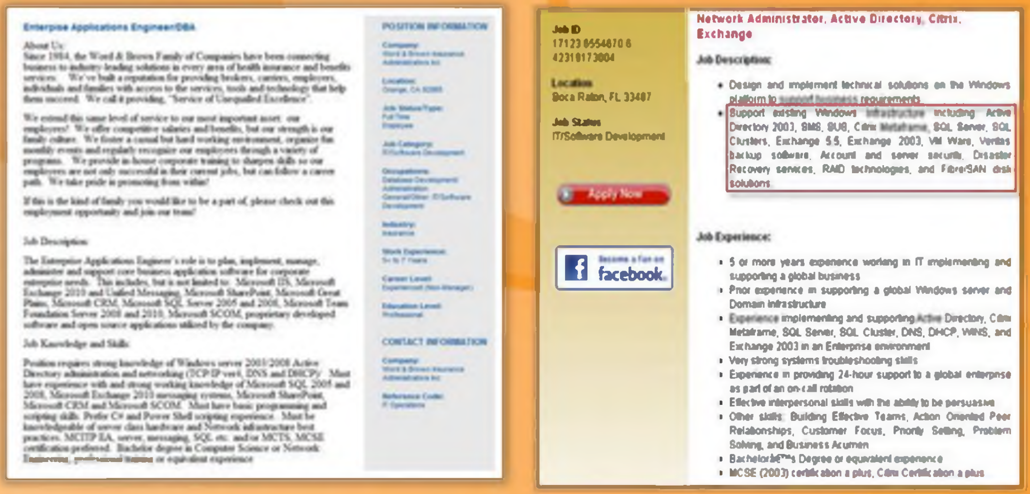
- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of Job Websites

- http://www.monster.com
- http://www.careerbuilder.com
- http://www.dice.com
- http://www.simplyhired.com
- http://www.indeed.com
- http://www.usajobs.gov

Footprinting through Job Sites

Attackers can gather valuable information about the operating system, software versions, company's infrastructure details, and database schema of an organization, through footprinting various job sites using different techniques. Depending upon the posted requirements for job openings, attackers may be able to study the hardware, network-related information, and technologies used by the company. Most of the company's websites have a key employees list with their email addresses. This information may prove to be beneficial for an attacker. For example, if a company wants to hire a person for a Network Administration job, it posts the requirements related to that position.



Enterprise Applications Engineer/DBA

About Us:
Since 1984, the Word & Brown Family of Companies have been connecting business to industry leading solutions in every area of health insurance and benefits services. We've built a reputation for providing brokers, carriers, employers, individuals and families with access to the services, tools and technology that help them succeed. We call it providing, "Service of Unequaled Excellence".

We extend this same level of service to our most important asset: our employees! We offer competitive salaries and benefits, but our strength is our family culture. We foster a casual but hard working environment, organize fun monthly events and regularly recognize our employees through a variety of programs. We provide in-house corporate training to sharpen skills so our employees are not only successful in their current jobs, but can follow a career path. We take pride in promoting from within!

If this is the kind of family you would like to be a part of, please check out this employment opportunity and join our team!

Job Description:

The Enterprise Applications Engineer's role is to plan, implement, manage, administer and support core business application software for corporate enterprise needs. This includes, but is not limited to: Microsoft IIS, Microsoft Exchange 2010 and Unified Messaging, Microsoft SharePoint, Microsoft Great Plains, Microsoft CRM, Microsoft SQL Server 2005 and 2008, Microsoft Team Foundation Server 2008 and 2010, Microsoft SCOM, proprietary developed software and open source applications utilized by the company.

Job Knowledge and Skills:

Position requires strong knowledge of Windows server 2003/2008 Active Directory administration and networking (TCP/IP ver4, DNS and DHCP). Must have experience with and strong working knowledge of Microsoft SQL 2005 and 2008, Microsoft Exchange 2010 messaging systems, Microsoft SharePoint, Microsoft CRM and Microsoft SCOM. Must have basic programming and scripting skills. Prefer C# and Power Shell scripting experience. Must be knowledgeable of server class hardware and Network infrastructure best practices. MCITP EA, server, messaging, SQL etc. and/or MCTS, MCSE certification preferred. Bachelor degree in Computer Science or Network Engineering, professional training or equivalent experience

POSITION INFORMATION

Company:
Word & Brown Insurance Administrators Inc

Location:
Orange, CA 92865

Job Status/Type:
Full Time
Employee

Job Category:
IT/Software Development

Occupations:
Database Development/Administration
General/Other: IT/Software Development

Industry:
Insurance

Work Experience:
5+ to 7 Years

Career Level:
Experienced (Non-Manager)

Education Level:
Professional

CONTACT INFORMATION

Company:
Word & Brown Insurance Administrators Inc

Reference Code:
IT Operations

Job ID
17123 0554870 6
42310173004

Location
Boca Raton, FL 33487

Job Status
IT/Software Development

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

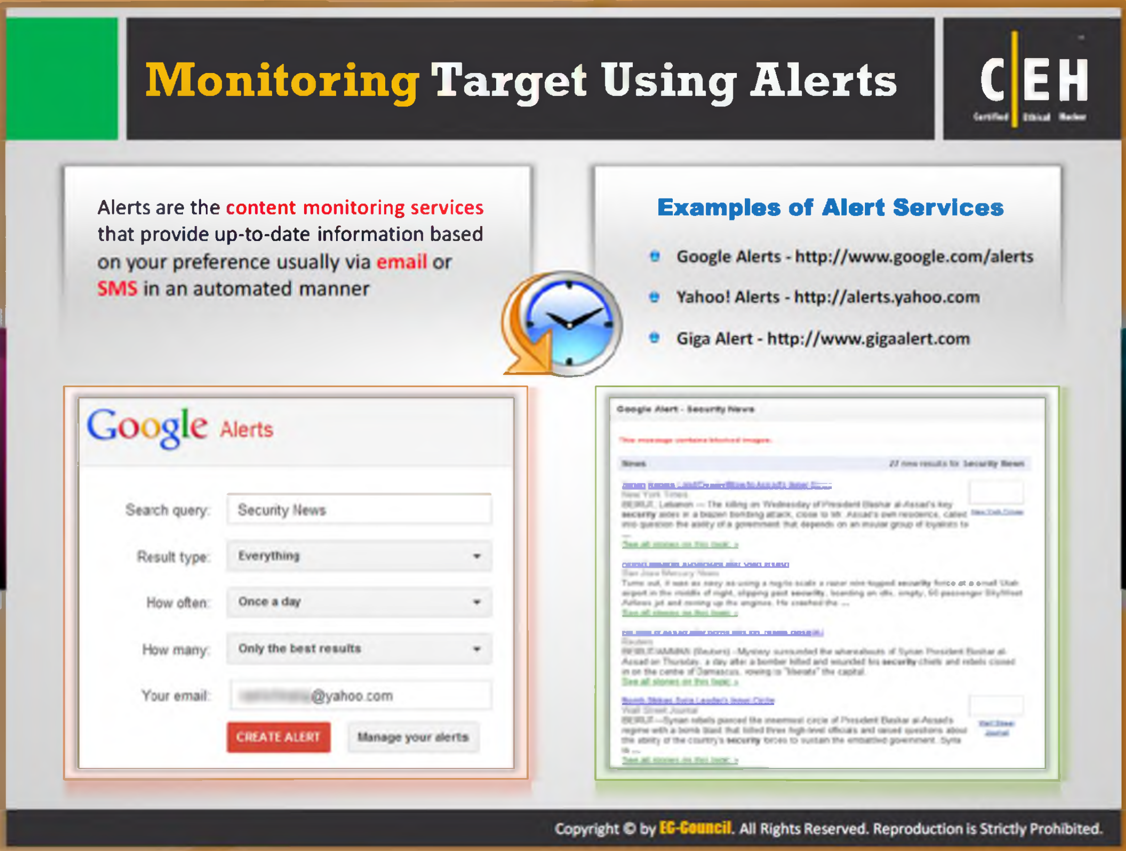
FIGURE 2.12: Gathering information through Job websites

Usually attackers look for the following information:

- Job requirements
- Employee's profile
- Hardware information
- Software information

Examples of job websites include:

- http://www.monster.com
- http://www.careerbuilder.com
- http://www.dice.com
- http://www.simplyhired.com
- http://www.indeed.com
- http://www.usajobs.gov



Monitoring Target Using Alerts

Alerts are the content monitoring services that provide up-to-date information based on your preference usually via email or SMS in an automated manner

Examples of Alert Services

- Google Alerts - http://www.google.com/alerts
- Yahoo! Alerts - http://alerts.yahoo.com
- Giga Alert - http://www.gigaalert.com

Google Alerts

Search query: Security News
Result type: Everything
How often: Once a day
How many: Only the best results
Your email: [redacted]@yahoo.com

Google Alert - Security News

This message contains blocked images.

News — 27 new results for Security News

[illegible]
New York Times
BEIRUT, Lebanon — The killing on Wednesday of President Bashar al-Assad's key security aides in a brazen bombing attack, close to Mr. Assad's own residence, called into question the ability of a government that depends on an insular group of loyalists to ...
See all stories on this topic »

[illegible]
San Jose Mercury News
Turns out, it was as easy as using a rug to scale a razor wire-topped security force at a small Utah airport in the middle of night, slipping past security, boarding an idle, empty, 50 passenger SkyWest Airlines jet and revving up the engines. He crashed the ...
See all stories on this topic »

[illegible]
Reuters
BEIRUT/AMMAN (Reuters) - Mystery surrounded the whereabouts of Syrian President Bashar al-Assad on Thursday, a day after a bomber killed and wounded his security chiefs and rebels closed in on the centre of Damascus, vowing to "liberate" the capital.
See all stories on this topic »

Bomb Strikes Syria Leader's Inner Circle
Wall Street Journal
BEIRUT—Syrian rebels pierced the innermost circle of President Bashar al-Assad's regime with a bomb blast that killed three high-level officials and raised questions about the ability of the country's security forces to sustain the embattled government. Syria is ...
See all stories on this topic »

Monitoring Targets Using Alerts

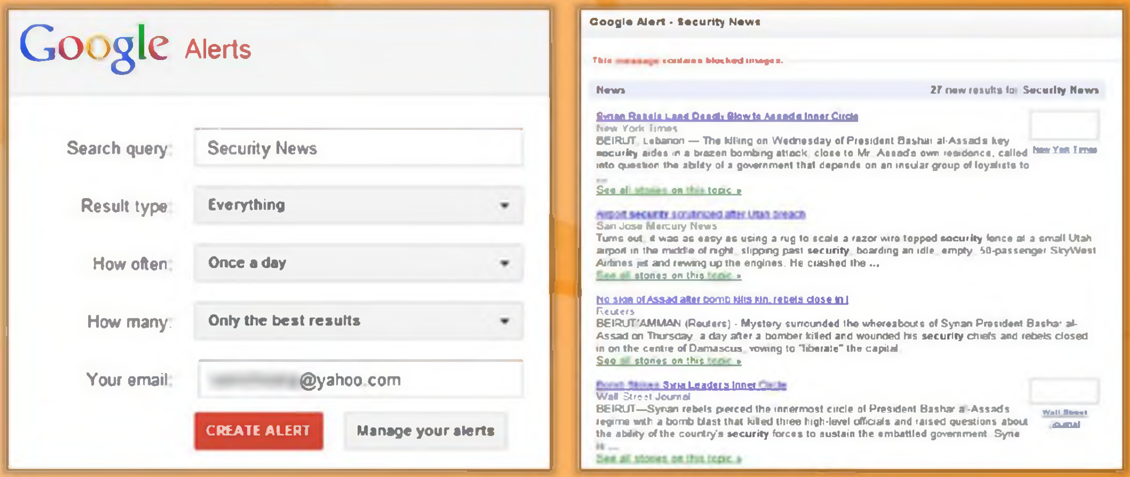
Alerts are the content monitoring services that provide automated up-to-date information based on your preference, usually via **email** or **SMS**. In order to get alerts, you need to register on the website and you should submit either an email or phone number to the service. Attackers can gather this sensitive information from the **alert services** and use it for further processing of an attack.

Google Alerts

Source: http://www.google.com/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 aids in monitoring a developing news story and keeping current on a **competitor** or **industry**.



Search query: Security News

Result type: Everything

How often: Once a day

How many: Only the best results

Your email: [redacted]@yahoo.com

Google Alert - Security News

This message contains blocked images.

News — 27 new results for Security News

Syrian Rebels Land Deadly Blow to Assad's Inner Circle
New York Times
BEIRUT, Lebanon — The killing on Wednesday of President Bashar al-Assad's key security aides in a brazen bombing attack, close to Mr. Assad's own residence, called into question the ability of a government that depends on an insular group of loyalists to ...
See all stories on this topic »

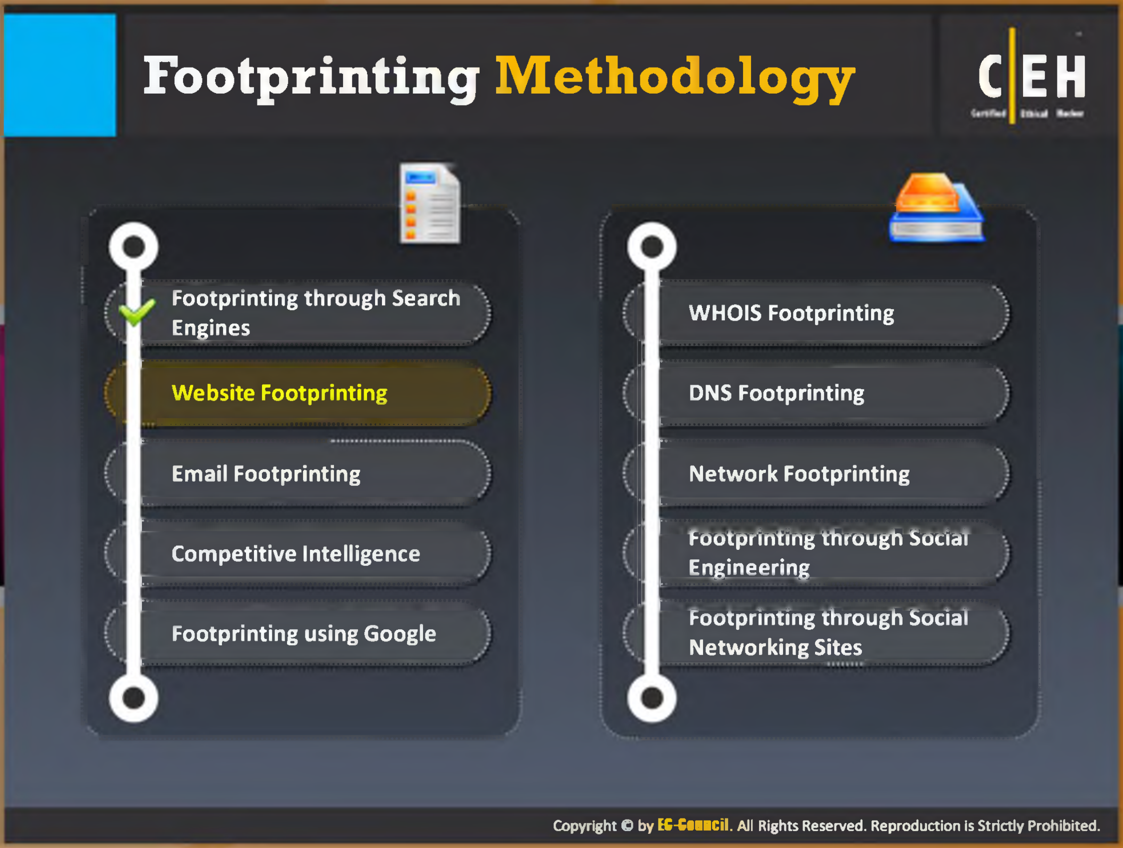
Airport security scrutinized after Utah breach
San Jose Mercury News
Turns out, it was as easy as using a rug to scale a razor wire topped security fence at a small Utah airport in the middle of night, slipping past security, boarding an idle, empty, 50-passenger SkyWest Airlines jet and rewing up the engines. He crashed the ...
See all stories on this topic »

No sign of Assad after bomb kills kin, rebels close in I
Reuters
BEIRUT/AMMAN (Reuters) - Mystery surrounded the whereabouts of Syrian President Bashar al-Assad on Thursday, a day after a bomber killed and wounded his security chiefs and rebels closed in on the centre of Damascus, vowing to "liberate" the capital.
See all stories on this topic »

Bomb Strikes Syria Leader's Inner Circle
Wall Street Journal
BEIRUT—Syrian rebels pierced the innermost circle of President Bashar al-Assad's regime with a bomb blast that killed three high-level officials and raised questions about the ability of the country's security forces to sustain the embattled government. Syria is ...
See all stories on this topic »

FIGURE 2.13: Google Alert services screenshot

Yahoo! Alerts is available at http://alerts.yahoo.com and Giga Alert is available at http://www.gigaalert.com; these are two more examples of alert services.



Footprinting Methodology

- ✓ Footprinting through Search Engines
- Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

So far, we have discussed the first step of footprinting methodology, i.e., footprinting via search engines. Now we will discuss website footprinting. An **organization's website** is a first place where you can get sensitive information such as names and contact details of chief persons in the company, upcoming project details, and so on. This section covers the website footprinting concept, mirroring websites, the tools used for mirroring, and **monitoring web updates.**

Website Footprinting

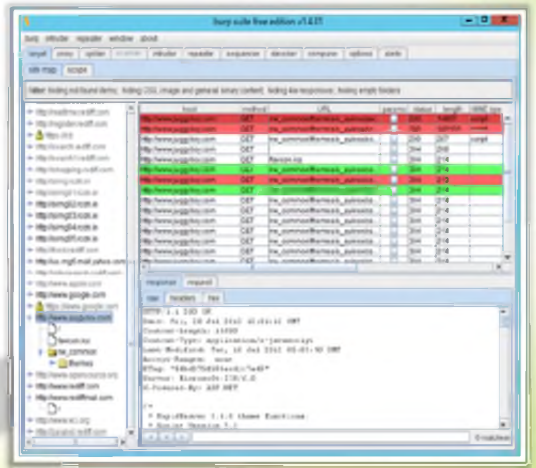
Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture

Browsing the target website may provide:

- Software used and its version
- Operating system used
- Sub-directories and parameters
- Filename, path, database field name, or query
- Scripting platform
- Contact details and CMS details

Use Zaproxy, Burp Suite, Firebug, etc. to view headers that provide:

- Connection status and content-type
- Accept-Ranges
- Last-Modified information
- X-Powered-By information
- Web server in use and its version



http://portswigger.net

Website Footprinting

It is possible for an attacker to build a detailed map of a website's structure and architecture without IDS being triggered or without raising any sys admin suspicions. It can be accomplished either with the help of sophisticated footprinting tools or just with the basic tools that come along with the operating system, such as telnet and a browser.

Using the Netcraft tool you can gather website information such as IP address, registered name and address of the domain owner, domain name, host of the site, OS details, etc. But this tool may not give all these details for every site. In such cases, you should browse the target website.

Browsing the target website will provide you with the following information:

- Software used and its version: You can find not only the software in use but also the version easily on the off-the-shelf software-based website.
- Operating system used: Usually the operating system can also be determined.
- Sub-directories and parameters: You can reveal the sub-directories and parameters by making a note of all the URLs while browsing the target website.

- Filename, path, database field name, or query: You should analyze anything after a query that looks like a filename, path, database field name, or query carefully to check whether it offers opportunities for SQL injection.
- Scripting platform: With the help of the script filename extensions such as .php, .asp, .jsp, etc. you can easily determine the scripting platform that the target website is using.
- Contact details and CMS details: The contact pages usually offer details such as names, phone numbers, email addresses, and locations of admin or support people. You can use these details to perform a social engineering attack.

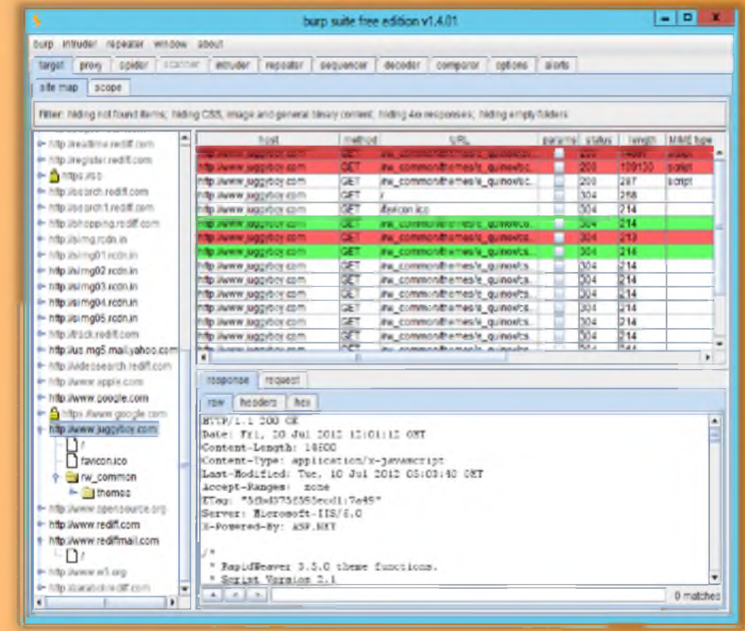
  CMS software allows URL rewriting in order to disguise the script filename extensions. In this case, you need to put little more effort to determine the scripting platform.

Use Paros Proxy, Burp Suite, Firebug, etc. to view headers that provide:

- Connection status and content-type
- Accept-ranges
- Last-Modified information
- X-Powered-By information
- Web server in use and its version

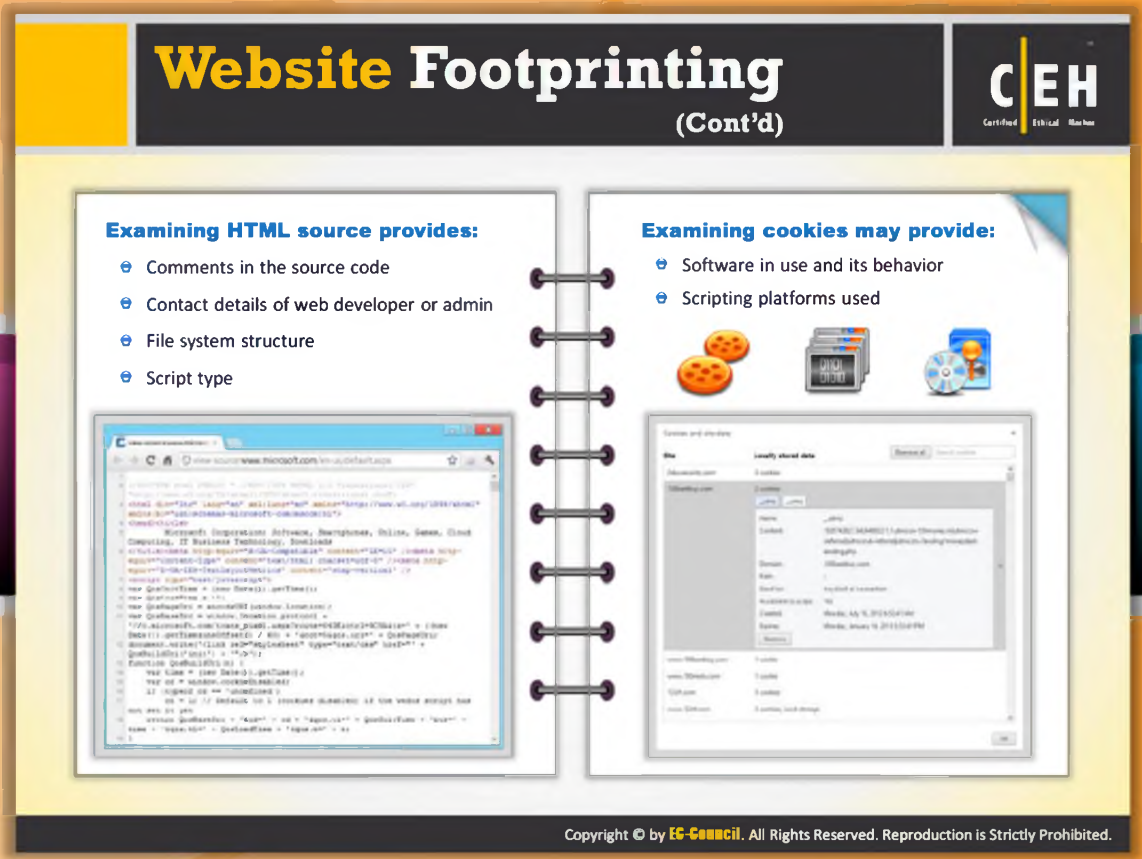
Source: http://portswigger.net

The following is a screenshot of Burp Suite showing headers of packets in the information pane:


burp suite free edition v1.4.01
burp intruder repeater window about
target proxy spider scanner intruder repeater sequencer decoder comparer options alerts
site map scope
response request
raw headers hex
0 matches

```
HTTP/1.1 200 OK
Date: Fri, 20 Jul 2012 12:01:12 GMT
Content-Length: 14800
Content-Type: application/x-javascript
Last-Modified: Tue, 10 Jul 2012 05:03:40 GMT
Accept-Ranges:  none
ETag: "5f0e4375f353ecd1:7e45"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET

/*
 * RapidWeaver 3.5.0 theme functions.
 * Script Version 2.1
```

FIGURE 2.14: Burp Suite showing headers of packets in the information pane



Website Footprinting (Cont'd)

Examining HTML source provides:

- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type

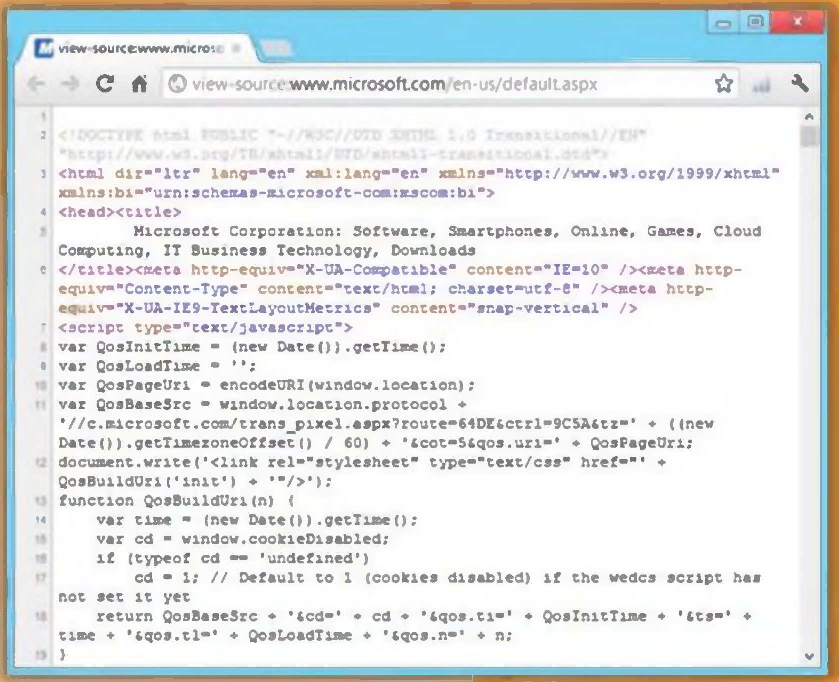
Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used

Website Footprinting (Cont'd)

Examine the HTML source code. Follow the comments that are either created by the CMS system or inserted manually. These comments may provide clues to help you understand what's running in the background. This may even provide contact details of the web admin or developer.

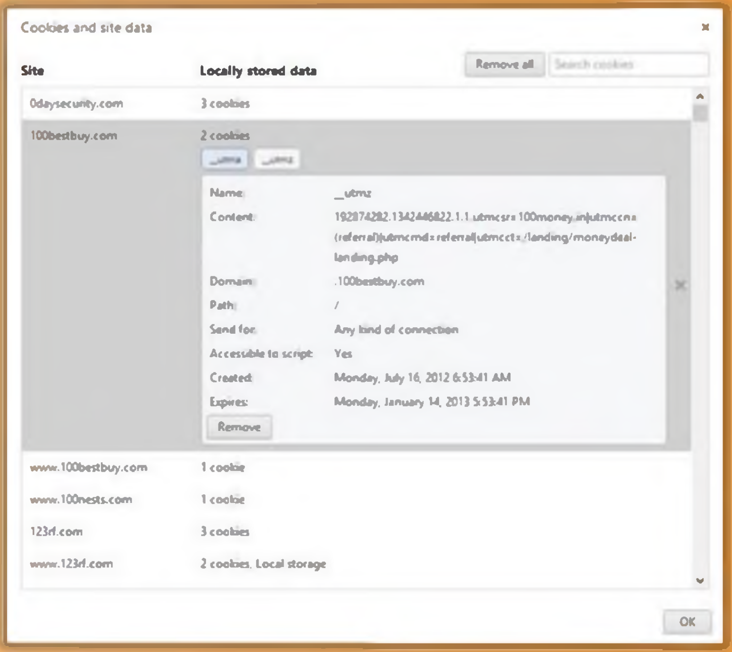
Observe all the links and image tags, in order to map the file system structure. This allows you to reveal the existence of hidden directories and files. Enter fake data to determine how the script works.



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html dir="ltr" lang="en" xml:lang="en" xmlns="http://www.w3.org/1999/xhtml"
xmlns:bi="urn:schemas-microsoft-com:mscom:bi">
<head><title>
        Microsoft Corporation: Software, Smartphones, Online, Games, Cloud
Computing, IT Business Technology, Downloads
</title><meta http-equiv="X-UA-Compatible" content="IE=10" /><meta http-
equiv="Content-Type" content="text/html; charset=utf-8" /><meta http-
equiv="X-UA-IE9-TextLayoutMetrics" content="snap-vertical" />
<script type="text/javascript">
var QosInitTime = (new Date()).getTime();
var QosLoadTime = '';
var QosPageUri = encodeURI(window.location);
var QosBaseSrc = window.location.protocol +
'//c.microsoft.com/trans_pixel.aspx?route=64DE&ctrl=9C5A&tz=' + ((new
Date()).getTimezoneOffset() / 60) + '&cot=5&qos.uri=' + QosPageUri;
document.write('<link rel="stylesheet" type="text/css" href="' +
QosBuildUri('init') + '"/>');
function QosBuildUri(n) {
    var time = (new Date()).getTime();
    var cd = window.cookieDisabled;
    if (typeof cd == 'undefined')
        cd = 1; // Default to 1 (cookies disabled) if the wedcs script has
not set it yet
    return QosBaseSrc + '&cd=' + cd + '&qos.ti=' + QosInitTime + '&ts=' +
time + '&qos.tl=' + QosLoadTime + '&qos.n=' + n;
}
```

FIGURE 2.15: Screenshot showing Microsoft script works

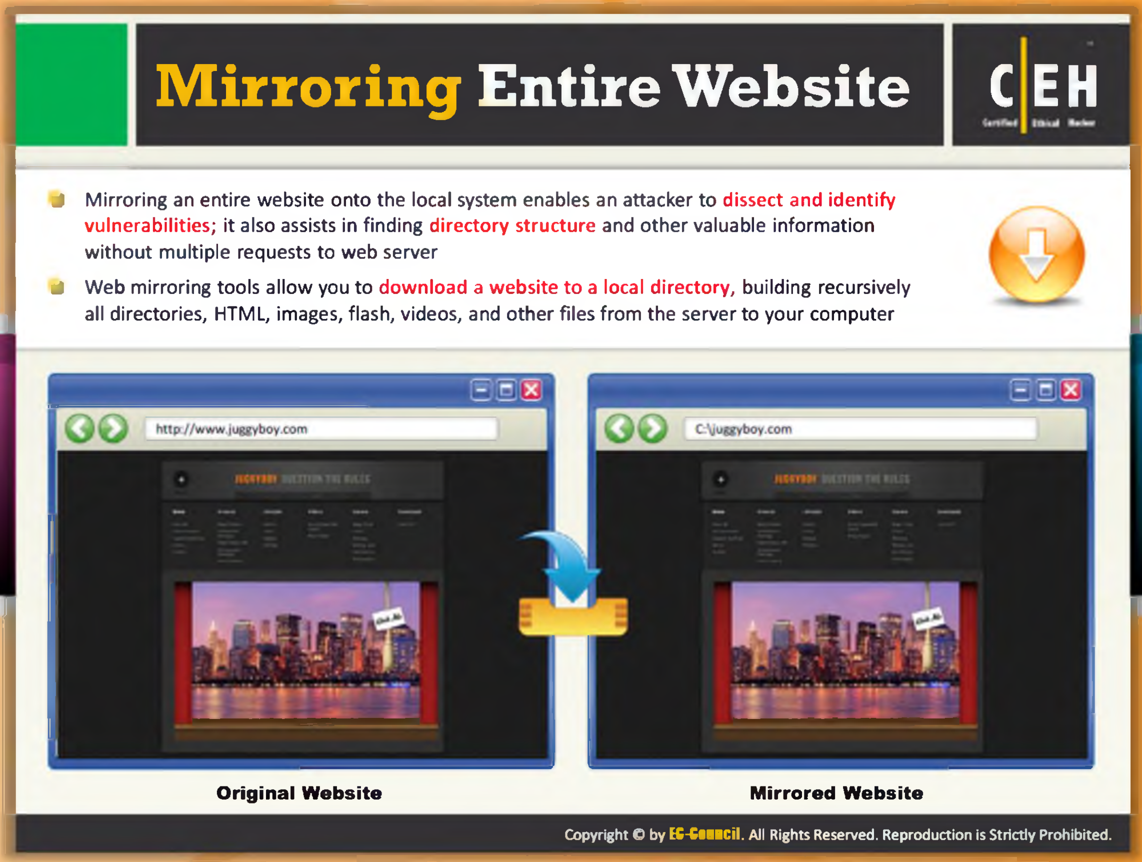
Examine cookies set by the server to determine the software running and its behavior. You can also identify the script in platforms by observing sessions and other supporting cookies.



Site	Locally stored data
0daysecurity.com	3 cookies
100bestbuy.com	2 cookies
www.100bestbuy.com	1 cookie
www.100nests.com	1 cookie
123rf.com	3 cookies
www.123rf.com	2 cookies, Local storage

Name:	__utmz
Content:	192874282.1342446822.1.1.utmcsr=100money.in|utmccn=(referral)|utmcmd=referral|utmcct=/landing/moneydeal-landing.php
Domain:	.100bestbuy.com
Path:	/
Send for:	Any kind of connection
Accessible to script:	Yes
Created:	Monday, July 16, 2012 6:53:41 AM
Expires:	Monday, January 14, 2013 5:53:41 PM

FIGURE 2.16: Showing details about the software running in a system by examining cookies



Mirroring Entire Website

- Mirroring an entire website onto the local system enables an attacker to dissect and identify vulnerabilities; it also assists in finding directory structure and other valuable information without multiple requests to web server
- Web mirroring tools allow 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

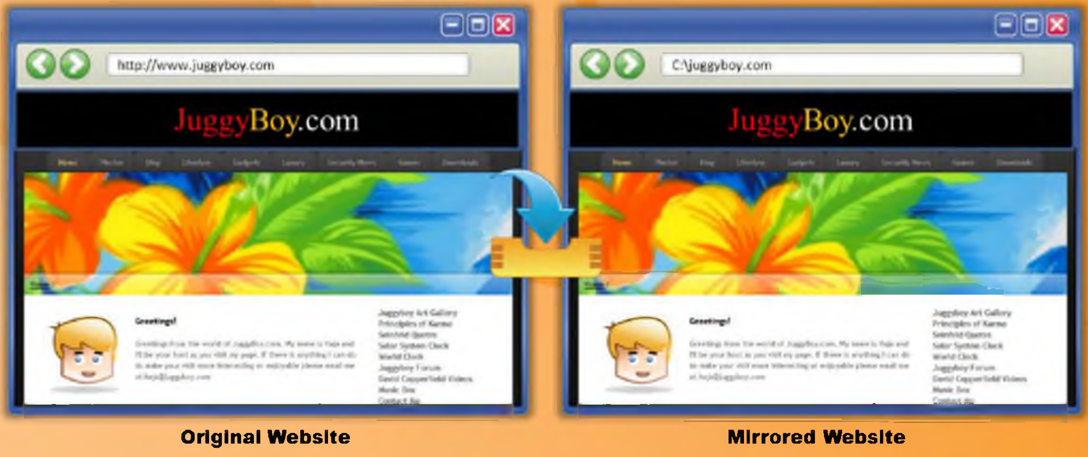
Mirrored Website

Mirroring an Entire Website

Website mirroring is the process of creating an exact replica of the original website. This can be done with the help of web mirroring tools. These tools allow you to download a website to a local directory, recursively building all **directories, HTML, images, flash, videos** and other files from the server to your computer.

Website mirroring has the following benefits:

- It is helpful for offline site browsing.
- Website mirroring helps in creating a backup site for the original one.
- A website clone can be created.
- Website mirroring is useful to test the site at the time of website design and development.
- It is possible to distribute to **multiple servers** instead of using only one server.



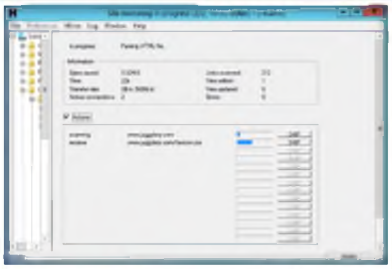
Original Website

Mirrored Website

FIGURE 2.17: JuggyBoy's Original and Mirrored website

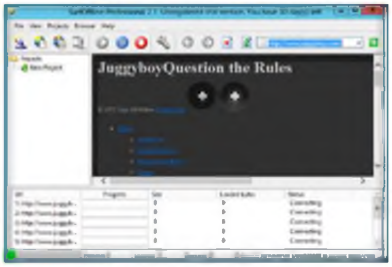
Website Mirroring Tools

CEH Certified Ethical Hacker

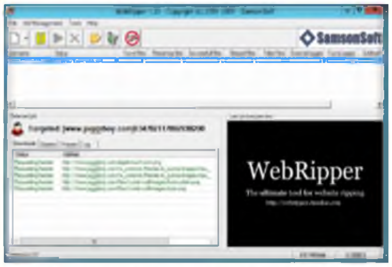


HTTrack Web Site Copier (http://www.httrack.com)

BlackWidow (http://softbytelabs.com)



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



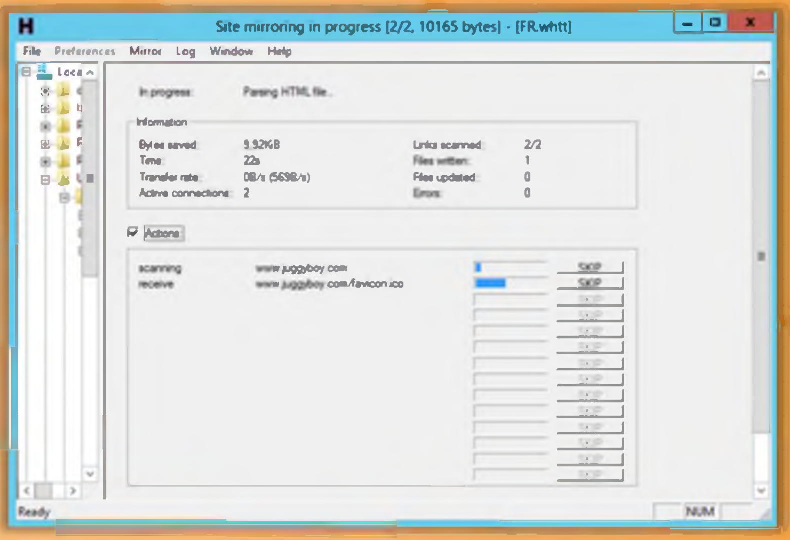
WebRipper (http://www.calluna-software.com)

Website Mirroring Tools

HTTrack Web Site Copier

Source: http://www.httrack.com

HTTrack is an offline browser utility. It allows you to download a World Wide Web site from the Internet to a **local directory**, building recursively all directories, getting HTML, images, and other files from the server to your computer. HTTrack arranges the original **site's relative link-structure**. Open a page of the "mirrored" website in your browser, browse the site from link to link, and you can view the site as if you were online. HTTrack can also update an existing mirrored site, and resume interrupted downloads.


Site mirroring in progress [2/2, 10165 bytes] - [FR.whtt]
File Preferences Mirror Log Window Help
Loca
Actions
SKIP
Ready
NUM

In progress: Parsing HTML file...

Information

Bytes saved:	9.92KB	Links scanned:	2/2
Time:	22s	Files written:	1
Transfer rate:	0B/s (569B/s)	Files updated:	0
Active connections:	2	Errors:	0

```
scanning    www.juggyboy.com
receive     www.juggyboy.com/favicon.ico
```

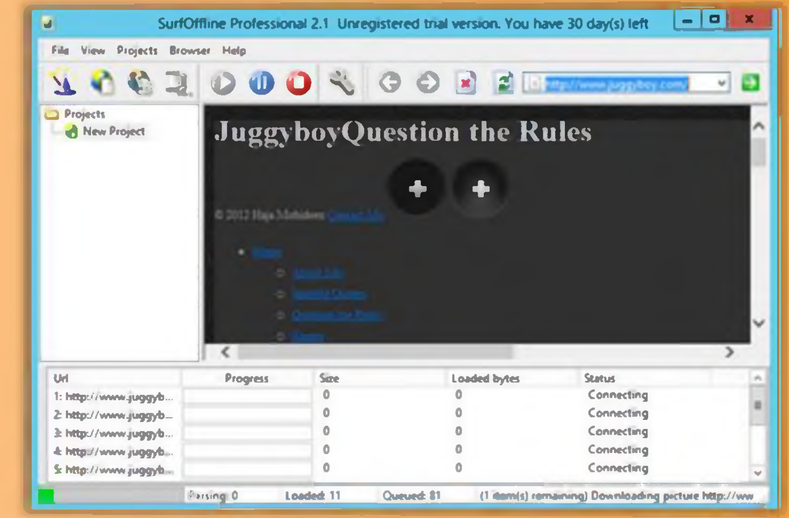
FIGURE 2.18: HTTrack Web Site Copier Screenshot

SurfOffline

Source: http://www.surfoffline.com

SurfOffline is a website download software. The software allows you to download entire websites and download web pages to your local hard drive. After downloading the target website, you can use SurfOffline as an offline browser and view downloaded web pages in it. If you prefer to view downloaded webpages in another browser, you can use the Export Wizard.

SurfOffline's Export Wizard also allows you to copy downloaded websites to other computers in order to view them later and prepares websites for burning them to a CD or DVD.


SurfOffline Professional 2.1 Unregistered trial version. You have 30 day(s) left
File View Projects Browser Help
http://www.juggyboy.com/
Projects
New Project
JuggyboyQuestion the Rules

Url	Progress	Size	Loaded bytes	Status
1: http://www.juggyb...		0	0	Connecting
2: http://www.juggyb...		0	0	Connecting
3: http://www.juggyb...		0	0	Connecting
4: http://www.juggyb...		0	0	Connecting
5: http://www.juggyb...		0	0	Connecting

Parsing: 0 Loaded: 11 Queued: 81 (1 item(s) remaining) Downloading picture http://ww

FIGURE 2.19: SurfOffline screenshot

BlackWidow

Source: http://softbytelabs.com

BlackWidow is a website scanner for both experts and beginners. It scans websites (it's a site ripper). It can download an entire website or part of a website. It will build a site structure first, and then downloads. It allows you to choose what to download from the website.

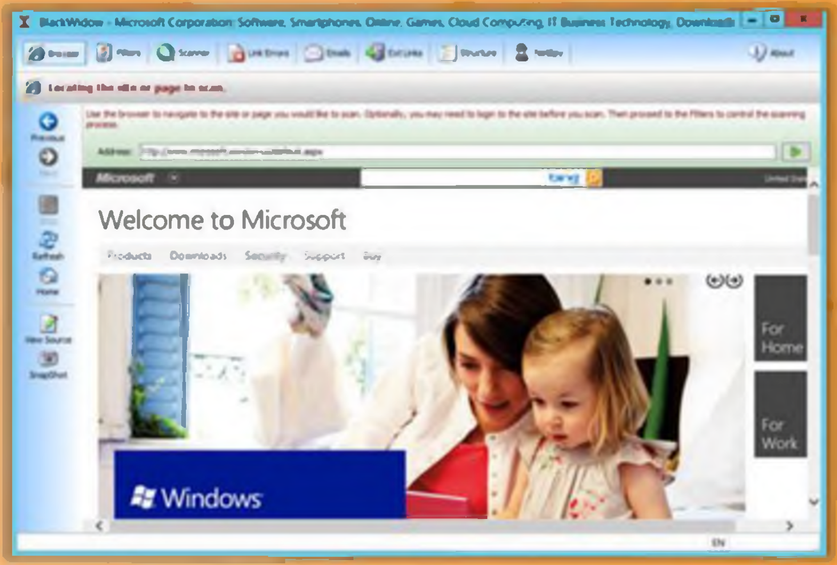


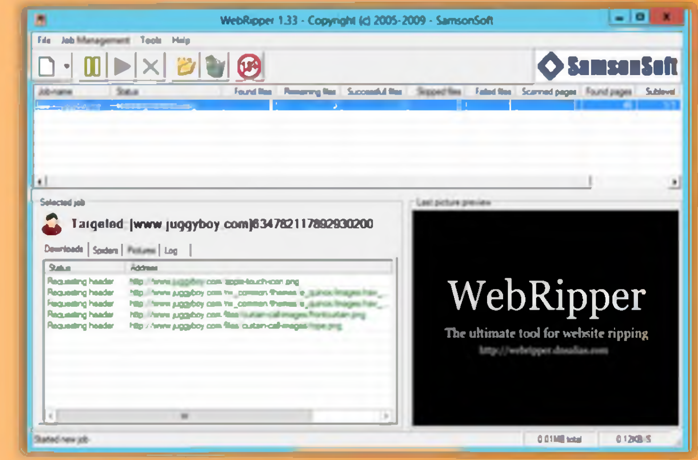
FIGURE 2.20: SurfOffline screenshot

Webripper

Source: http://www.calluna-software.com

WebRipper is an Internet scanner and downloader. It downloads massive amount of images, videos, audio, and executable documents from any website. WebRipper uses **spider-technology** to follow the links in all directions from the start-address. It filters out the interesting files, and adds them to the download-queue for downloading.

You can restrict downloaded items by file type, minimum file, maximum file, and image size. All the downloaded links can also be restricted by keywords to avoid wasting your **bandwidth**.



Targeted [www.juggyboy.com]634782117892930200

Status	Address
Requesting header	http://www.juggyboy.com/apple-touch-icon.png
Requesting header	http://www.juggyboy.com/_common/themes/...
Requesting header	http://www.juggyboy.com/_common/themes/...
Requesting header	http://www.juggyboy.com/files/custom-call-images/...
Requesting header	http://www.juggyboy.com/files/custom-call-images/...

FIGURE 2.21: Webripper screenshot

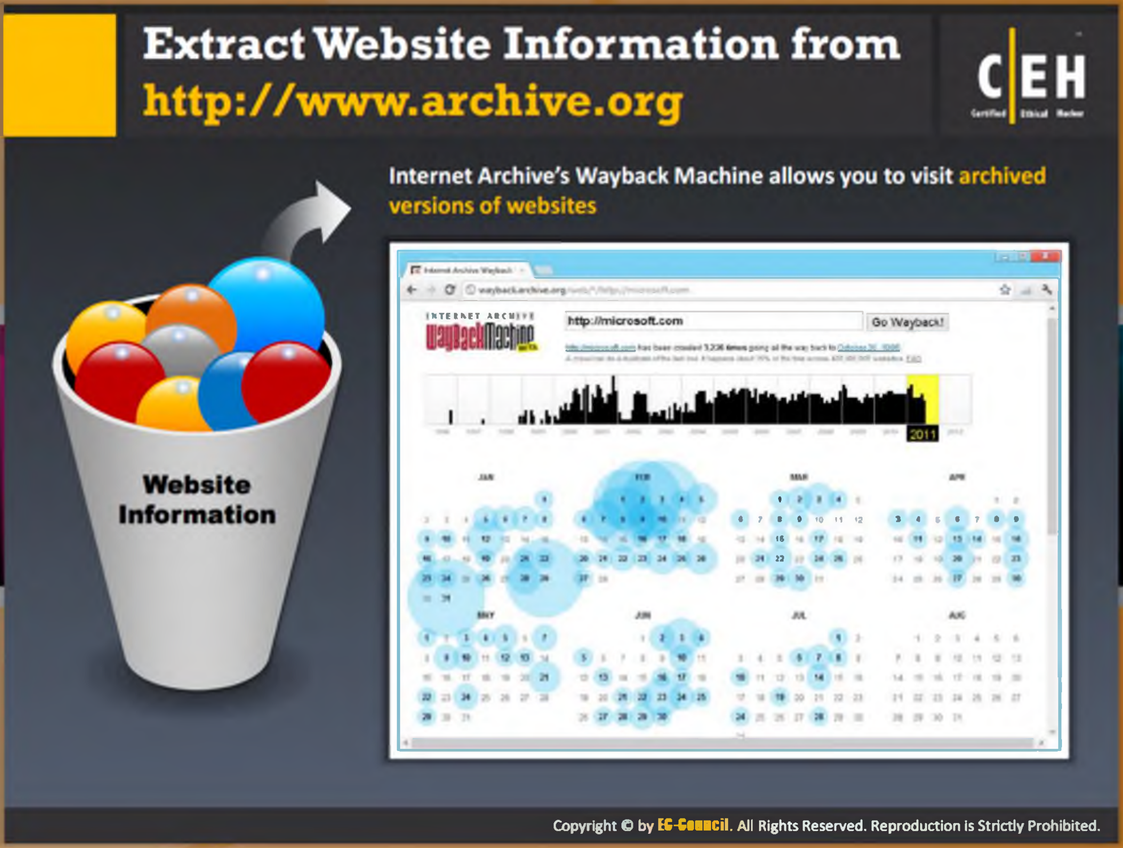
Website Mirroring Tools (Cont'd)

Website Ripper Copier http://www.tensons.com	PageNest http://www.pagenest.com
Teleport Pro http://www.tenmax.com	Backstreet Browser http://www.spadixbd.com
Portable Offline Browser http://www.metaproducts.com	Offline Explorer Enterprise http://www.metaproducts.com
Proxy Offline Browser http://www.proxy-offline-browser.com	GNU Wget http://www.gnu.org
iMiser http://internetresearchtool.com	Hooeey Webprint http://www.hooeeywebprint.com

Website Mirroring Tools (Cont'd)

In addition to the website mirroring tools mentioned previously, a few more well-known tools are mentioned as follows:

- Webiste Ripper Copier available at http://www.tensons.com
- Teleport Pro available at http://www.tenmax.com
- Portable Offline Browser available at http://www.metaproducts.com
- Proxy Offline Browser available at http://www.proxy-offline-browser.com
- iMiser available at http://internetresearchtool.com
- PageNest available at http://www.pagenest.com
- Backstreet Browser available at http://www.spadixbd.com
- Offline Explorer Enterprise available at http://www.metaproducts.com
- GNU Wget available at http://www.gnu.org
- Hooeey Webprint available at http://www.hooeeywebprint.com

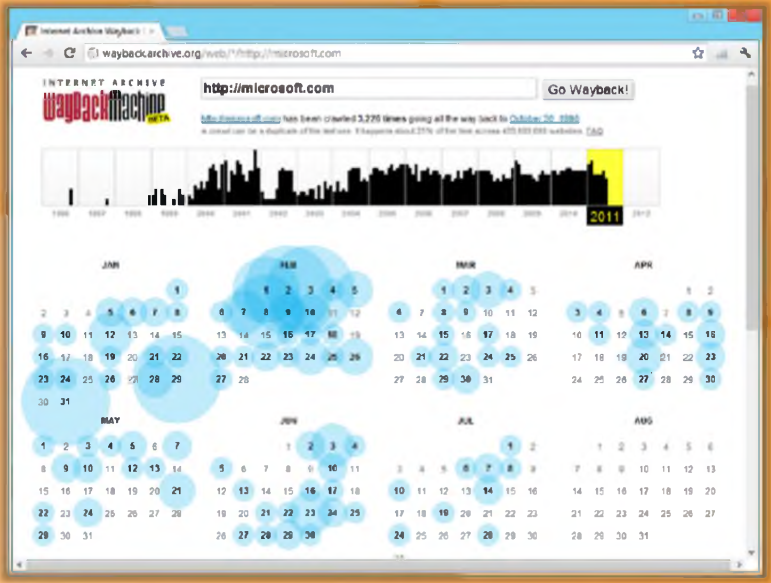


Extract Website Information from http://www.archive.org

Internet Archive's Wayback Machine allows you to visit archived versions of websites

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

Archive is an Internet Archive Wayback Machine that allows you to visit archived versions of websites. This allows you to gather information on a company's web pages since their creation. As the website www.archive.org keeps track of web pages from the time of their inception, you can retrieve even information that has been removed from the target website.

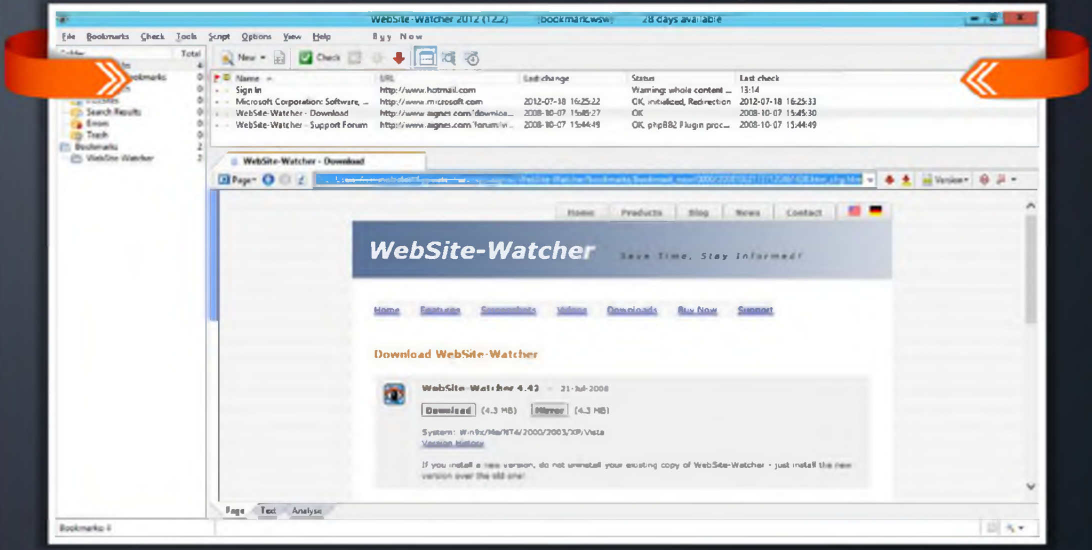


http://microsoft.com has been crawled 3,220 times going all the way back to October 30, 1996

FIGURE 2.22: Internet Archive Wayback Machine screenshot

Monitoring Web Updates Using Website Watcher

Website Watcher **automatically checks web pages** for updates and changes


WebSite-Watcher 2012 (12.2) [bookmark.wsw] 28 days available
File Bookmarks Check Tools Script Options View Help Buy Now
New Check
Total
Search Results
Errors
Trash
Bookmarks
WebSite-Watcher
WebSite-Watcher - Download
Page
Version
Home Products Blog News Contact
WebSite-Watcher Save Time, Stay Informed!
Home Features Screenshots Videos Downloads Buy Now Support
Download WebSite-Watcher
WebSite-Watcher 4.42 21-Jul-2008
Download (4.3 MB) Mirror (4.3 MB)
Page Text Analyse
Bookmarks 4

Name	URL	Last change	Status	Last check
Sign In	http://www.hotmail.com		Warning: whole content ...	13:14
Microsoft Corporation: Software, ...	http://www.microsoft.com	2012-07-18 16:25:22	OK, initialized, Redirection	2012-07-18 16:25:33
WebSite-Watcher - Download	http://www.aignes.com/downloa...	2008-10-07 15:48:27	OK	2008-10-07 15:45:30
WebSite-Watcher - Support Forum	http://www.aignes.com/forum/vi...	2008-10-07 15:44:49	OK, phpBB2 Plugin proc...	2008-10-07 15:44:49

System: Win9x/Me/NT4/2000/2003/XP/Vista
Version History

If you install a new version, do not uninstall your existing copy of WebSite-Watcher - just install the new version over the old one!

http://aignes.com

Monitoring Web Updates Using Website Watcher

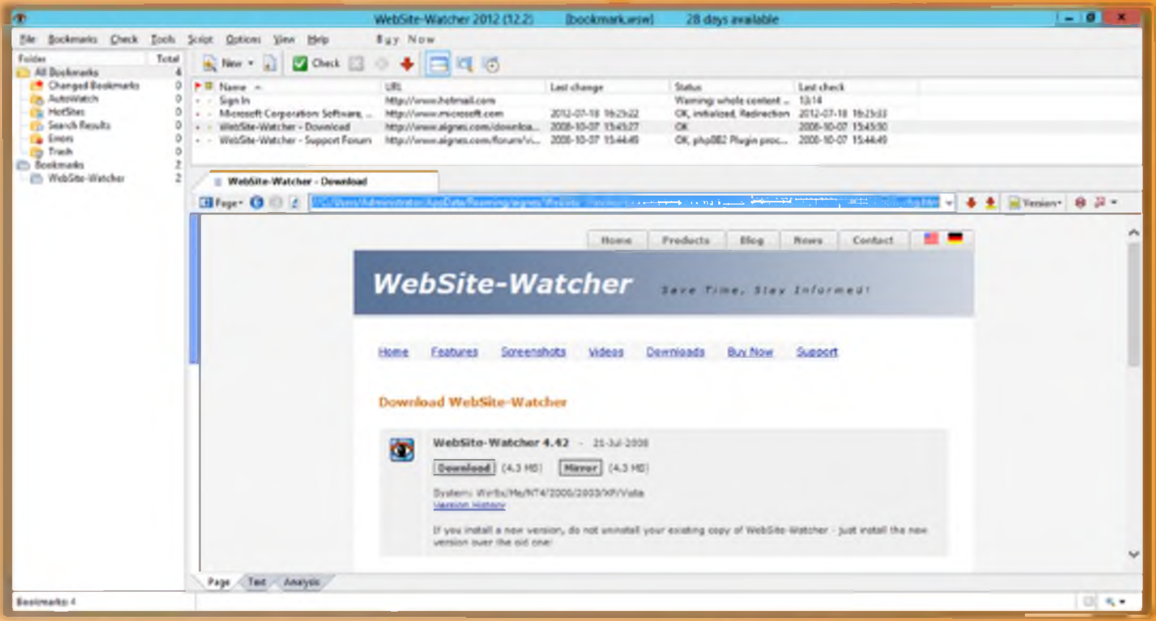
Source: http://www.aignes.com

Website Watcher is used to keep track of websites for updates and automatic changes. When an update or change occurs, Website Watcher automatically detects and saves the last two versions onto your disk, and highlights changes in the text. It is a useful tool for monitoring sites to gain **competitive advantage**.

Benefits:

Frequent manual checking of updates is not required. Website Watcher can automatically detect and notify users of updates:

- It allows you to know what your competitors are doing by scanning your competitors' websites
- The site can keep track of new software versions or driver updates
- It stores images of the modified websites to a **disk**


WebSite-Watcher 2012 (12.2) [bookmark.wsw] 28 days available
File Bookmarks Check Tools Script Options View Help Buy Now
New Check
Folder Total
All Bookmarks 4
Changed Bookmarks 0
AutoWatch 0
HotSites 0
Search Results 0
Errors 0
Trash 0
Bookmarks 2
WebSite-Watcher 2
WebSite-Watcher - Download
Page
Version
Home Products Blog News Contact
WebSite-Watcher
Save Time, Stay Informed!
Home Features Screenshots Videos Downloads Buy Now Support
Download
Mirror
Page Text Analysis
Bookmarks: 4

Name	URL	Last change	Status	Last check
Sign In	http://www.hotmail.com		Warning: whole content ...	13:14
Microsoft Corporation: Software, ...	http://www.microsoft.com	2012-07-18 16:23:22	OK, initialized, Redirection	2012-07-18 16:23:33
WebSite-Watcher - Download	http://www.aignes.com/downloa...	2008-10-07 15:45:27	OK	2008-10-07 15:45:30
WebSite-Watcher - Support Forum	http://www.aignes.com/forum/vi...	2008-10-07 15:44:45	OK, phpBB2 Plugin proc...	2008-10-07 15:44:49

Download WebSite-Watcher

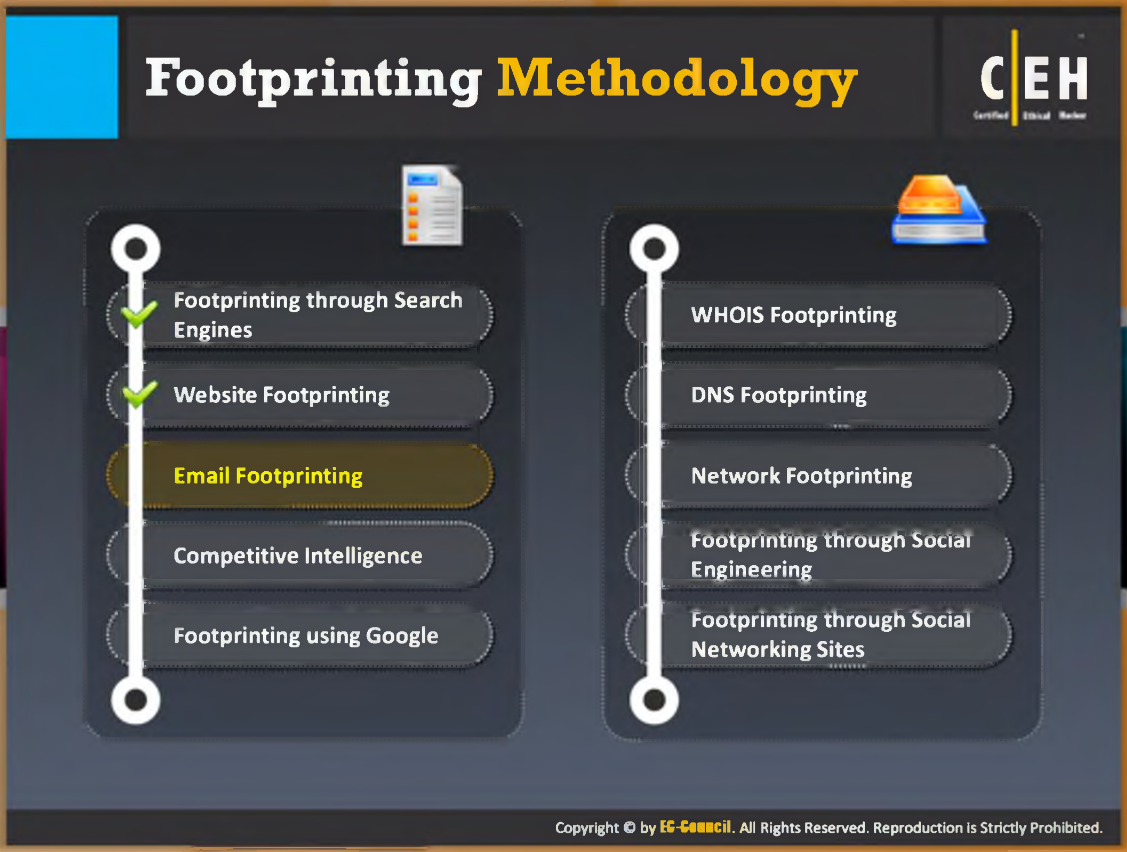
WebSite-Watcher 4.42 - 21-Jul-2008

Download (4.3 MB) Mirror (4.3 MB)

System: Win9x/Me/NT4/2000/2003/XP/Vista
Version History

If you install a new version, do not uninstall your existing copy of WebSite-Watcher - just install the new version over the old one!

FIGURE 2.23: Website watcher monitoring web updates



Footprinting Methodology

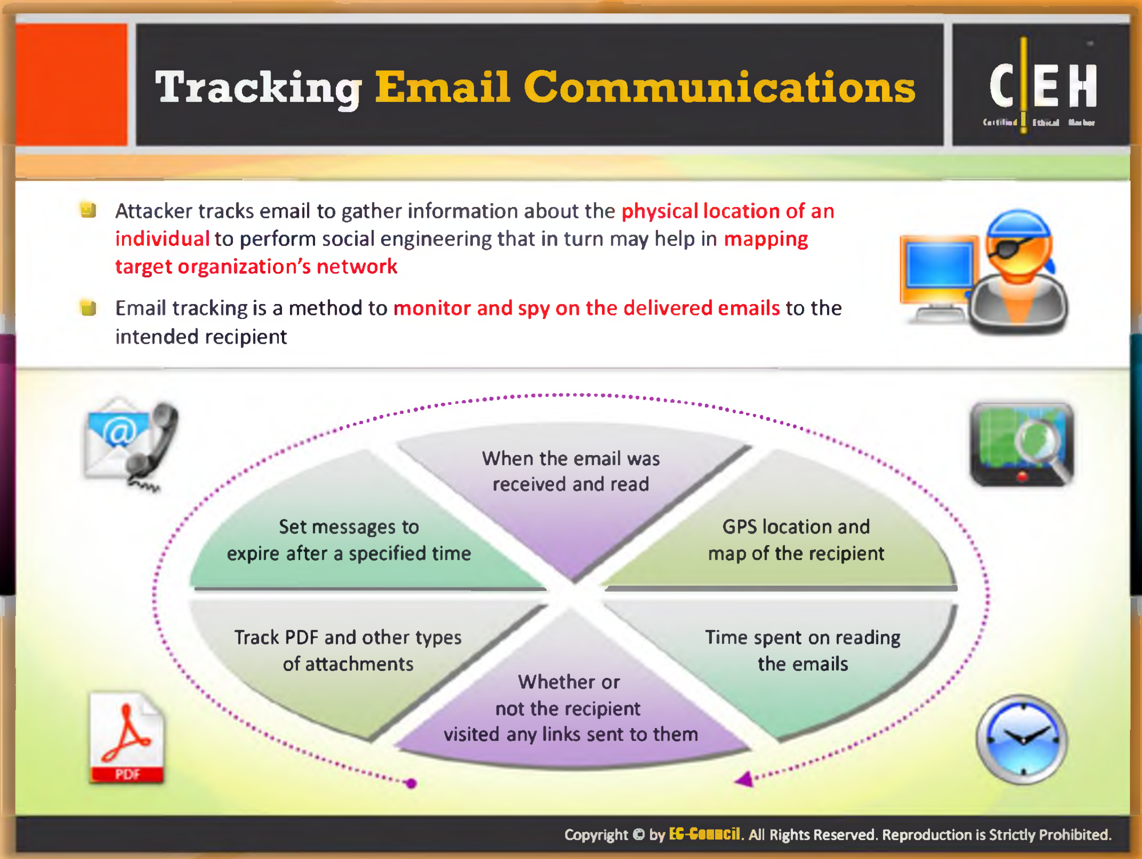
- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- Email Footprinting
- Competitive Intelligence
- Footprinting using Google
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

So far we have discussed Footprinting through search engines and website footprinting, the two initial phases of footprinting methodology. Now we will discuss email footprinting.

Footprinting through Search Engines
Website Footprinting
Email Footprinting
Competitive Intelligence
Footprinting using Google
WHOIS Footprinting
DNS Footprinting
Network Footprinting
Footprinting through Social Engineering
Footprinting through Social Networking Sites

This section describes how to track email communications, how to collect information from email headers, and email tracking tools.



Tracking Email Communications

CEH
Certified Ethical Hacker

- Attacker tracks email to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping target organization's network
- Email tracking is a method to monitor and spy on the delivered emails to the intended recipient

When the email was received and read

GPS location and map of the recipient

Time spent on reading the emails

Whether or not the recipient visited any links sent to them

Track PDF and other types of attachments

Set messages to expire after a specified time

Tracking Email Communications

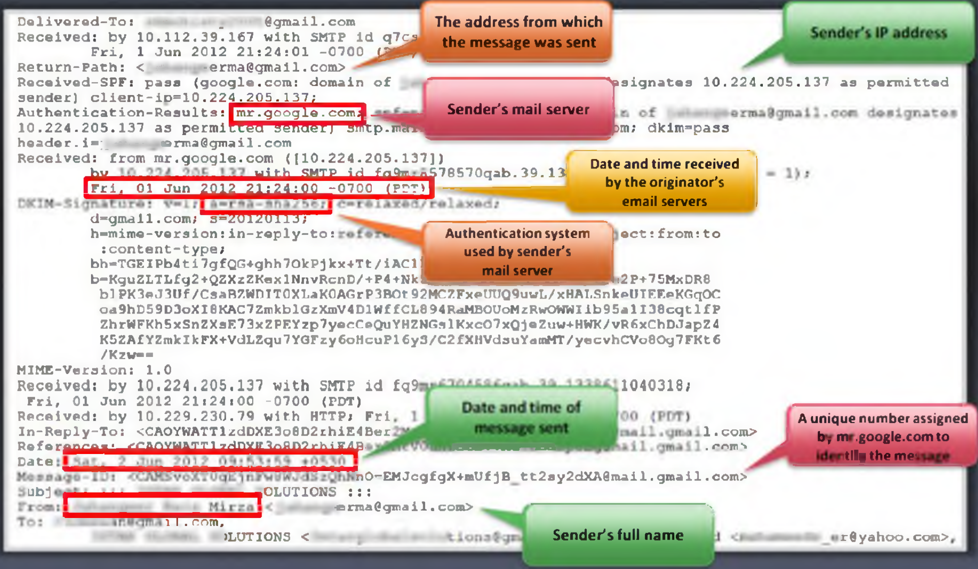
Email tracking is a method that helps you to monitor as well as to track the emails of a particular user. This kind of tracking is possible through digitally time stamped records to reveal the time and date a particular email was received or opened by the target. A lot of email tracking tools are readily available in the market, using which you can collect information such as IP addresses, mail servers, and service provider from which the mail was sent. Attackers can use this information to build the hacking strategy. Examples of email tracking tools include: eMailTrackerPro and Paraben E-mail Examiner.

By using email tracking tools you can gather the following information about the victim:

- **Geolocation:** Estimates and displays the location of the recipient on the map and may even calculate distance from your location.
- **Read duration:** The duration of time spent by the recipient on reading the mail sent by the sender.
- **Proxy detection:** Provides information about the type of server used by the recipient.
- **Links:** Allows you to check whether the links sent to the recipient through email have been checked or not.

- **Operating system:** This reveals information about the type of operating system used by the recipient. The attacker can use this information to launch an attack by finding loopholes in that particular operating system.
- **Forward email:** Whether or not the email sent to you is forwarded to another person can be determined easily by using this tool.

Collecting Information from Email Header



```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7cs
        Fri, 1 Jun 2012 21:24:01 -0700 (
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]          esignates 10.224.205.137 as permitted
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=                  n of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.mai                 om; dkim=pass
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
        by 10.224.205.137 with SMTP id fq9mr6578570qab.39.13                    = 1);
        Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:in-reply-to:refere                    ect:from:to
         :content-type;
        bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1
        b=KguZLTLfg2+QZXzZKex1NnvRcnD/+P4+Nk                 2P+75MxDR8
         blPK3eJ3Uf/CsaBZWDITOXLaKOAGrP3BOt92MCZFxeUUQ9uwL/xHALSnkeUIEEeKGqOC
         oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqtlfP
         ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNGslKxcO7xQjeZuw+HWK/vR6xChDJapZ4
         K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuPl6y3/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
         /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9mr6704586qab.39.1338611040318;
 Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Fri, 1                 00 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber2                   mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4Be                      mail.gmail.com>
Date: Sat, 2 Jun 2012 09:53:59 +0530
Message-ID: <CAMSvoXTUqEjnFW8WJdSzQhNnO-EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ::: [redacted] OLUTIONS :::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]n@gmail.com,
        [redacted] OLUTIONS <[redacted]tions@gm                  <[redacted]_er@yahoo.com>,
```

The address from which the message was sent

Sender's IP address

Sender's mail server

Date and time received by the originator's email servers

Authentication system used by sender's mail server

Date and time of message sent

A unique number assigned by mr.google.com to identify the message

Sender's full name

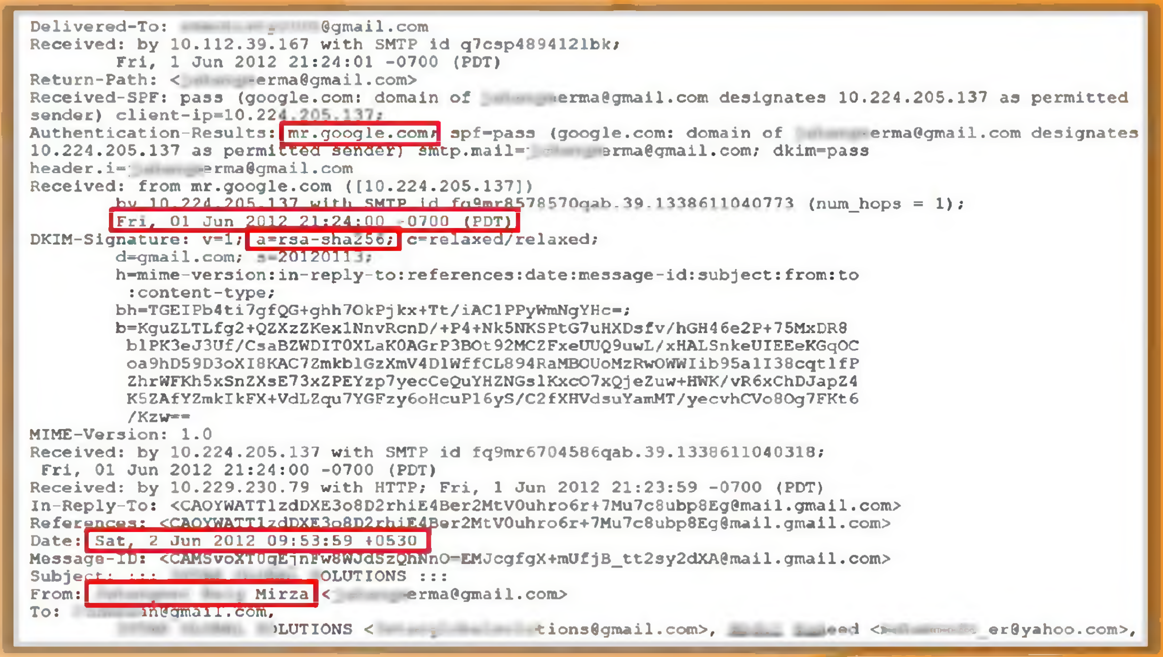
Collecting Information from Email Headers

An email header is the information that travels with every email. It contains the details of the sender, routing information, date, subject, and recipient. The process of viewing the email header varies with different mail programs.

Commonly used email programs:

- SmarterMail Webmail
- Outlook Express 4-6
- Outlook 2000-2003
- Outlook 2007
- Eudora 4.3/5.0
- Entourage
- Netscape Messenger 4.7
- MacMail

The following is a screenshot of a sample email header.



```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7csp489412lbk;
        Fri, 1 Jun 2012 21:24:01 -0700 (PDT)
Return-Path: <[redacted]erma@gmail.com>
Received-SPF: pass (google.com: domain of [redacted]erma@gmail.com designates 10.224.205.137 as permitted
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=pass (google.com: domain of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.mail=[redacted]erma@gmail.com; dkim=pass
header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
        by 10.224.205.137 with SMTP id fq9mr8578570qab.39.1338611040773 (num_hops = 1);
        Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20120113;
        h=mime-version:in-reply-to:references:date:message-id:subject:from:to
         :content-type;
        bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1PPyWmNgYHc=;
        b=KguZLTLfg2+QZXzZKex1NnvRcnD/+P4+Nk5NKSPtG7uHXDsfv/hGH46e2P+75MxDR8
         b1PK3eJ3Uf/CsaBZWDIT0XLaK0AGrP3BOt92MCZFxeUUQ9uwL/xHALSnkeUIEEeKGqOC
         oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqt1fP
         ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNGs1KxcO7xQjeZuw+HWK/vR6xChDJapZ4
         K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuP16yS/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
         /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9mr6704586qab.39.1338611040318;
 Fri, 01 Jun 2012 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Fri, 1 Jun 2012 21:23:59 -0700 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber2MtV0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4Ber2MtV0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
Date: Sat, 2 Jun 2012 09:53:59 +0530
Message-ID: <CAMSvoXT0qEjnFw8WJdSzQhNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ::: [redacted]OLUTIONS :::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]in@gmail.com,
        [redacted]LUTIONS <[redacted]tions@gmail.com>, [redacted]eed <[redacted]er@yahoo.com>,
```

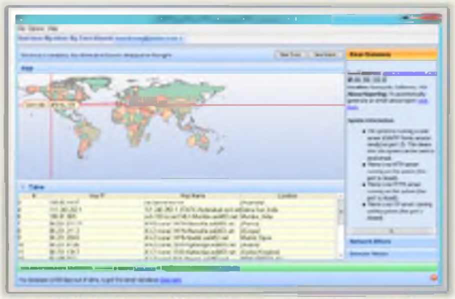
FIGURE 2.24: Email header screenshot

This email header contains the following information:

- Sender's mail server
- Data and time received by the originator's email servers
- Authentication system used by sender's mail server
- Data and time of message sent
- A unique number assigned by mr.google.com to identify the message
- Sender's full name
- Senders IP address
- The address from which the message was sent

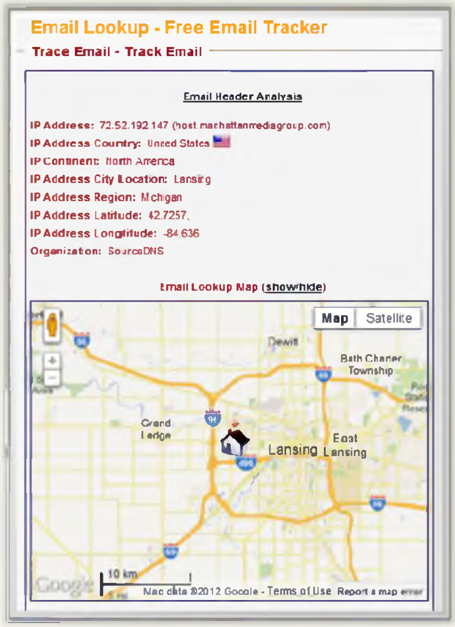
The attacker can trace and collect all of this information by performing a detailed analysis of the complete email header.

Email Tracking Tools



eMailTrackerPro (*http://www.emailtrackerpro.com*)

PoliteMail (*http://www.politemail.com*)



Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

IP Address: 72.52.192.147 (host.manhattanmediagroup.com)
IP Address Country: United States
IP Continent: North America
IP Address City Location: Lansing
IP Address Region: Michigan
IP Address Latitude: 42.7257,
IP Address Longtitude: -84.636
Organization: SourceDNS

Email Lookup Map (show/hide)

Email Lookup – Free Email Tracker (*http://www.ipaddresslocation.org*)

Email Tracking Tools

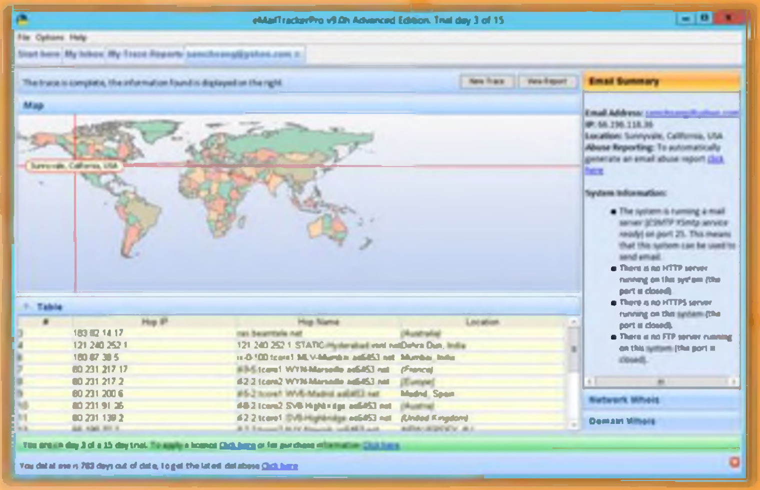
Email tracking tools allow you to track an email and extract information such as **sender identity, mail server, sender's IP address**, etc. You can use the extracted information to attack the target organization's systems by sending malicious emails. Numerous email tracking tools are readily available in the market.

The following are a few commonly used email tracking tools:

eMailTrackerPro

Source: http://www.emailtrackerpro.com

eMailTrackerPro is an email tracking tool that analyzes email headers and reveals information such as sender's geographical location, IP address, etc. It allows you to review the traces later by saving all past traces.


eMailTrackerPro v9.0h Advanced Edition. Trial day 3 of 15
File Options Help
Start here My Inbox My Trace Reports
New Trace
View Report
Map
Sunnyvale, California, USA
Table
Email Summary
Network Whois
Domain Whois

The trace is complete, the information found is displayed on the right

#	Hop IP	Hop Name	Location
3	183 82 14 17	ras bearnsle net	(Australia)
4	121 240 252 1	121 240 252 1 STATIC-Hyderabad vsnl net	Dehra Dun, India
6	180 87 38 5	[illegible]	Mumbai, India
7	80 231 217 17	[illegible]	(France)
8	80 231 217 2	[illegible]	(Europe)
9	80 231 200 6	[illegible]	Madrid, Spain
10	80 231 91 26	[illegible]	(Austria)
11	80 231 139 2	[illegible]	(United Kingdom)

Email Address: [illegible]
IP: 66.196.118.36
Location: Sunnyvale, California, USA
Abuse Reporting: To automatically generate an email abuse report click here

System Information:

- The system is running a mail server (ESMTP YSmtp service ready) on port 25. This means that this system can be used to send email.
- There is no HTTP server running on this system (the port is closed).
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

You are on day 3 of a 15 day trial. To apply a licence Click here or for purchase information Click here

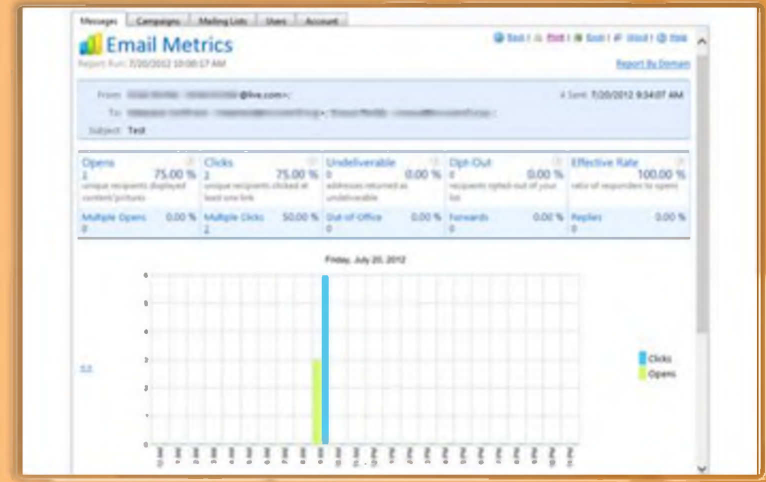
You data at one is 783 days out of date, to get the latest database Click here

FIGURE 2.25: eMailTrackerPro showing geographical location of sender

PoliteMail

Source: http://www.politemail.com

PoliteMail is an email tracking tool for Outlook. It tracks and provides complete details about who opened your mail and which document has been opened, as well as which links are being clicked and read. It offers mail merging, split testing, and full list management including segmenting. You can compose an email containing malicious links and send it to the employees of the target organization and keep track of your email. If the employee clicks on the link, he or she is infected and you will be notified. Thus, you can gain control over the system with the help of this tool.



Report Run: 7/20/2012 10:00:17 AM

From: [illegible] @live.com>;
Sent: 7/20/2012 9:34:07 AM
To: [illegible]
Subject: Test

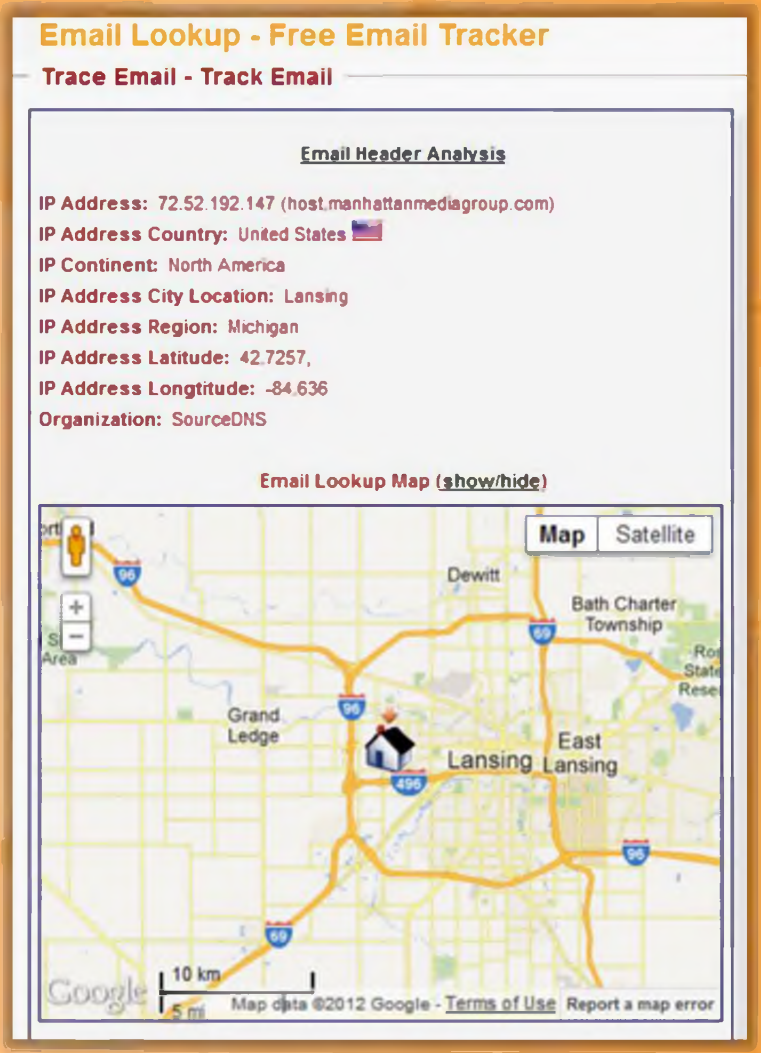
Opens		Clicks		Undeliverable		Opt-Out		Effective Rate	
3	75.00 %	3	75.00 %	0	0.00 %	0	0.00 %		100.00 %
unique recipients displayed content/pictures		unique recipients clicked at least one link		addresses returned as undeliverable		recipients opted-out of your list		ratio of responders to opens	
Multiple Opens	0.00 %	Multiple Clicks	50.00 %	Out of Office	0.00 %	Forwards	0.00 %	Replies	0.00 %
0		2		0		0		0	

FIGURE 2.26: Politemail screenshot

Email Lookup – Free Email Tracker

Source: http://www.ipaddresslocation.org

Email Lookup is an email tracking tool that determines the IP address of the sender by analyzing the **email header**. You can copy and paste the email header into this email tracking tool and start tracing email.



Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

IP Address: 72.52.192.147 (host.manhattanmediagroup.com)

IP Address Country: United States

IP Continent: North America

IP Address City Location: Lansing

IP Address Region: Michigan

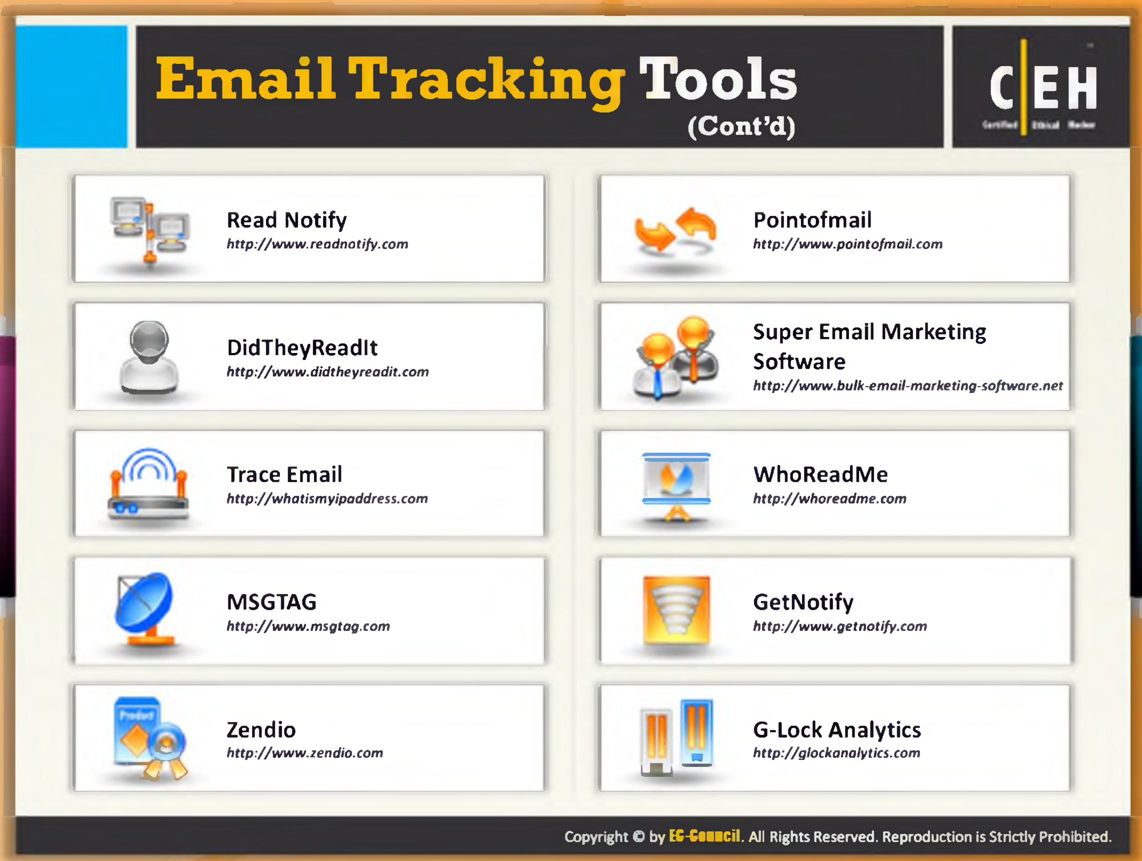
IP Address Latitude: 42.7257,

IP Address Longtitude: -84.636

Organization: SourceDNS

Email Lookup Map (show/hide)

FIGURE 2.27: Email Lookup Screenshot



Email Tracking Tools (Cont'd)

- Read Notify http://www.readnotify.com
- Pointofmail http://www.pointofmail.com
- DidTheyReadIt http://www.didtheyreadit.com
- Super Email Marketing Software http://www.bulk-email-marketing-software.net
- Trace Email http://whatismyipaddress.com
- WhoReadMe http://whoreadme.com
- MSGTAG http://www.msgtag.com
- GetNotify http://www.getnotify.com
- Zendio http://www.zendio.com
- G-Lock Analytics http://glockanalytics.com

Email Tracking Tools (Cont'd)

Read Notify

Source: http://www.readnotify.com

Read Notify provides an email tracking service. It notifies you when a tracked email is opened, re-opened, or forwarded. Read Notify tracking reports contain information such as complete delivery details, date and time of opening, geographic location of recipient, visualized map of location, IP address of the recipients, referrer details (i.e., if accessed via web email account etc.), etc.

DidTheyReadIt

Source: http://www.didtheyreadit.com

DidTheyReadIt is an email tracking utility. In order to use this utility you need to sign up for an account. Then you need to add ".DidTheyReadIt.com" to the end of the recipient's e-mail address. For example, if you were sending an e-mail to ellen@aol.com, you'd just send it to ellen@aol.com.DidTheyReadIt.com instead, and your email would be tracked. ellen@aol.com would not see that you added .DidTheyReadIt.com to her email address. This utility tracks every email that you send invisibly, without alerting the recipient. If the user opens your mail, then it informs you when your mail was opened, how long your email remained open, and the geographic location where your email was viewed.

TraceEmail

Source: http://whatismyipaddress.com

The TraceEmail tool attempts to locate the source IP address of an email based on the email headers. You just need to copy and paste the full headers of the target email into the Headers box and then click the Get Source button. It shows the **email header analysis** and results.

This Email header analysis tool does not have the ability to detect forged emails headers. These forged email headers are common in malicious email and spam. This tool assumes all mail servers and email clients in the transmission path are trustworthy.

MSGTAG

Source: http://www.msgtag.com

MSGTAG is Windows email tracking software that uses a read receipt technology to tell you when your emails are opened and when your emails are actually read. This software adds a **small track** and trace tag that is unique to each email you need delivery confirmation for. When the email is opened an email tracking code is sent to the MSGTAG email tracking system and an email read confirmation is delivered to you. MSGTAG will notify you when the message is read via an emailed confirmation, a pop-up message, or an **SMS text message**.

Zendio

Source: http://www.zendio.com

Zendio, the email tracking software add-in for Outlook, notifies you once your recipient reads the email, so you can follow up, knowing when they read it and if they clicked on any links included in the email.

Pointofmail

Source: http://www.pointofmail.com

Pointofmail.com is a proof of receipt and reading service for email. It ensures read receipts, tracks attachments, and lets you modify or delete sent messages. It provides detailed information about the recipient, full history of email reads and forwards, links and attachments tracking, email, and web and SMS text notifications.

Super Email Marketing Software

Source: http://www.bulk-email-marketing-software.net

Super Email Marketing Software is a professional and standalone bulk mailer program. It has the ability to send mails to a list of addresses. It supports both text as well as **HTML formatted emails.** All duplicate email addresses are removed automatically by using this application. Each mail is sent individually to the recipient so that the recipient can only see his or her email in the email header. It saves the email addresses of the successful sent mails as well as the failed mails to a text, CSV, TSV or Microsoft Excel file.

WhoReadMe

ource: http://whoreadme.com

WhoReadMe is an email tracking tool. It is completely invisible to recipients. The recipients will have no idea that the emails sent to them are being tracked. The sender is notified every time the recipient opens the mail sent by the sender. It tracks information such as type of operating system and browser used, Active X Controls, CSS version, duration between the mails sent and read time, etc.

GetNotify

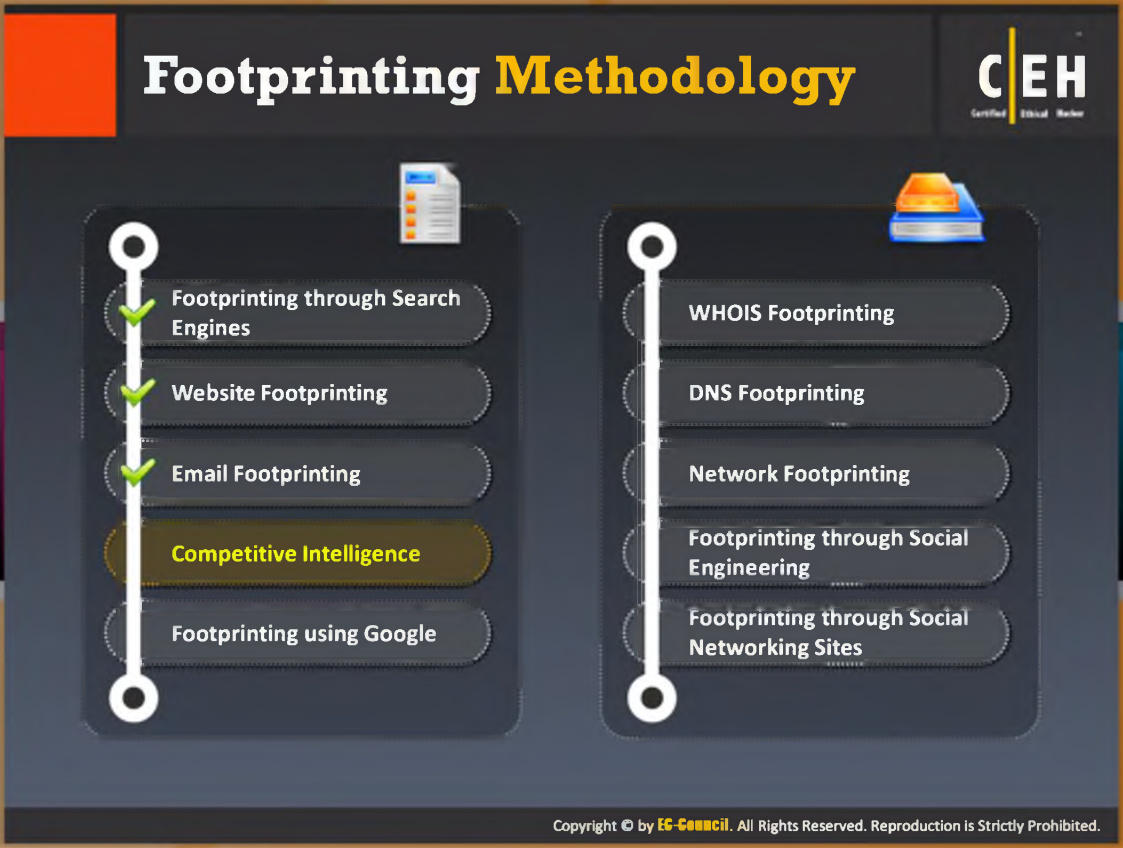
Source: http://www.getnotify.com

GetNotify is an email tracking tool that sends notifications when the recipient opens and reads the mail. It sends notifications without the knowledge of recipient.

G-Lock Analytics

Source: http://glockanalytics.com

G-Lock Analytics is an **email** tracking service. This allows you to know what happens to your emails after they are sent. This tool reports to you how many times the email was printed and forwarded.



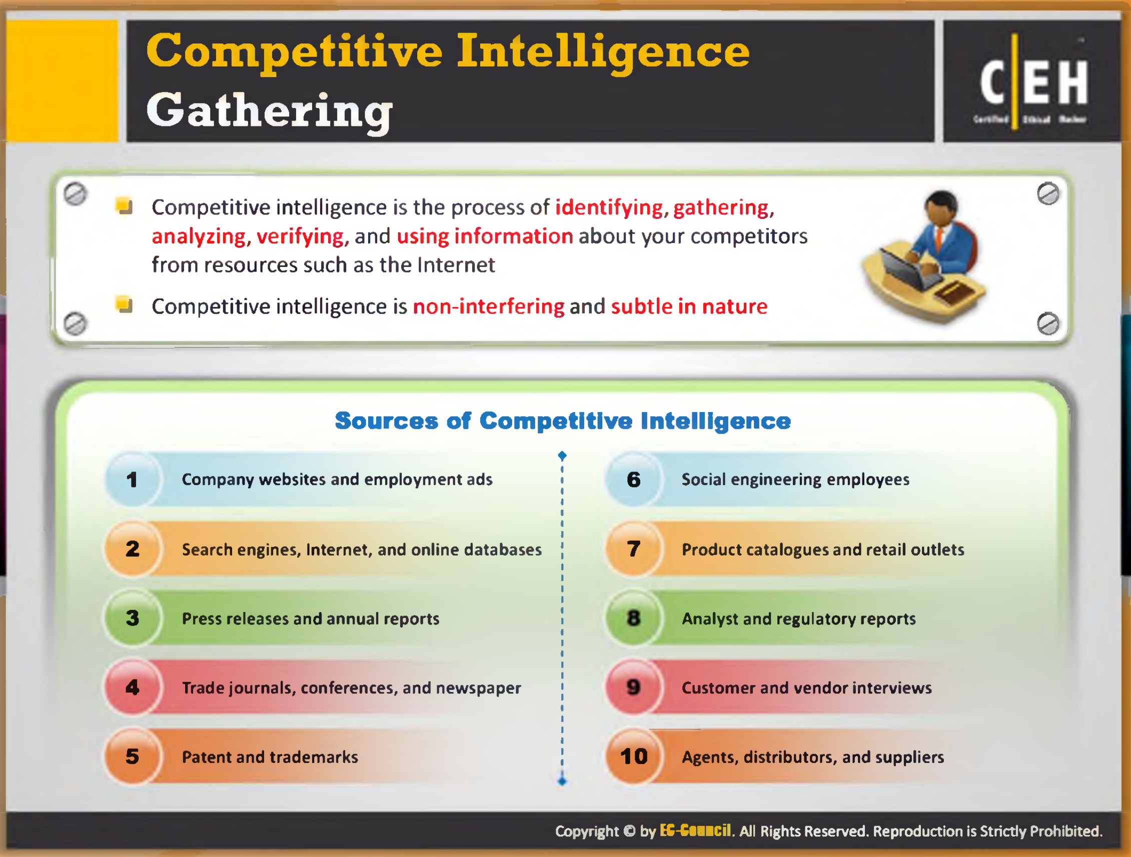
Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- Competitive Intelligence
- Footprinting using Google
- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

The next phase in footprinting methodology after email footprinting is **competitive intelligence**.

Competitive intelligence is a process that gathers, analyzes, and distributes intelligence about products, customers, competitors, and technologies using the Internet. The information that is gathered can help managers and executives of a company make **strategic decisions**. This section is about competitive intelligence gathering and sources where you can get valuable information.



Competitive Intelligence Gathering

- Competitive intelligence is the process of **identifying, gathering, analyzing, verifying,** and **using information** about your competitors from resources such as the Internet
- Competitive intelligence is **non-interfering** and **subtle in nature**

Sources of Competitive Intelligence

1. Company websites and employment ads
2. Search engines, Internet, and online databases
3. Press releases and annual reports
4. Trade journals, conferences, and newspaper
5. Patent and trademarks
6. Social engineering employees
7. Product catalogues and retail outlets
8. Analyst and regulatory reports
9. Customer and vendor interviews
10. Agents, distributors, and suppliers

Competitive Intelligence Gathering

Various tools are readily available in the market for the purpose of competitive intelligence gathering.

Acquisition of information about products, competitors, and technologies of a company using the Internet is defined as competitive intelligence. Competitive intelligence is not just about **analyzing competitors but also analyzing their products, customers, suppliers**, etc. that impact the organization. It is non-interfering and subtle in nature compared to the direct intellectual property theft carried out through hacking or industrial espionage. It mainly concentrates on the external business environment. It gathers information ethically and legally instead of gathering it secretly. According to CI professionals, if the intelligence information gathered is not useful, then it is not called intelligence. **Competitive intelligence** is performed for determining:

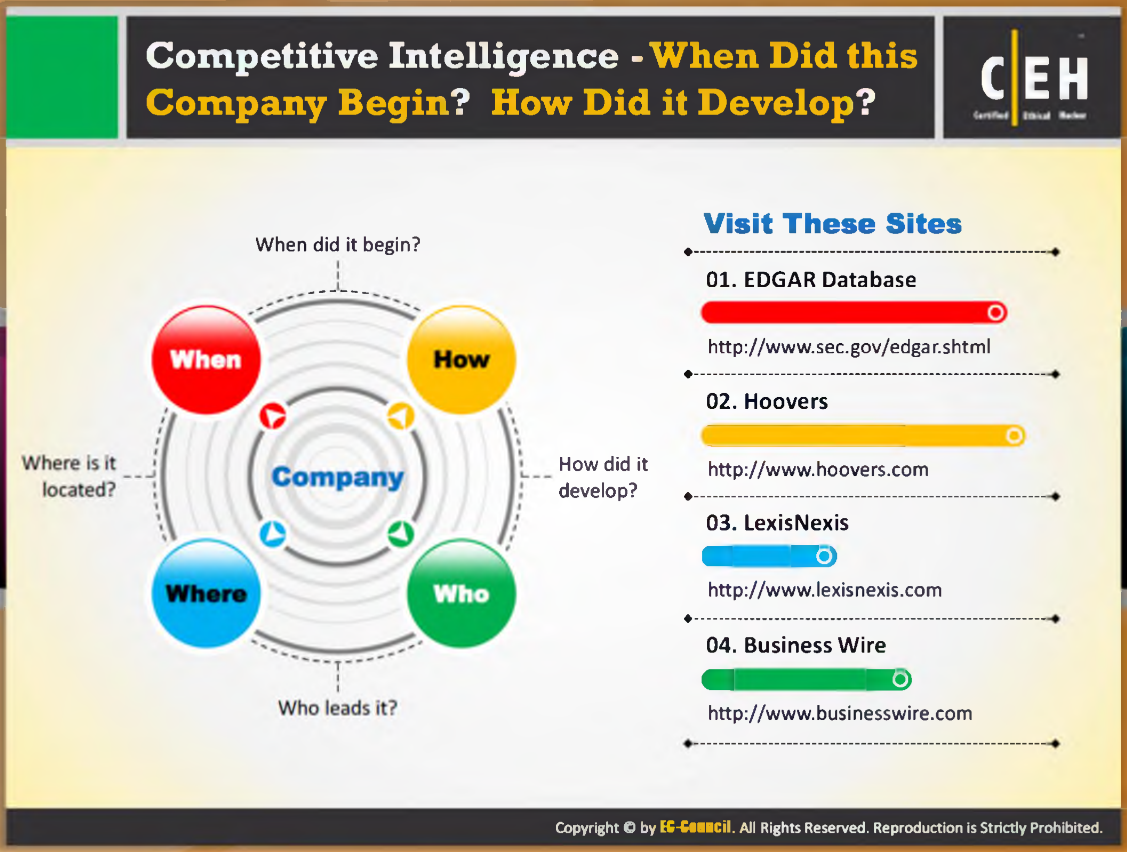
- What the competitors are doing
- How competitors are positioning their products and services

Sources of Competitive Intelligence:

- Company websites and employment ads
- Search engines, Internet, and online databases

- Press releases and annual reports
- Trade journals, conferences, and newspapers
- Patents and trademarks
- Social engineering employees
- Product catalogs and retail outlets
- Analyst and regulatory reports
- Customer and vendor interviews
- Agents, distributors, and suppliers

Competitive intelligence can be carried out by either employing people to search for the information or by utilizing a commercial database service, which incurs a lower cost than employing personnel to do the same thing.



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. Business Wire
http://www.businesswire.com

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

Gathering competitor documents and records helps improve **productivity** and **profitability** and stimulate the growth. It helps determine the answers to the following:

When did it begin?

Through competitive intelligence, the history of a company can be collected, such as when a particular company was established. Sometimes, crucial information that isn’t usually available for others can also be collected.

How did it develop?

It is very beneficial to know about how exactly a particular company has developed. What are the various strategies used by the company? Their advertisement policy, customer relationship management, etc. can be learned.

Who leads it?

This information helps a company learn details of the leading person (decision maker) of the company.

Where is it located?

The location of the company and information related to various branches and their operations can be collected through competitive intelligence.

You can use this information gathered through competitive intelligence to build a hacking strategy.

The following are information resource sites that help users **gain competitive intelligence**.

EDGAR

Source: http://www.sec.gov/edgar.shtml

All companies, foreign and domestic, are required to file registration statements, periodic reports, and other forms electronically through EDGAR. Anyone can view the **EDGAR database** freely through the Internet (web or FTP). All the documents that are filed with the commission by public companies may not be available on EDGAR.

Hoovers

Source: http://www.hoovers.com

Hoovers is a business research company that provides complete details about companies and industries all over the world. Hoovers provides patented business-related information through Internet, data feeds, wireless devices, and co-branding agreements with other online services. It gives complete information about the organizations, industries, and people that drive the economy and also provide the tools for connecting to the right people, in order for getting business done.

LexisNexis

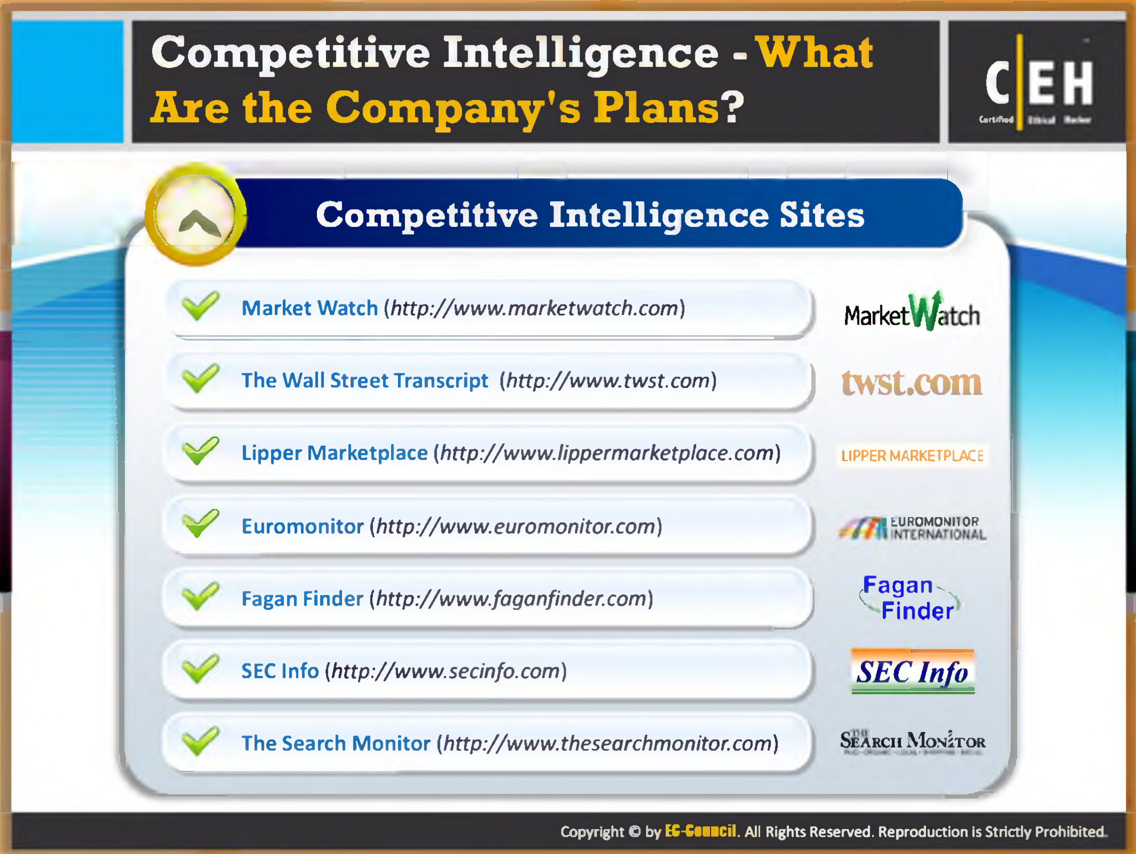
Source: http://www.lexisnexis.com

LexisNexis is a global provider of content-enabled workflow solutions designed specifically for **professionals in the legal, risk management, corporate, government, law enforcement, accounting, and academic markets**. It maintains an electronic database through which you can get legal and public-records related information. Documents and records of legal, news, and business sources are made accessible to customers.

Business Wire

Source: http://www.businesswire.com

Business Wire is a company that focuses on press release distribution and regulatory disclosure. Full text news releases, photos, and other multimedia content from thousands of companies and organizations are distributed by this company across the globe to journalists, news media, financial markets, investors, information website, databases, and general audiences. This company has its own patented electronic network through which it releases its news.



Competitive Intelligence - What Are the Company's Plans?

Competitive Intelligence Sites

- ✓ Market Watch (*http://www.marketwatch.com*)
- ✓ The Wall Street Transcript (*http://www.twst.com*)
- ✓ Lipper Marketplace (*http://www.lippermarketplace.com*)
- ✓ Euromonitor (*http://www.euromonitor.com*)
- ✓ Fagan Finder (*http://www.faganfinder.com*)
- ✓ SEC Info (*http://www.secinfo.com*)
- ✓ The Search Monitor (*http://www.thesearchmonitor.com*)

Competitive Intelligence - What Are the Company's Plans?

The following are a few more examples of websites that are useful to gather valuable information about various companies and their plans through competitive intelligence:

MarketWatch

Source: http://www.marketwatch.com

MarketWatch tracks the pulse of markets. The site provides business news, personal finance information, real-time commentary, and investment tools and data, with dedicated journalists generating hundreds of headlines, stories, videos, and market briefs a day.

The Wall Street Transcript

Source: http://www.twst.com

The Wall Street Transcript is a website as well as paid subscription publication that publishes industry reports. It expresses the views of money managers and equity analysts of different industry sectors. Interviews with CEOs of companies are published.

Lipper Marketplace

Source: http://www.lippermarketplace.com

Lipper Marketplace offers web-based solutions that are helpful for identifying the market of a company. Marketplace helps in qualifying prospects and provides the competitive intelligence needed for transforming these prospects into clients. Its solutions allow users to identify net flows and track institutional trends.

Euromonitor

Source: http://www.euromonitor.com

Euromonitor provides strategy research for consumer markets. It publishes reports on industries, consumers, and demographics. It provides market research and surveys focused on your organization's needs.

Fagan Finder

Source: http://www.faganfinder.com

Fagan Finder is a collection of internet tools. It is a directory of blog sites, news sites, search engines, photo sharing sites, science and education sites, etc. Specialized tools such as Translation Wizard and URL info are available for finding information about various actions with a web page.

SEC Info

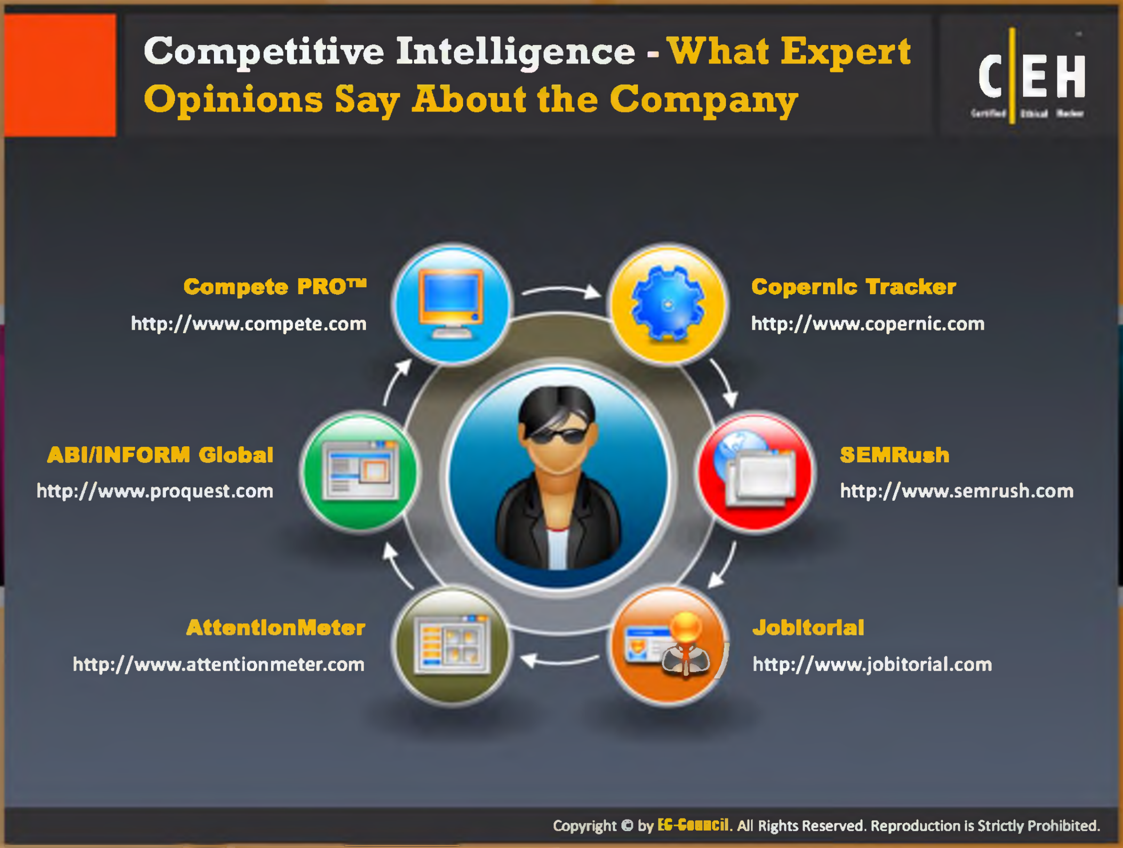
Source: http://www.secinfo.com

SEC Info offers the U.S. Securities and **Exchange Commission (SEC) EDGAR** database service on the web, with billions of links added to the SEC documents. It allows you to search by Name, Industry, and Business, SIC Code, Area Code, Accession Number, File Number, CIK, Topic, ZIP Code, etc.

The Search Monitor

Source: http://www.thesearchmonitor.com

The Search Monitor provides real-time competitive intelligence to monitor a number of things. It allows you to monitor market share, page rank, ad copy, landing pages, and the budget of your competitors. With the **trademark monitor**, you can monitor the buzz about yours as well as your competitor's brand and with the affiliate monitor; you can watch monitor ad and landing page copy.



Competitive Intelligence - What Expert Opinions Say About the Company

Compete PRO™
http://www.compete.com

Copernic Tracker
http://www.copernic.com

ABI/INFORM Global
http://www.proquest.com

SEMRush
http://www.semrush.com

AttentionMeter
http://www.attentionmeter.com

Jobitorial
http://www.jobitorial.com

Competitive Intelligence - What Expert Opinions Say About the Company

Copernic Tracker

Source: http://www.copernic.com

Copernic is website tracking software. It monitors a competitor's website continuously and acknowledges you content changes via an email, if any. The updated pages as well as the changes made in the site are highlighted for your convenience. You can even watch for specific keywords, to see the changes made on your **competitor's sites**.

SEMRush

Source: http://www.semrush.com

SEMRush is a competitive keyword research tool. For any site, you can get a list of Google keywords and AdWords, as well as a competitors list in the organic and paid Google search results. Necessary means for gaining in-depth knowledge about what competitors are advertising and their budget allocation to specific Internet marketing tactics are provided by SEMRush

Jobitorial

Source: http://www.jobitorial.com

Jobitorial provides anonymous employee reviews posted for jobs at thousands of companies and allows you to review a company.

AttentionMeter

Source: http://www.attentionmeter.com

AttentionMeter is a tool used for comparing any website you want (traffic) by using Alexa, Compete, and Quancast. It gives you a snapshot of traffic data as well as graphs from Alexa, Compete, and QuantCast.

ABI/INFORM Global

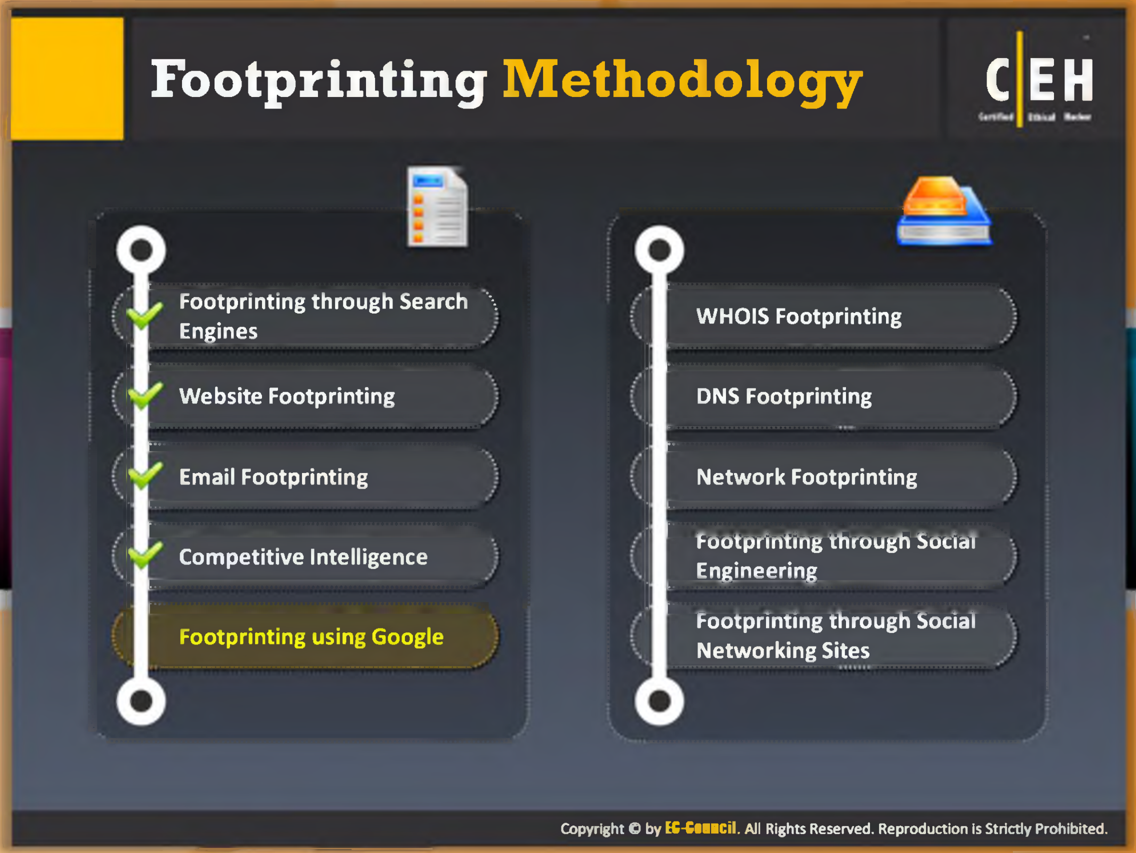
Source: http://www.proquest.com

ABI/INFORM Global is a business database. ABI/INFORM Global offers the latest business and financial information for researchers at all levels. With ABI/INFORM Global, users can determine business conditions, management techniques, business trends, management practice and theory, corporate strategy and tactics, and the competitive landscape.

Compete PRO

Source: http://www.compete.com

Compete PRO provides an online **competitive intelligence service**. It combines all the site, search, and referral analytics in a single product.



Footprinting Methodology

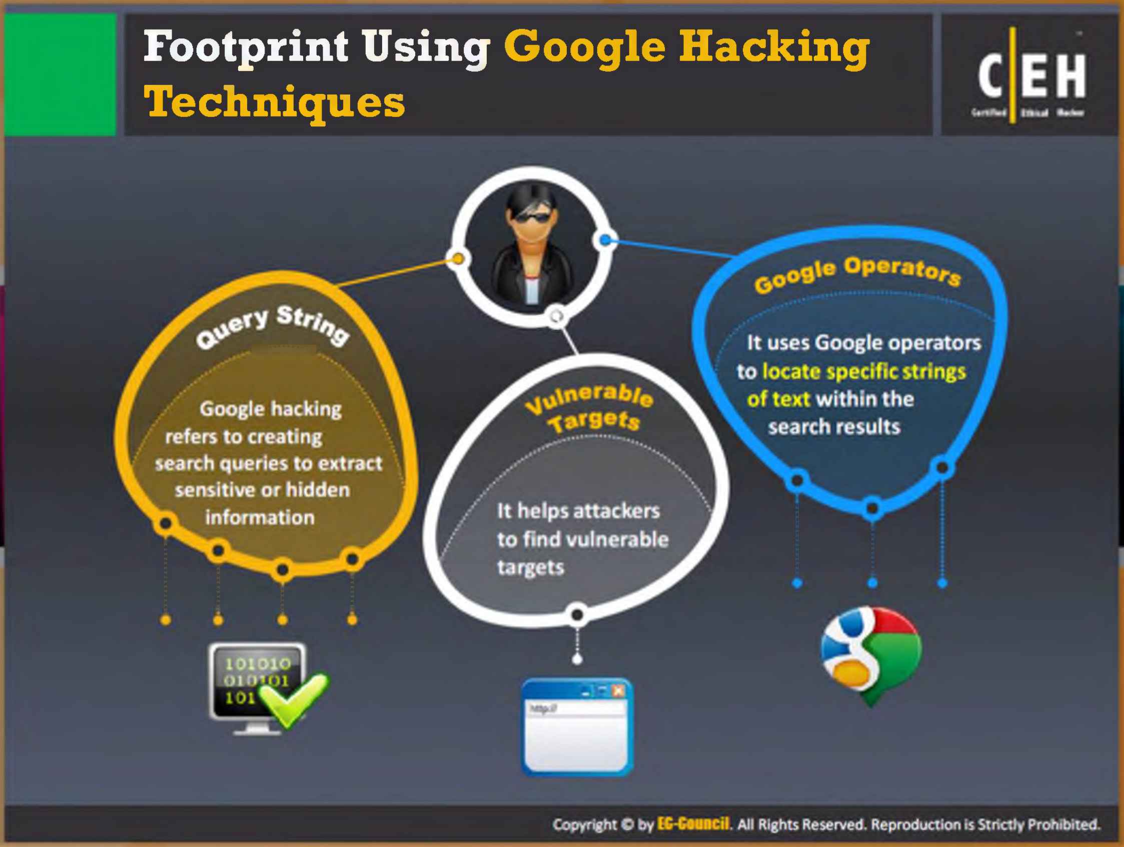
- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

Footprinting using Google

Though Google is a search engine, the process of footprinting using Google is not similar to the process of footprinting through search engines. Footprinting using Google deals with gathering information by Google hacking. Google hacking is a hacking technique to locate specific strings of text within search results using an advanced operator in Google search engine. Google will filter for excessive use of advanced search operators and will drop the requests with the help of an Intrusion Prevention System



Footprint Using Google Hacking Techniques

Query String

Google hacking refers to creating search queries to extract sensitive or hidden information

Vulnerable Targets

It helps attackers to find vulnerable targets

Google Operators

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

Footprinting using Google Hacking Techniques

Google hacking refers to the art of creating complex search engine queries. If you can construct proper queries, you can retrieve valuable data about a target company from the Google search results. Through Google hacking, an attacker tries to find websites that are vulnerable to numerous exploits and vulnerabilities. This can be accomplished with the help of Google hacking database (GHDB), a database of queries to identify sensitive data. Google operators help in finding required text and avoiding irrelevant data. Using advanced Google operators, attackers locate specific strings of text such as specific versions of vulnerable web applications.

Some of the popular Google operators include:

- **.Site**: The .Site operator in Google helps to find only pages that belong to a specific URL.
- **allinurl**: This operator finds the required pages or websites by restricting the results containing all query terms.
- **Inurl**: This will restrict the results to only websites or pages that contain the query terms that you have specified in the URL of the website.
- **allintitle**: It restricts results to only web pages that contain all the query terms that you have specified.

- **intitle**: It restricts results to only the web pages that contain the query term that you have specified. It will show only websites that mention the query term that you have used.
- **Inanchor**: It restricts results to pages containing the query term that you have specified in the anchor text on links to the page.
- **Allinanchor**: It restricts results to pages containing all query terms you specify in the anchor text on links to the page.

What a Hacker can do with Google Hacking?

Attacker gathers:

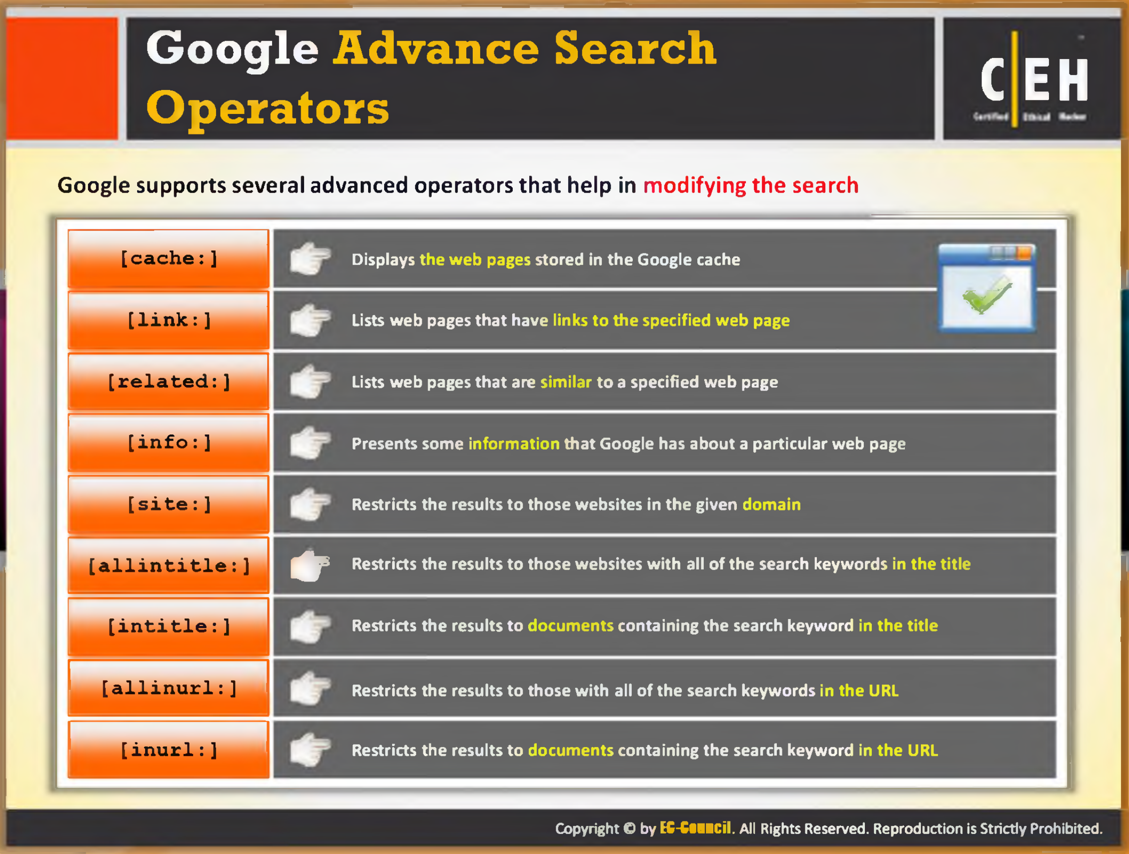
- Advisories and server vulnerabilities
- Error messages that contain sensitive information
- Pages containing network or vulnerability data
- Files containing passwords
- Pages containing logon portals
- Sensitive directories

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What Can a Hacker Do with Google Hacking?

If the target website is vulnerable to Google hacking, then the attacker can find the following with the help of queries in Google hacking database:

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data
- Advisories and server vulnerabilities



Google Advance Search Operators

Google supports several advanced operators that help in modifying the search

[cache:]	Displays the web pages stored in the Google 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:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain
[allintitle:]	Restricts the results to those websites with all of the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those with all of the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL

Google Advance Search Operators

Source: http://www.googleguide.com

Cache: The CACHE query displays Google's cached version of a web page, instead of the current version of the page.

Example:

cache: www.eff.org will show Google’s cached version of the Electronic Frontier Foundation home page.

Note: Do not put a space between cache: and the URL (web address).

link: Link lists web pages that have links to the specified web page. For example, to find pages that point to Google Guide’s home page, enter:

link: www.googleguide.com

Note: According to Google’s documentation, “you cannot combine a link: search with a regular keyword search.”

Also note that when you combine link: with another advanced operator, Google may not return all the pages that match. The following queries should return lots of results, as you can see if you remove the -site: term in each of these queries.

related: If you start your query with "related:", then Google displays websites similar to the site mentioned in the search query.

Example: related:www.microsoft.com will provide the Google search engine results page with websites similar to microsoft.com.

info: Info will present some information the corresponding web page.

For instance, info:gothotel.com will show information about the national hotel directory GotHotel.com home page.

Note: There must be no space between the info: and the web page URL.

This functionality can also be obtained by typing the web page URL directly into a Google search box.

site: If you include site: in your query, Google will restrict your search results to the site or domain you specify.

For example, admissions site:www.lse.ac.uk will show admissions information from London School of Economics' site and [peace site:gov] will find pages about peace within the .gov domain. You can specify a domain with or without a period, e.g., either as .gov or gov.

Note: Do not include a space between the "site:" and the domain.

allintitle: If you start your query with allintitle:, Google restricts results to those containing all the query terms you specify in the title.

For example, allintitle: detect plagiarism will return only documents that contain the words "detect" and "plagiarism" in the title. This functionality can also be obtained through the Advanced Web Search page, under Occurrences.

intitle: The query intitle: term restricts results to documents containing term in the title. For instance, flu shot intitle:help will return documents that mention the word "help" in their titles, and mention the words "flu" and "shot" anywhere in the document (title or not).

Note: There must be no space between the intitle: and the following word.

allinurl: If you start your query with allinurl:, Google restricts results to those containing all the query terms you specify in the URL.

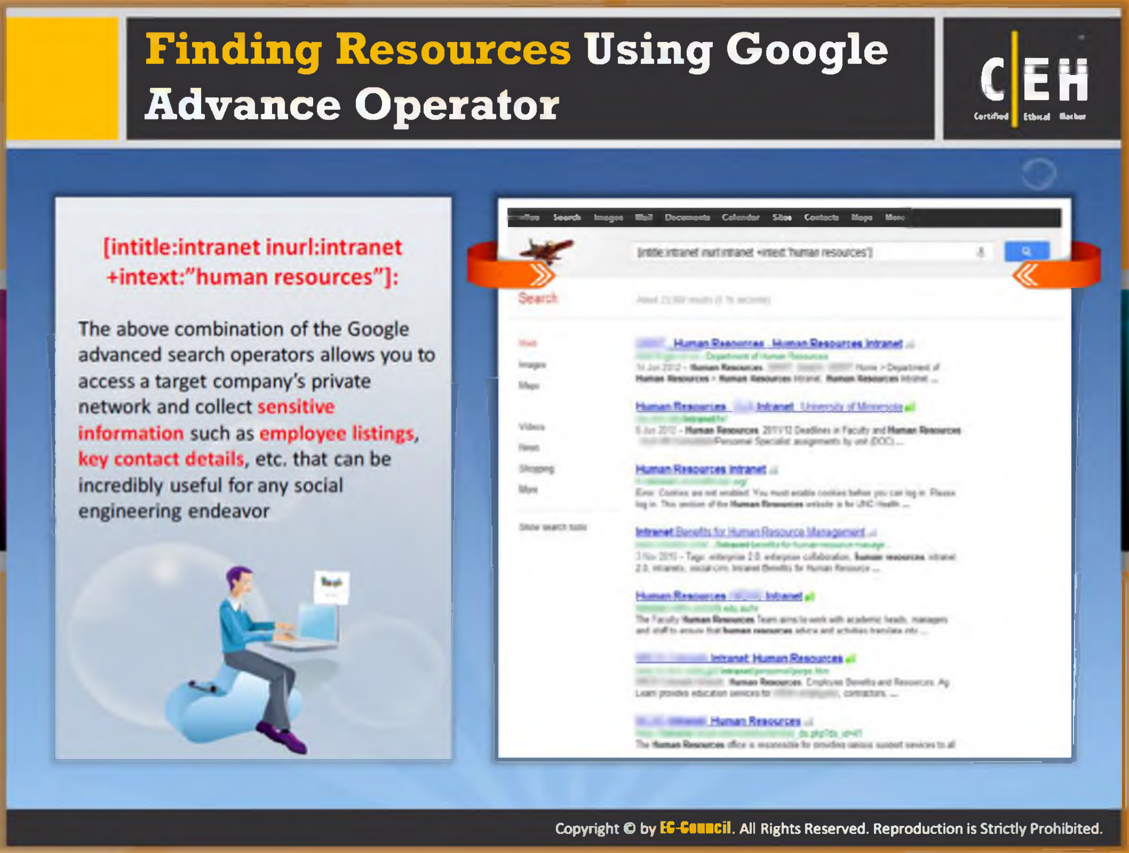
For example, allinurl: google faq will return only documents that contain the words "google" and "faq" in the URL, such as "www.google.com/help/faq.html." This functionality can also be obtained through the Advanced Web Search page, under Occurrences.

In URLs, words are often run together. They need not be run together when you're using allinurl.

inurl: If you include inurl: in your query, Google will restrict the results to documents containing that word in the URL.

For instance, inurl:print site:www.googleguide.com searches for pages on Google Guide in which the URL contains the word "print." It finds PDF files that are in the directory or folder named "print" on the Google Guide website. The query [inurl:healthy eating] will return documents that mention the words “healthy” in their URL, and mention the word “eating” anywhere in the document.

Note: There must be no space between the inurl: and the following word.



Finding Resources Using Google Advance Operator

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

The above combination of the Google advanced search operators allows you to access a target company's private network and collect sensitive information such as employee listings, key contact details, etc. that can be incredibly useful for any social engineering endeavor

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

Human Resources Intranet

Intranet Benefits for Human Resource Management

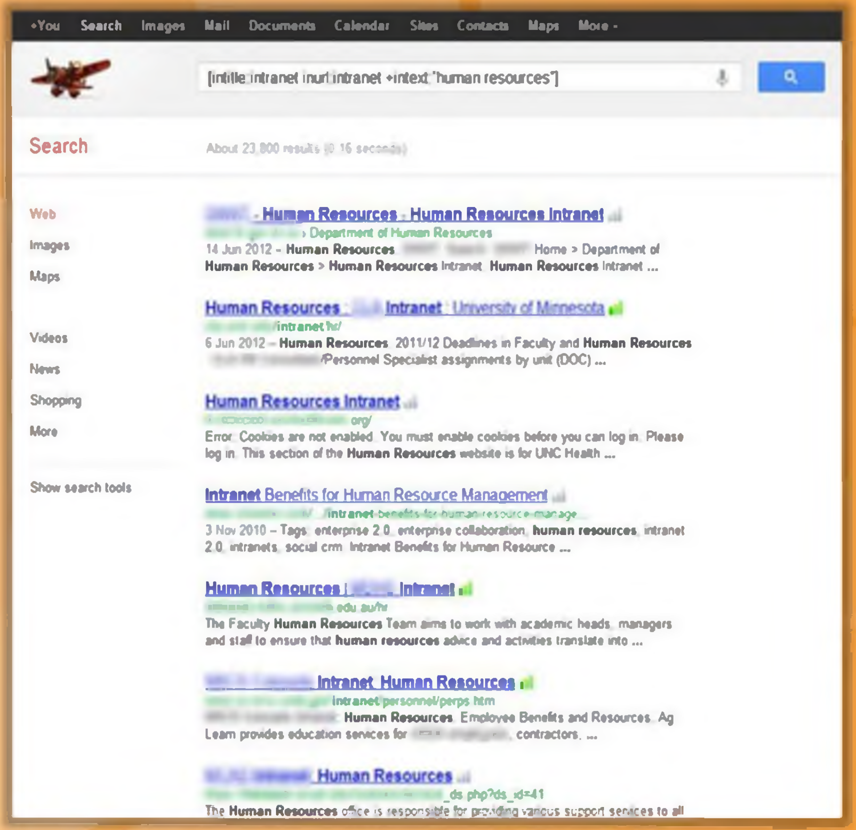
Intranet Human Resources

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Resources using Google Advance Operator

By using the Google Advance Operator syntax `[intitle:intranet inurl:intranet +intext:"human resources"]`: the attacker can find private information of a target company as well as sensitive information about the employees of that particular company. The information gathered by the attackers can be used to perform social engineering attacks. Google will filter for excessive use of advanced search operators and will drop the requests with the help of an Intrusion Prevention System.

The following screenshot shows a Google search engine results page displaying the results of the previously mentioned query:



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

About 23,800 results (0.16 seconds)

[redacted] - **Human Resources** - **Human Resources Intranet**
[redacted] › Department of Human Resources
14 Jun 2012 – **Human Resources** [redacted] Home > Department of **Human Resources** > **Human Resources** Intranet. **Human Resources** Intranet ...

Human Resources : [redacted] **Intranet** : University of Minnesota
[redacted]/**intranet**/hr/
6 Jun 2012 – **Human Resources**. 2011/12 Deadlines in Faculty and **Human Resources** [redacted]/Personnel Specialist assignments by unit (DOC) ...

Human Resources Intranet
[redacted] org/
Error: Cookies are not enabled. You must enable cookies before you can log in. Please log in. This section of the **Human Resources** website is for UNC Health ...

Intranet Benefits for Human Resource Management
[redacted]/.../**intranet**-benefits-for-human-resource-manage...
3 Nov 2010 – Tags: enterprise 2.0, enterprise collaboration, **human resources**, intranet 2.0, intranets, social crm. Intranet Benefits for Human Resource ...

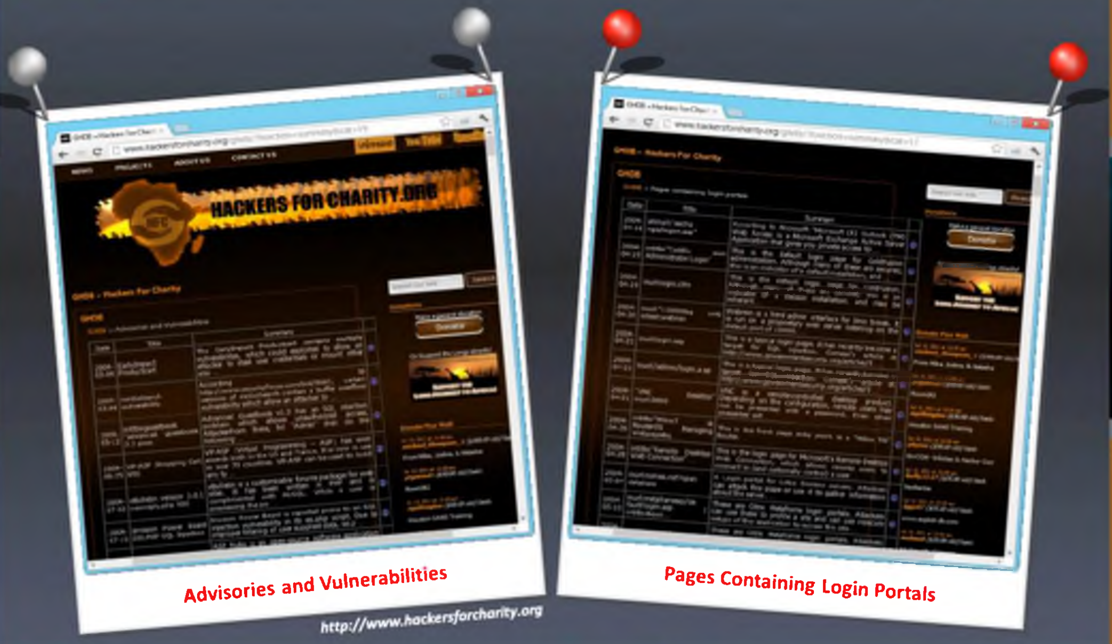
Human Resources | [redacted] **Intranet**
[redacted] edu.au/hr
The Faculty **Human Resources** Team aims to work with academic heads, managers and staff to ensure that **human resources** advice and activities translate into ...

[redacted] **Intranet**: **Human Resources**
[redacted] **intranet**/personnel/perps.htm
[redacted] **Human Resources**. Employee Benefits and Resources. Ag Learn provides education services for [redacted] contractors. ...

[redacted] **Human Resources**
[redacted]_ds.php?ds_id=41
The **Human Resources** office is responsible for providing various support services to all

FIGURE 2.28: Search engine showing results for given Google Advance Operator syntax

Google Hacking Tool: Google Hacking Database (GHDB)



Advisories and Vulnerabilities

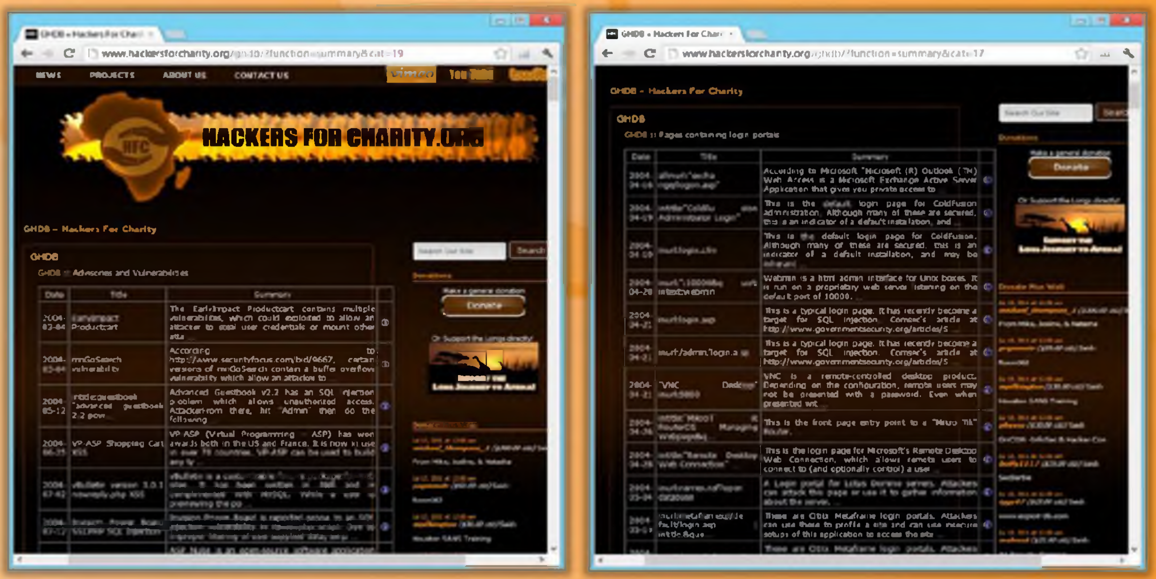
Pages Containing Login Portals

http://www.hackersforcharity.org

Google Hacking Tool: Google Hacking Database (GHDB)

Source: http://www.hackersforcharity.org

The Google Hacking database (GHDB) is a database of queries that identify sensitive data. GHDB is an **HTML/JavaScript wrapper application** that uses advanced JavaScript techniques to scrape information from Johnny's Google Hacking Database without the need for hosted server-side scripts. The Google Hacking Database exposes known issues with software that run websites. There are some bugs that expose information that might not warrant public reading.



GHDB – Hackers For Charity

GHDB

GHDB :: Advisories and Vulnerabilities

Date	Title	Summary
2004-03-04	Earlyimpact Productcart	The EarlyImpact Productcart contains multiple vulnerabilities, which could exploited to allow an attacker to steal user credentials or mount other atta ...
2004-03-04	mnGoSearch vulnerability	According to http://www.securityfocus.com/bid/9667, certain versions of mnoGoSearch contain a buffer overflow vulnerability which allow an attacker to ...
2004-05-12	intitle:guestbook "advanced guestbook 2.2 pow ...	Advanced Guestbook v2.2 has an SQL injection problem which allows unauthorized access. Attacker-from there, hit "Admin" then do the following
2004-06-25	VP-ASP Shopping Cart XSS	VP-ASP (Virtual Programming - ASP) has won awards both in the US and France. It is now in use in over 70 countries. VP-ASP can be used to build any ty ...
2004-07-02	vBulletin version 3.0.1 newreply.php XSS	vBulletin is a customizable forums package [illegible] site. It has been written in PHP and is complemented with MySQL. While a user is previewing the po ...
2004-07-12	Invision Power Board SSI.PHP SQL Injection	Invision Power Board is reported prone to an SQL injection vulnerability in its ssi.php script. Due to improper filtering of user supplied data, an ...
		ASP Nuke is an open-source software application

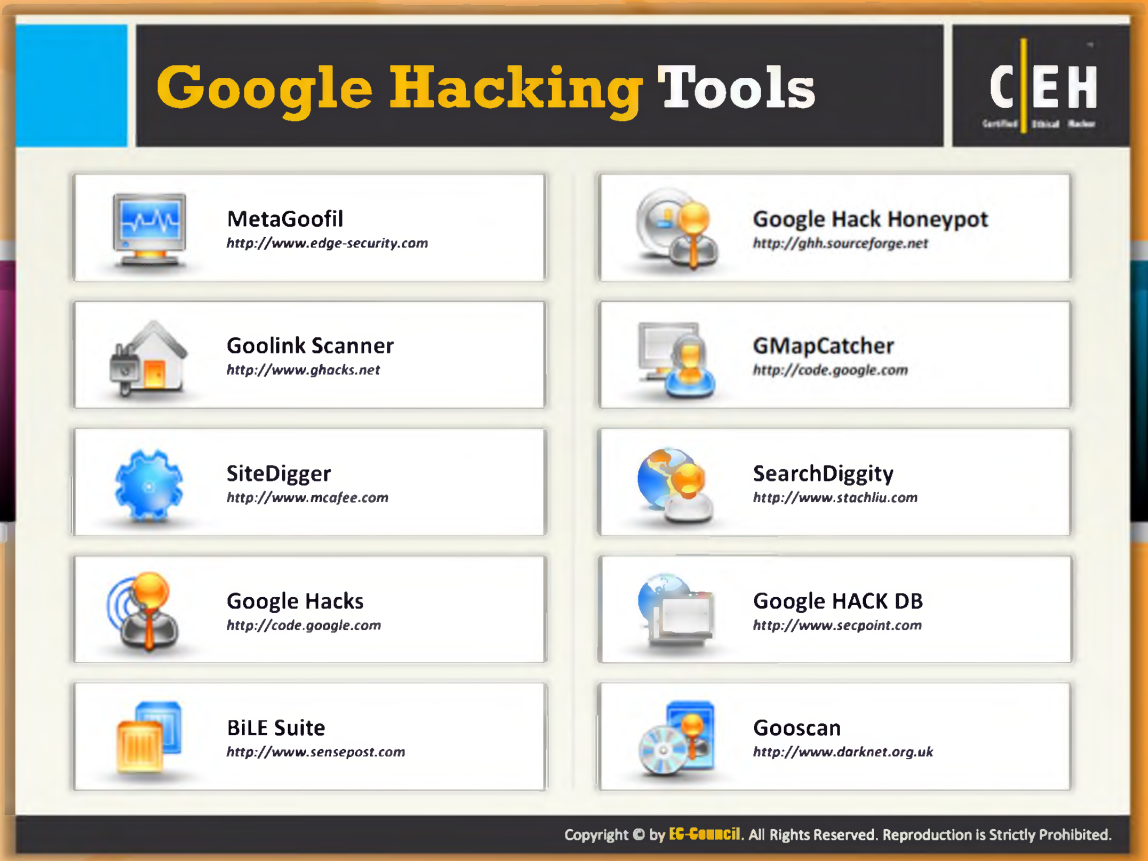
GHDB – Hackers For Charity

GHDB

GHDB :: Pages containing login portals

Date	Title	Summary
2004-04-06	allinurl:"exchange/logon.asp"	According to Microsoft "Microsoft (R) Outlook (TM) Web Access is a Microsoft Exchange Active Server Application that gives you private access to ...
2004-04-19	intitle:"ColdFusion Administrator Login"	This is the default login page for ColdFusion administration. Although many of these are secured, this is an indicator of a default installation, and ...
2004-04-09	inurl:login.cfm	This is the default login page for ColdFusion. Although many of these are secured, this is an indicator of a default installation, and may be inherent ...
2004-04-20	inurl:":10000" intext:webmin	Webmin is a html admin interface for Unix boxes. It is run on a proprietary web server listening on the default port of 10000. ...
2004-04-21	inurl:login.asp	This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/S ...
2004-04-21	inurl:/admin/login.asp	This is a typical login page. It has recently become a target for SQL injection. Comsec's article at http://www.governmentsecurity.org/articles/S ...
2004-04-21	"VNC Desktop" inurl:5800	VNC is a remote-controlled desktop product. Depending on the configuration, remote users may not be presented with a password. Even when presented wit ...
2004-04-26	intitle:"MikroTik RouterOS Managing Webpage"	This is the front page entry point to a "Mikro Tik" Router.
2004-04-26	intitle:"Remote Desktop Web Connection"	This is the login page for Microsoft's Remote Desktop Web Connection, which allows remote users to connect to (and optionally control) a user ...
2004-03-04	inurl:names.nsf?opendatabase	A login portal for Lotus Domino servers. Attackers can attack this page or use it to gather information about the server. ...
2004-03-01	inurl:metaframexp/default/login.asp intitle:&que ...	These are Citrix Metaframe login portals. Attackers can use these to profile a site and can use insecure setups of this application to access the site ...
		These are Citrix Metaframe login portals. Attackers

FIGURE 2.29: Screenshots showing Advisories and Vulnerabilities & pages containing login portals



Google Hacking Tools

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

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

Goolink Scanner
http://www.ghacks.net

GMapCatcher
http://code.google.com

SiteDigger
http://www.mcafee.com

SearchDiggity
http://www.stachliu.com

Google Hacks
http://code.google.com

Google HACK DB
http://www.secpoint.com

BiLE Suite
http://www.sensepost.com

Gooscan
http://www.darknet.org.uk

Google Hacking Tools

Besides the Google Hacking Database (GHDB) tool featured previously, there are some other tools that can help you with Google hacking. There are a few more Google hacking tools mentioned as follows. Using these tools, attackers can gather advisories and server vulnerabilities, error message information that may reveal attack paths, sensitive files, directories, logon portals, etc.

Metagoofil

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

Metagoofil is an information-gathering tool designed for extracting metadata of public documents (pdf, doc, xls, ppt, docx, pptx, xlsx) belonging to a target company.

Metagoofil performs a search in Google to identify and download the documents to a local disk and then extracts the metadata with different libraries such as Hachoir, PdfMiner?, and others. With the results, it generates a report with usernames, software versions, and servers or machine names that may help penetration testers in the information gathering phase.

Goolink Scanner

Source: http://www.ghacks.net

The Goolink Scanner **removes the cache** from your searches, and collects and displays only vulnerable site's links. Thus, it allows you to find vulnerable sites wide open to Google and googlebots.

SiteDigger

Source: http://www.mcafee.com

SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and **interesting security nuggets** on websites.

Google Hacks

Source: http://code.google.com

Google Hacks is a compilation of carefully crafted Google searches that **expose novel functionality** from Google's search and map services. It allows you to view a timeline of your search results, view a map, search for music, search for books, and perform many other specific kinds of searches.

BiLE Suite

Source: http://www.sensepost.com

BiLE stands for **Bi-directional** Link Extractor. The BiLE suite includes a couple of Perl scripts used in enumeration processes. Each Perl script has its own functionality. BiLE.pl is the first tool or Perl script in the collection. BiLE leans on Google and HTTrack to automate the collections to and from the target site, and then applies a simple **statistical weighing algorithm** to deduce which websites have the strongest relationships with the target site.

Google Hack Honeypot

Source: http://ghh.sourceforge.net

Google Hack Honeypot is the reaction to a new type of **malicious web traffic**: search engine hackers. It is designed to provide reconnaissance against attackers that use search engines as a hacking tool against your resources. GHH implements the honeypot theory to provide additional security to your web presence.

GMapCatcher

Source: http://code.google.com

GMapCatcher is an **offline maps viewer**. It displays maps from many providers such as: CloudMade, OpenStreetMap, Yahoo Maps, Bing Maps, Nokia Maps, and SkyVector. maps.py is a GUI program used to browse Google map. With the offline toggle button unchecked, it can download Google map tiles automatically. Once the file downloads, it resides on your hard disk. Thus, you don't need to download it again.

SearchDiggity

Source: http://www.stachliu.com

SearchDiggity is the primary attack tool of the **Google Hacking Diggity Project**. It is Stach & Liu's MS Windows GUI application that serves as a front-end to the most recent versions of Diggity tools such as GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

Google HACK DB

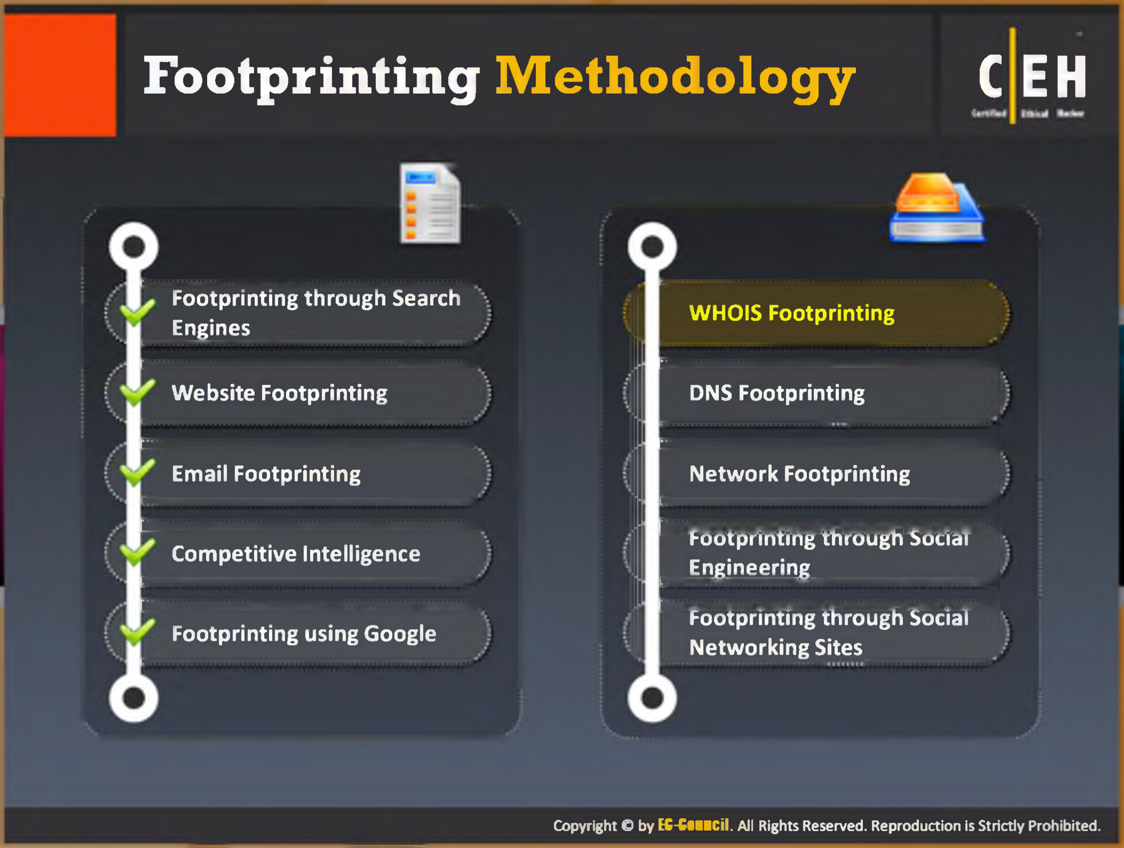
Source: http://www.secpoint.com

The attacker can also use the SecPoint Google HACK DB tool to determine sensitive information from the target site. This tool helps an attacker to extract files containing passwords, database files, clear text files, customer database files, etc.

Gooscan

Source: http://www.darknet.org.uk

Gooscan is a tool that automates queries against **Google search appliances**. These queries are designed to find potential vulnerabilities on web pages.



Footprinting Methodology

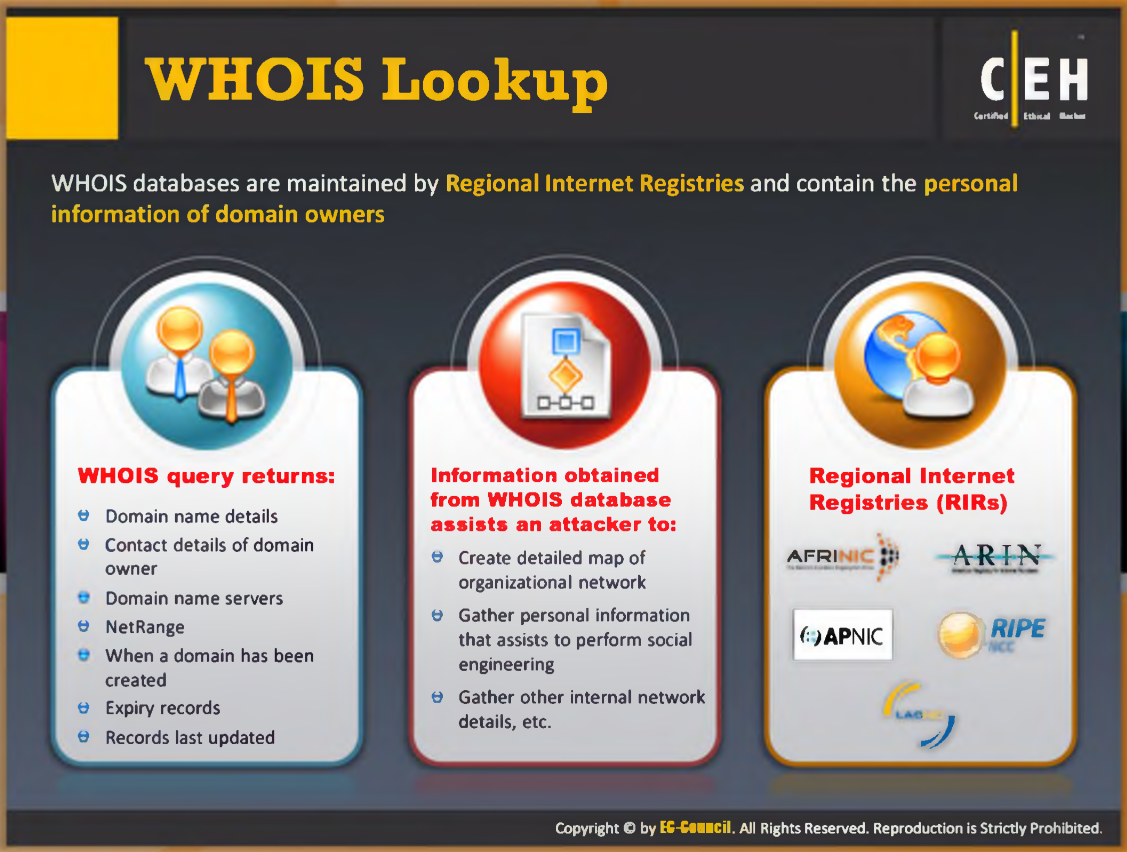
- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

Gathering **network-related** information such as whois information of the target organization is very important when hacking a system. So, now we will discuss whois footprinting.

Whois footprinting focuses on how to perform a whois lookup, analyzing the whois lookup results, and the tools to gather whois information.



WHOIS Lookup

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

WHOIS query returns:

- Domain name details
- Contact details of domain owner
- Domain name servers
- NetRange
- When a domain has been created
- Expiry records
- Records last updated

Information obtained from WHOIS database assists an attacker to:

- Create detailed map of organizational network
- Gather personal information that assists to perform social engineering
- Gather other internal network details, etc.

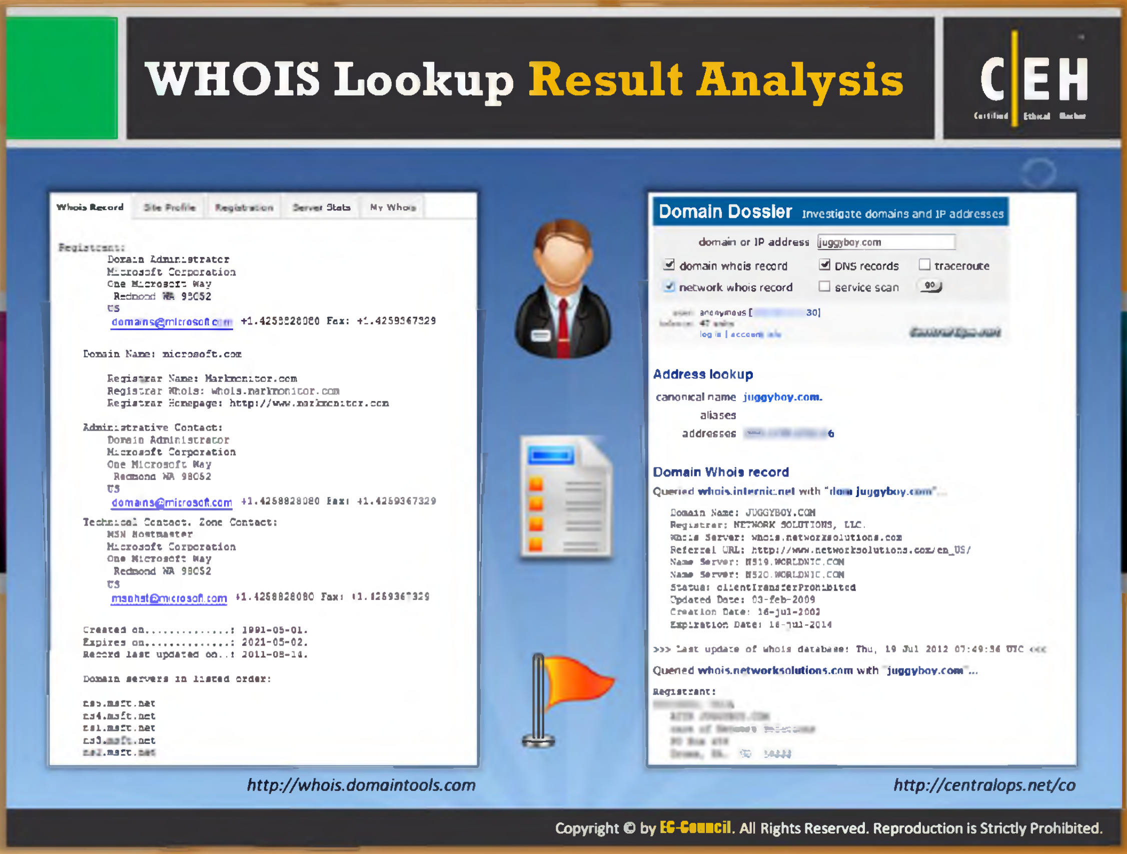
Regional Internet Registries (RIRs)

AFRINIC
ARIN
APNIC
RIPE NCC
LACNIC

WHOIS Lookup

WHOIS is a query and response protocol used for **querying databases** that stores the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. WHOIS databases are maintained by Regional Internet Registries and contain the personal information of domain owners. They maintain a record called a **LOOKUP table** that contains all the information associated with a particular network, domain, and host. Anyone can connect and query to this server to get information about particular networks, domains, and hosts.

An attacker can send a query to the appropriate **WHOIS** server to obtain the information about the target domain name, contact details of its owner, expiry date, creation date, etc. The WHOIS sever will respond to the query with respective information. Then, the attacker can use this information to create a map of the organization network, trick domain owners with social engineering once he or she gets contact details, and then get **internal details** of the network.



WHOIS Lookup Result Analysis

```
Registrant:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329

    Domain Name: microsoft.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329
    Technical Contact, Zone Contact:
        MSN Hostmaster
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

    Created on..............: 1991-05-01.
    Expires on..............: 2021-05-02.
    Record last updated on..: 2011-08-14.

    Domain servers in listed order:

    ns5.msft.net
    ns4.msft.net
    ns1.msft.net
    ns3.msft.net
    ns2.msft.net
```

http://whois.domaintools.com

Domain Dossier Investigate domains and IP addresses

domain or IP address: juggyboy.com

☑ domain whois record ☑ DNS records ☐ traceroute
☑ network whois record ☐ service scan [go]

user: anonymous [[redacted]30]
balance: 47 units
log in | account info

Address lookup

canonical name juggyboy.com.
aliases
addresses [redacted]6

Domain Whois record

Queried whois.internic.net with "dom juggyboy.com"...

```
   Domain Name: JUGGYBOY.COM
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com/en_US/
   Name Server: NS19.WORLDNIC.COM
   Name Server: NS20.WORLDNIC.COM
   Status: clientTransferProhibited
   Updated Date: 03-feb-2009
   Creation Date: 16-jul-2002
   Expiration Date: 16-jul-2014

>>> Last update of whois database: Thu, 19 Jul 2012 07:49:56 UTC <<<
```

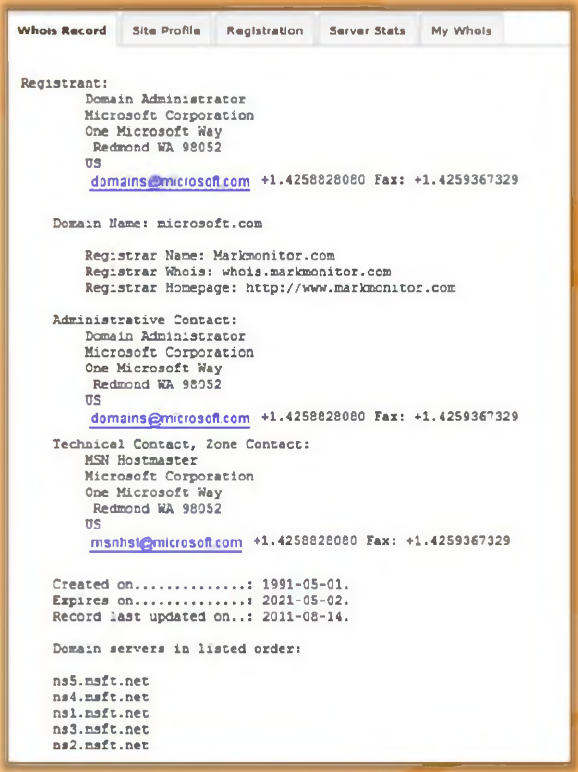
Queried whois.networksolutions.com with "juggyboy.com"...

```
Registrant:
[redacted]
```

http://centralops.net/co

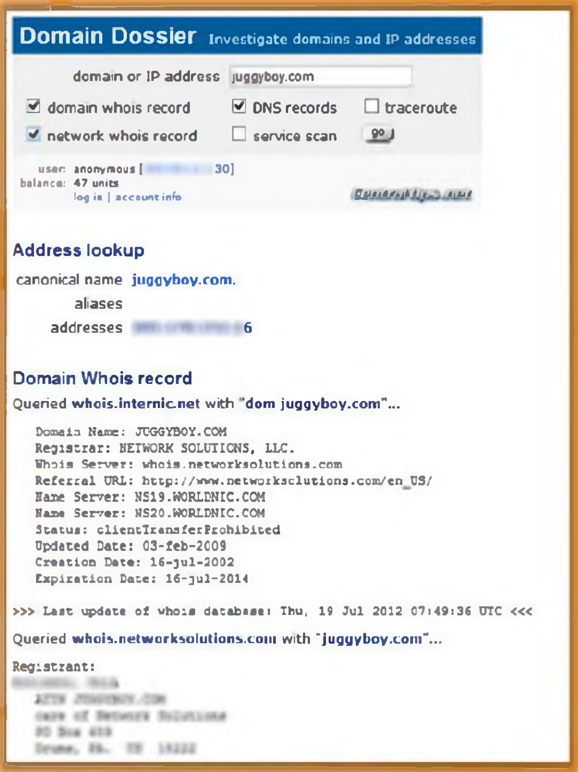
WHOIS Lookup Result Analysis

A whois lookup can be performed using Whois services such as http://whois.domaintools.com or http://centralops.net/co. Here you can see the result analysis of a Whois lookup obtained with the two mentioned Whois services. Both these services allow you to perform w whois lookup by entering the target's domain or IP address. The domaintools.com service provides whois information such as registrant information, email, administrative contact information, created and expiry date, a list of domain servers, etc. The Domain Dossier available at http://centralops.net/co/ gives the address lookup, domain Whois record, network whois record, and DNS records information.



```
Registrant:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329

    Domain Name: microsoft.com

        Registrar Name: Markmonitor.com
        Registrar Whois: whois.markmonitor.com
        Registrar Homepage: http://www.markmonitor.com

    Administrative Contact:
        Domain Administrator
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         domains@microsoft.com +1.4258828080 Fax: +1.4259367329
    Technical Contact, Zone Contact:
        MSN Hostmaster
        Microsoft Corporation
        One Microsoft Way
         Redmond WA 98052
        US
         msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

    Created on..............: 1991-05-01.
    Expires on..............: 2021-05-02.
    Record last updated on..: 2011-08-14.

    Domain servers in listed order:

    ns5.msft.net
    ns4.msft.net
    ns1.msft.net
    ns3.msft.net
    ns2.msft.net
```

http://whois.domaintools.com



domain or IP address juggyboy.com

☑ domain whois record ☑ DNS records ☐ traceroute
☑ network whois record ☐ service scan go

user: anonymous [[redacted]30]
balance: 47 units
log in | account info

Address lookup

canonical name juggyboy.com.
aliases
addresses [redacted]6

Domain Whois record

Queried whois.internic.net with "dom juggyboy.com"...

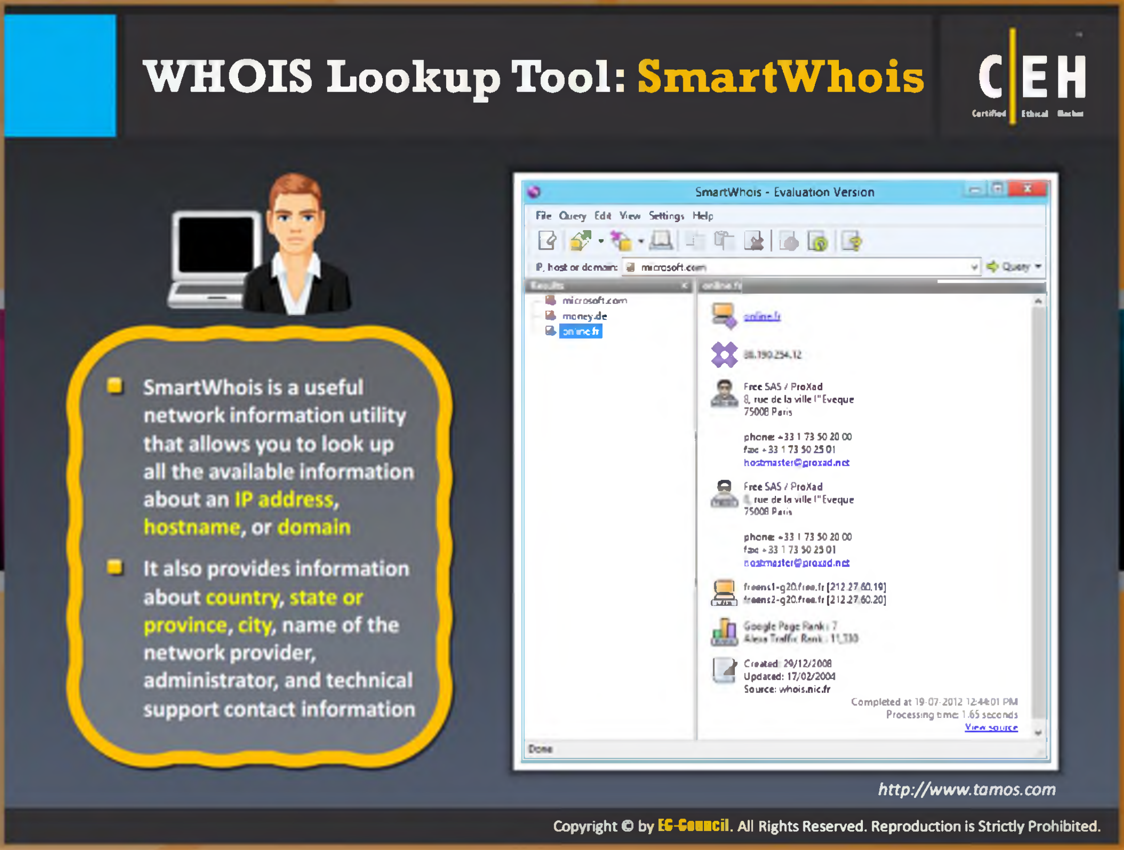
```
   Domain Name: JUGGYBOY.COM
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com/en_US/
   Name Server: NS19.WORLDNIC.COM
   Name Server: NS20.WORLDNIC.COM
   Status: clientTransferProhibited
   Updated Date: 03-feb-2009
   Creation Date: 16-jul-2002
   Expiration Date: 16-jul-2014

>>> Last update of whois database: Thu, 19 Jul 2012 07:49:36 UTC <<<
```

Queried whois.networksolutions.com with "juggyboy.com"...

```
Registrant:
[redacted]
```

http://centralops.net/co

FIGURE 2.30: Whois services screenshots



WHOIS Lookup Tool: 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

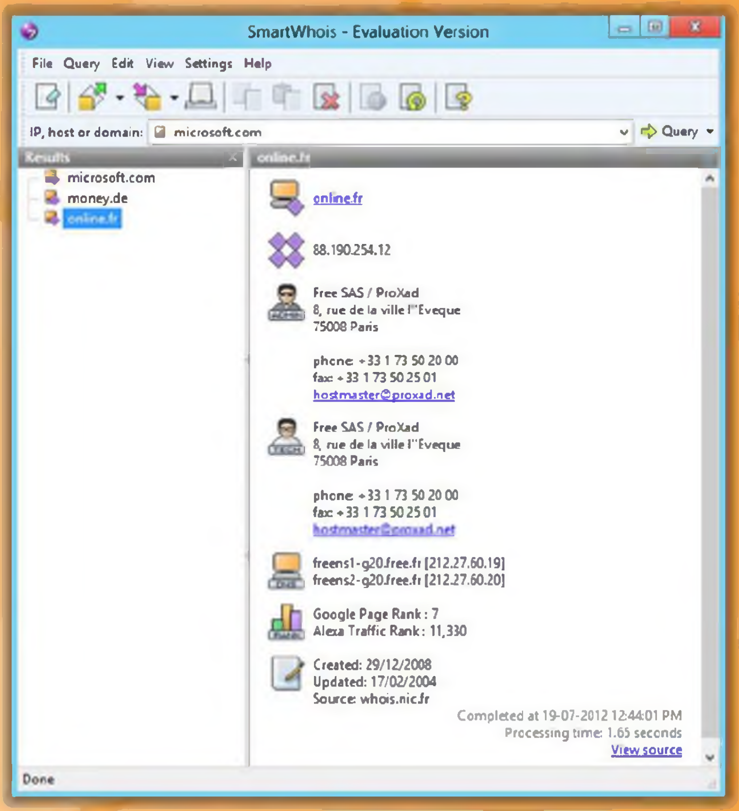
```
IP, host or domain: microsoft.com

microsoft.com
money.de
online.fr

online.fr

88.190.254.12

Free SAS / ProXad
8, rue de la ville l'"Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

Free SAS / ProXad
8, rue de la ville l'"Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

freens1-g20.free.fr [212.27.60.19]
freens2-g20.free.fr [212.27.60.20]

Google Page Rank: 7
Alexa Traffic Rank: 11,330

Created: 29/12/2008
Updated: 17/02/2004
Source: whois.nic.fr
                                Completed at 19-07-2012 12:44:01 PM
                                    Processing time: 1.65 seconds
                                                      View source
```

http://www.tamos.com

WHOIS Lookup Tool: SmartWhois

Source: http://www.tamos.com

SmartWhois is a useful **network information** utility that allows you to look up all the available information about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator, and technical support contact information. It also assists you in finding the owner of the domain, the owner's contact information, the owner of the **IP address block**, registered date of the domain, etc.


SmartWhois - Evaluation Version
File Query Edit View Settings Help
Query
Results
online.fr
Done

IP, host or domain: microsoft.com

microsoft.com
money.de
online.fr

online.fr

88.190.254.12

Free SAS / ProXad
8, rue de la ville l''Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

Free SAS / ProXad
8, rue de la ville l''Eveque
75008 Paris

phone: +33 1 73 50 20 00
fax: +33 1 73 50 25 01
hostmaster@proxad.net

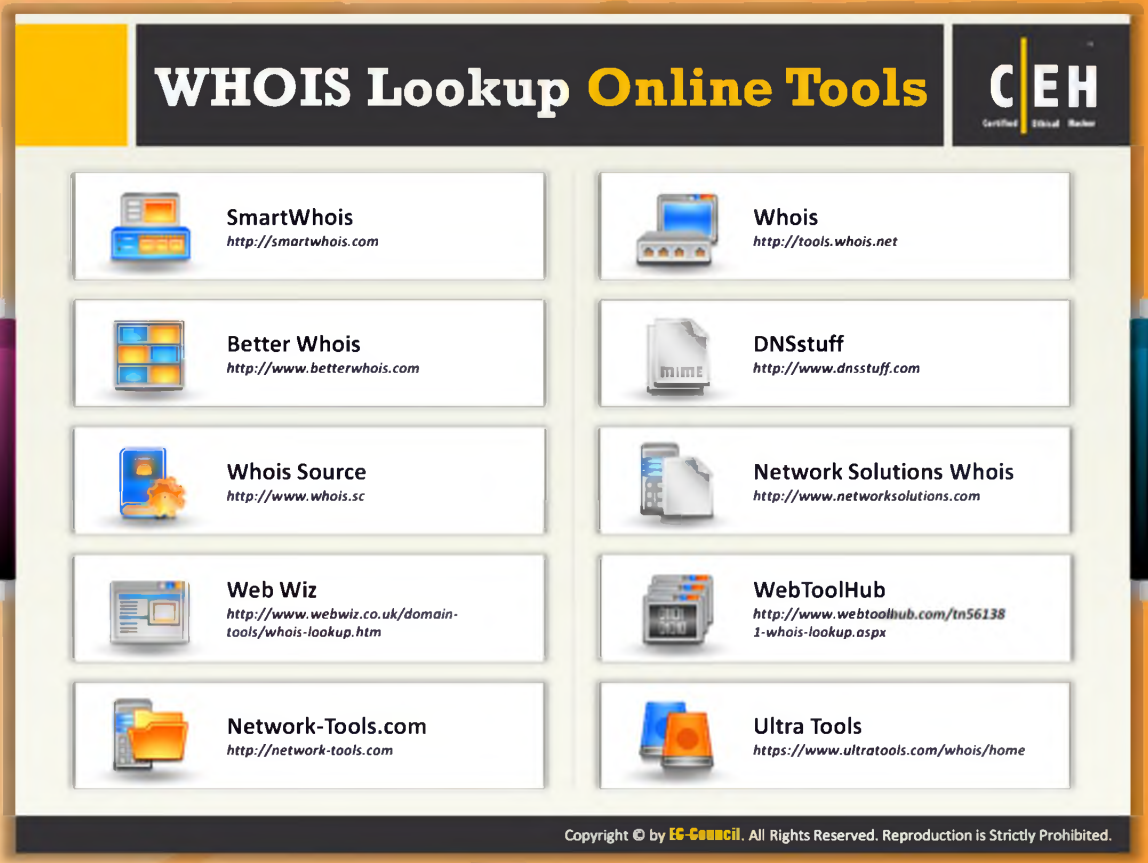
freens1-g20.free.fr [212.27.60.19]
freens2-g20.free.fr [212.27.60.20]

Google Page Rank : 7
Alexa Traffic Rank : 11,330

Created: 29/12/2008
Updated: 17/02/2004
Source: whois.nic.fr

Completed at 19-07-2012 12:44:01 PM
Processing time: 1.65 seconds
View source

FIGURE 2.31: SmartWhois screenshot



WHOIS Lookup Online Tools

SmartWhois
http://smartwhois.com

Better Whois
http://www.betterwhois.com

Whois Source
http://www.whois.sc

Web Wiz
http://www.webwiz.co.uk/domain-tools/whois-lookup.htm

Network-Tools.com
http://network-tools.com

Whois
http://tools.whois.net

DNSstuff
http://www.dnsstuff.com

Network Solutions Whois
http://www.networksolutions.com

WebToolHub
http://www.webtoolhub.com/tn561381-whois-lookup.aspx

Ultra Tools
https://www.ultratools.com/whois/home

WHOIS Lookup Tools

Similar to SmartWhois, there are numerous tools available in the market to retrieve Whois information. A few are mentioned as follows:

CountryWhois

Source: http://www.tamos.com

CountryWhois is a utility for identifying the geographic location of an IP address. CountryWhois can be used to analyze server logs, check email address headers, identify online credit card fraud, or in any other instance where you need to quickly and accurately determine the country of origin by IP address.

LanWhoIs

Source: http://lantricks.com

LanWhoIs provides information about domains and addresses on the Internet. This program helps you determine who, where, and when the domain or site you are interested in was registered, and the information about those who support it now. This tool allows you to save your search result in the form of an archive to view it later. You can print and save the search result in HTML format.

Batch IP Converter

Source: http://www.networkmost.com

Batch IP Converter is a network tool to work with IP addresses. It combines Domain-to-IP Converter, Batch Ping, Tracert, Whois, Website Scanner, and Connection Monitor into a single interface as well as an **IP-to-Country Converter**. It allows you to look up the IP address for a single or list of domain names and vice versa.

CallerIP

Source: http://www.callerippro.com

CallerIP is basically IP and port monitoring software that displays the incoming and outgoing connection made to your computer. It also allows you to find the origin of all connecting IP addresses on the world map. The Whois reporting feature provides key information such as who an IP is registered to along with **contact email addresses** and **phone numbers**.

WhoIs Lookup Multiple Addresses

Source: http://www.sobolsoft.com

This software offers a solution for users who want to **look up ownership details** for one or more IP addresses. Users can simply enter **IP addresses** or load them from a file. There are three options for lookup sites: whois.domaintools.com, whois-search.com, and whois.arin.net. The user can set a delay period between lookups, to avoid lockouts from these websites. The resulting list shows the IP addresses and details of each. It also allows you to save results to a text file.

WhoIs Analyzer Pro

Source: http://www.whoisanalyzer.com

This tool allows you to access information about a **registered domain worldwide**; you can view the domain owner name, domain name, and contact details of domain owner. It also helps in finding the location of a specific domain. You can also submit multiple queries with this tool simultaneously. This tool gives you the ability to print or save the result of the query in **HTML format**.

HotWhois

Source: http://www.tialsoft.com

HotWhois is an IP tracking tool that can **reveal valuable information**, such as country, state, city, address, contact phone numbers, and email addresses of an IP provider. The query mechanism resorts to a variety of Regional Internet Registries, to obtain IP Whois information about IP address. With HotWhois you can make whois queries even if the registrar, supporting a particular domain, doesn't have the **whois server itself**.

Whois 2010 Pro

Source: http://lapshins.com

Whois 2010 PRO is **network information software** that allows you to look up all the available information about a domain name, including country, state or province, city, administrator, and technical support contact information.

ActiveWhois

Source: http://www.johnru.com

ActiveWhois is a network tool to find information about the owners of IP addresses or Internet domains. You can determine the country, personal and postal addresses of the owner, and/or users of IP addresses and domains.

WhoisThisDomain

Source: http://www.nirsoft.net

WhoisThisDomain is a domain registration lookup utility that allows you to get information about a registered domain. It automatically connects to the right WHOIS server and retrieves the WHOIS record of the domain. It supports both generic domains and country code domains.

WHOIS Lookup Online Tools

SmartWhois
http://smartwhois.com

Whois
http://tools.whois.net

Better Whois
http://www.betterwhois.com

DNSstuff
http://www.dnsstuff.com

Whois Source
http://www.whois.sc

Network Solutions Whois
http://www.networksolutions.com

Web Wiz
http://www.webwiz.co.uk/domain-tools/whois-lookup.htm

WebToolHub
http://www.webtoolhub.com/tn561381-whois-lookup.aspx

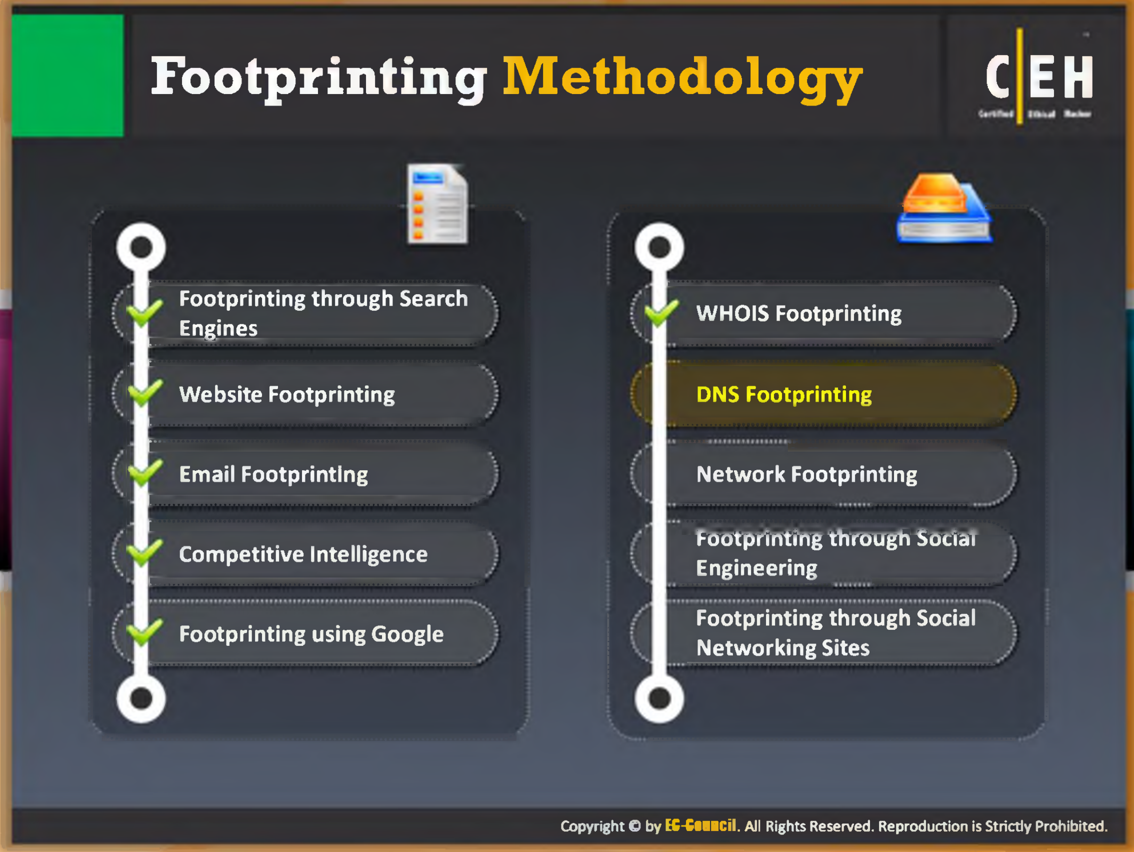
Network-Tools.com
http://network-tools.com

Ultra Tools
https://www.ultratools.com/whois/home

WHOIS Lookup Online Tools

In addition to the Whois lookup tools mentioned so far, a few online Whois lookup tools are listed as follows:

- SmartWhois available at http://smartwhois.com
- Better Whois available at http://www.betterwhois.com
- Whois Source available at http://www.whois.sc
- Web Wiz available at http://www.webwiz.co.uk/domain-tools/whois-lookup.htm
- Network-Tools.com available at http://network-tools.com
- Whois available at http://tools.whois.net
- DNSstuff available at http://www.dnsstuff.com
- Network Solutions Whois available at http://www.networksolutions.com
- WebToolHub available at http://www.webtoolhub.com/tn561381-whois-lookup.aspx
- Ultra Tools available at https://www.ultratools.com/whois/home



Footprinting Methodology

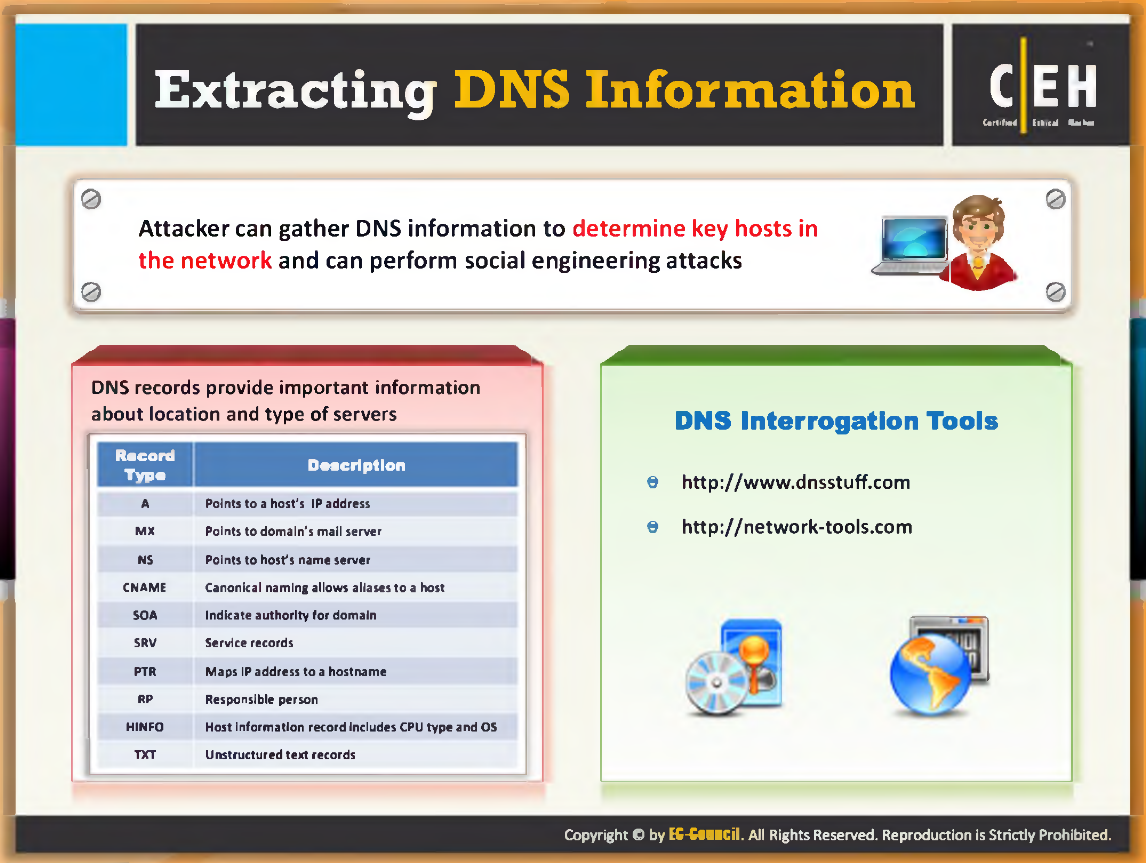
- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprintlng
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- ✓ WHOIS Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

The next phase in footprinting methodology is DNS footprinting.

This section describes how to extract DNS information and the **DNS interrogation** tools.



Extracting DNS Information

CEH
Certified Ethical Hacker

Attacker can gather DNS information to determine key hosts in the network and can perform social engineering attacks

DNS records provide important information about location and type of servers

Record Type	Description
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
TXT	Unstructured text records

DNS Interrogation Tools

- http://www.dnsstuff.com
- http://network-tools.com

Extracting DNS Information

DNS footprinting allows you to obtain information about **DNS zone data**. This DNS zone data includes DNS domain names, computer names, IP addresses, and much more about a particular network. The attacker performs **DNS footprinting** on the target network in order to obtain the information about DNS. He or she then uses the gathered DNS information to determine key hosts in the network and then performs social engineering attacks to gather more information.

DNS footprinting can be performed using DNS interrogation tools such as www.DNSstuff.com. By using www.DNSstuff.com, it is possible to extract DNS information about IP addresses, mail server extensions, DNS lookups, Whois lookups, etc. If you want information about a target company, it is possible to extract its range of IP addresses utilizing the **IP routing** lookup of DNS stuff. If the target network allows unknown, unauthorized users to transfer DNS zone data, then it is easy for you to obtain the information about DNS with the help of the DNS interrogation tool.

Once you send the query using the DNS interrogation tool to the **DNS server**, the server will respond to you with a record structure that contains information about the target DNS. DNS records provide important information about location and type of servers.

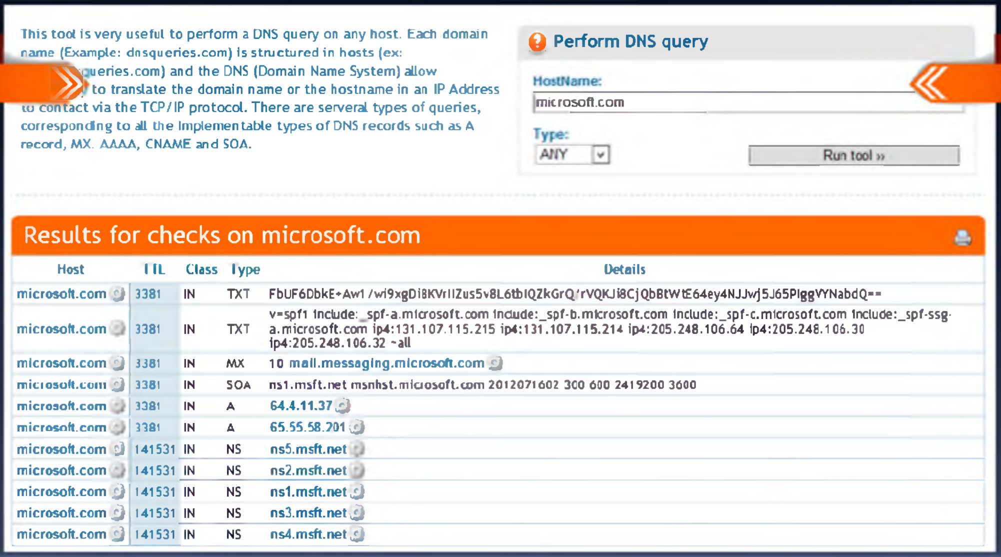
- A - Points to a host's IP address

- 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

A few more examples of DNS interrogation tools to send a DNS query include:

- http://www.dnsstuff.com
- http://network-tools.com

Extracting DNS Information (Cont'd)



This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: ...queries.com) and the DNS (Domain Name System) allow ... to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are serveral types of queries, corresponding to all the implementable types of DNS records such as A record, MX. AAAA, CNAME and SOA.

Perform DNS query

HostName: microsoft.com

Type: ANY

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJvj5J65PIggVYNabdQ==
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

http://www.dnsqueries.com

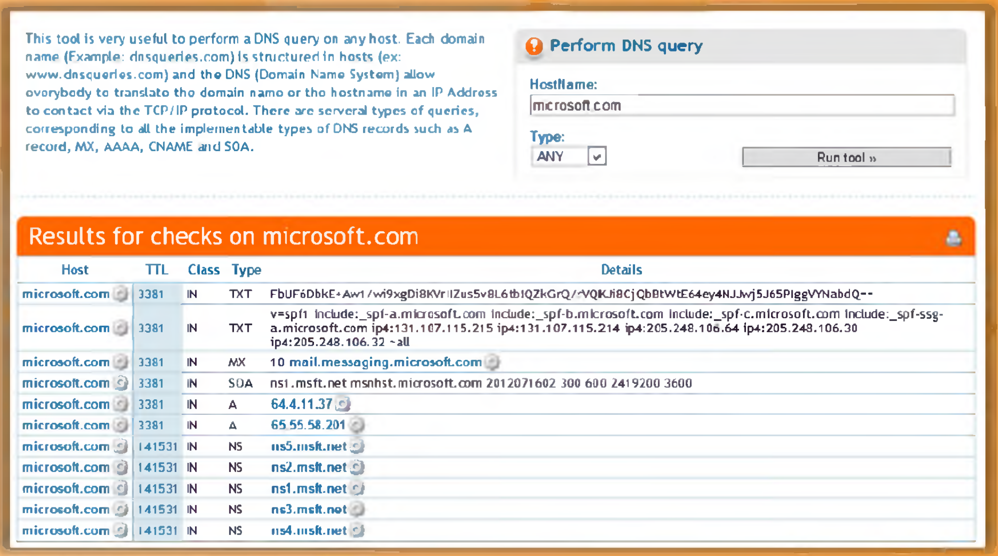
Extracting DNS Information (Cont'd)

Source: http://www.dnsqueries.com

Perform DNS query available at http://www.dnsqueries.com is a tool that allows you to perform a DNS query on any host. Each domain name (example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allows anyone to translate the domain name or the hostname in an IP address to contact via the TCP/IP protocol. There are several types of queries, corresponding to all the implementable types of DNS records such as a record, MX, AAAA, CNAME, and SOA.

Now let's see how the DNS interrogation tool retrieves information about the DNS. Go to the browser and type http://www.dnsqueries.com and press Enter. The DNS query's homesite will be displayed in the browser.

Enter the domain name of your interest in the Perform DNS query's HostName field (here we are entering Microsoft.com) and click the Run tool button; the DNS information for Microsoft.com will be displayed as shown in the following figure.



This tool is very useful to perform a DNS query on any host. Each domain name (Example: dnsqueries.com) is structured in hosts (ex: www.dnsqueries.com) and the DNS (Domain Name System) allow everybody to translate the domain name or the hostname in an IP Address to contact via the TCP/IP protocol. There are serveral types of queries, corresponding to all the implementable types of DNS records such as A record, MX, AAAA, CNAME and SOA.

Perform DNS query

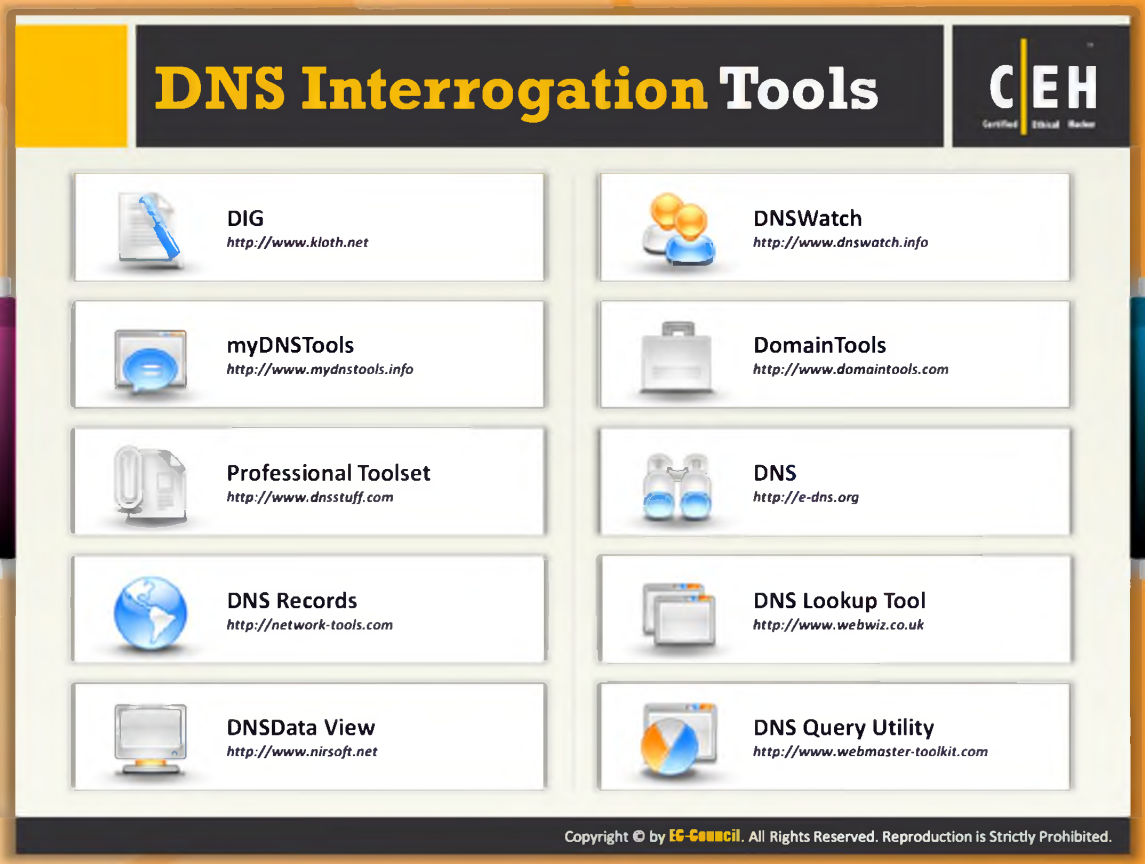
HostName: microsoft.com

Type: ANY

Results for checks on microsoft.com

Host	TTL	Class	Type	Details
microsoft.com	3381	IN	TXT	FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/+VQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVYNabdQ--
microsoft.com	3381	IN	TXT	v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com include:_spf-ssg-a.microsoft.com ip4:131.107.115.215 ip4:131.107.115.214 ip4:205.248.106.64 ip4:205.248.106.30 ip4:205.248.106.32 ~all
microsoft.com	3381	IN	MX	10 mail.messaging.microsoft.com
microsoft.com	3381	IN	SOA	ns1.msft.net msnhst.microsoft.com 2012071602 300 600 2419200 3600
microsoft.com	3381	IN	A	64.4.11.37
microsoft.com	3381	IN	A	65.55.58.201
microsoft.com	141531	IN	NS	ns5.msft.net
microsoft.com	141531	IN	NS	ns2.msft.net
microsoft.com	141531	IN	NS	ns1.msft.net
microsoft.com	141531	IN	NS	ns3.msft.net
microsoft.com	141531	IN	NS	ns4.msft.net

FIGURE 2.32: Screenshot showing DNS information for Microsoft.com



DNS Interrogation Tools

DIG
http://www.kloth.net

myDNSTools
http://www.mydnstools.info

Professional Toolset
http://www.dnsstuff.com

DNS Records
http://network-tools.com

DNSData View
http://www.nirsoft.net

DNSWatch
http://www.dnswatch.info

DomainTools
http://www.domaintools.com

DNS
http://e-dns.org

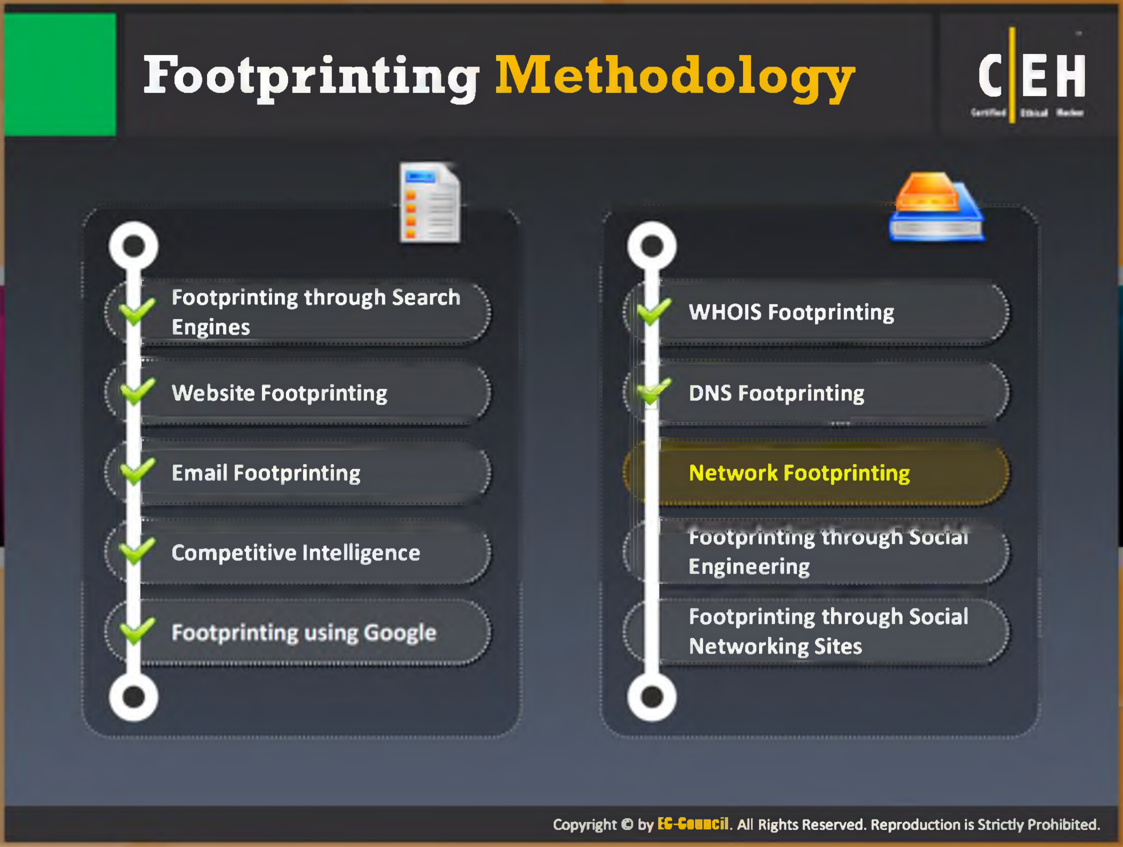
DNS Lookup Tool
http://www.webwiz.co.uk

DNS Query Utility
http://www.webmaster-toolkit.com

DNS Interrogation Tools

A few more well-known DNS interrogation tools are listed as follows:

- DIG available at http://www.kloth.net
- myDNSTools available at http://www.mydnstools.info
- Professional Toolset available at http://www.dnsstuff.com
- DNS Records available at http://network-tools.com
- DNSData View available athttp://www.nirsoft.net
- DNSWatch available at http://www.dnswatch.info
- DomainTools Pro available at http://www.domaintools.com
- DNS available at http://e-dns.org
- DNS Lookup Tool available at http://www.webwiz.co.uk
- DNS Query Utility available at http://www.webmaster-toolkit.com



Footprinting Methodology

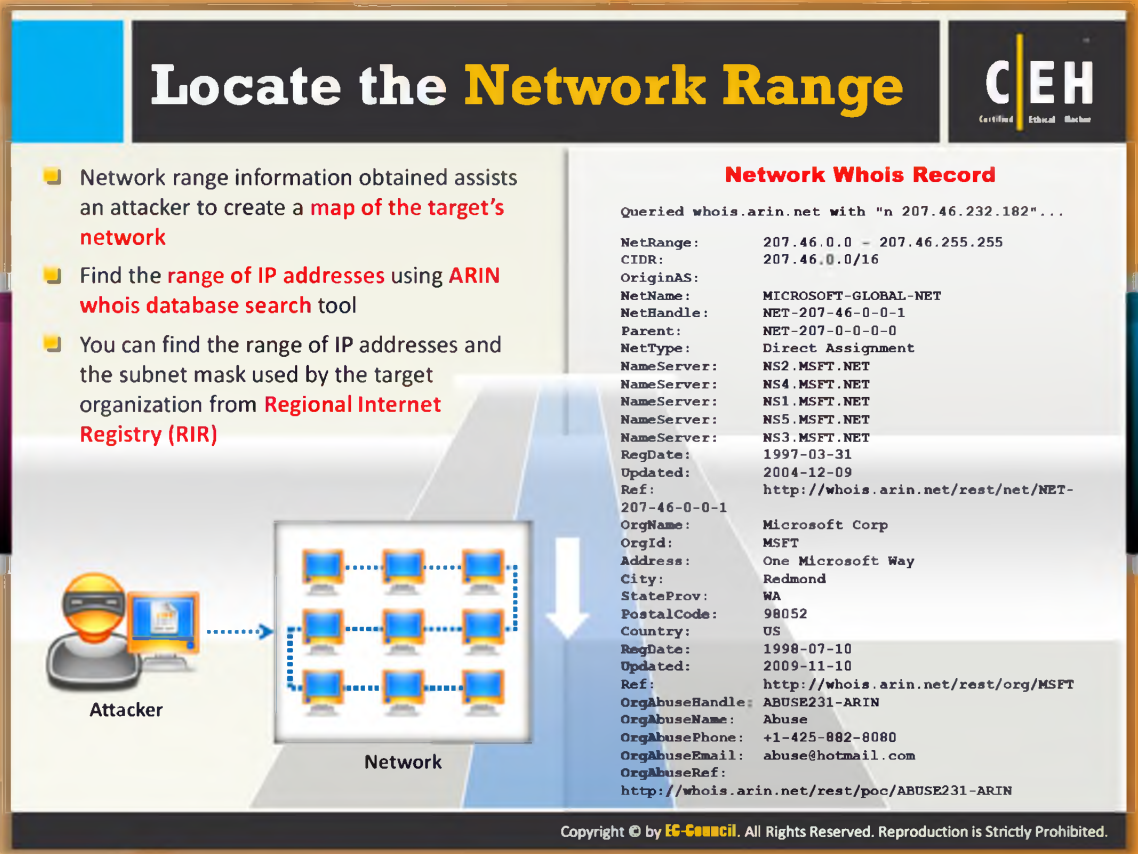
- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- ✓ WHOIS Footprinting
- ✓ DNS Footprinting
- **Network Footprinting**
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

The next step after retrieving the DNS information is to gather network-related information. So, now we will discuss network footprinting, a method of gathering network-related information.

This section describes how to locate network range, determine the operating system, Traceroute, and the Traceroute tools.



Locate the Network Range

- Network range information obtained assists an attacker to create a map of the target's network
- Find the range of IP addresses using 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
```

Locate the Network Range

To perform network footprinting, you need to gather basic and important information about the target organization such as what the organization does, who they work for, and what type of work they perform. The answers to these questions give you an idea about the internal structure of the target network.

After gathering the aforementioned information, an attacker can proceed to find the network range of a target system. He or she can get more detailed information from the appropriate regional registry database regarding IP allocation and the nature of the allocation. An attacker can also determine the subnet mask of the domain. He or she can also trace the route between the system and the target system. Two popular traceroute tools are NeoTrace and Visual Route.

Obtaining private IP addresses can be useful for an attacker. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private Internets: 10.0.0.0–10.255.255.255 (10/8 prefix), 172.16.0.0–172.31.255.255 (172.16/12 prefix), and 192.168.0.0–192.168.255.255 (192.168/16 prefix).

The network range gives you an idea about how the network is, which machines in the networks are alive, and it helps to identify the network topology, access control device, and OS used in the target network. To find the **network range** of the target network, enter the server IP address (that was gathered in **WHOIS footprinting**) in the ARIN whois database search tool or you can go to the ARIN website (https://www.arin.net/knowledge/rirs.html) and enter the server IP in the SEARCH Whois text box. You will get the network range of the target network. If the DNS servers are not set up correctly, the attacker has a good chance of obtaining a list of internal machines on the server. Also, sometimes if an attacker traces a route to a machine, he or she can get the internal IP address of the **gateway**, which might be useful.

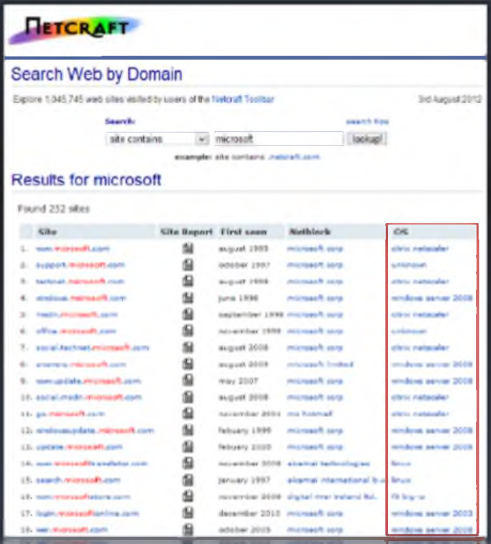
Network Whois Record

```
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
```

You need to use more than one tool to obtain network information as sometimes a single tool is not capable of delivering the information you want.

Determine the Operating System

Use the Netcraft tool to determine the OSes in use by the target organization



Search Web by Domain

Explore 1,045,745 web sites visited by users of the Netcraft Toolbar 3rd August 2012

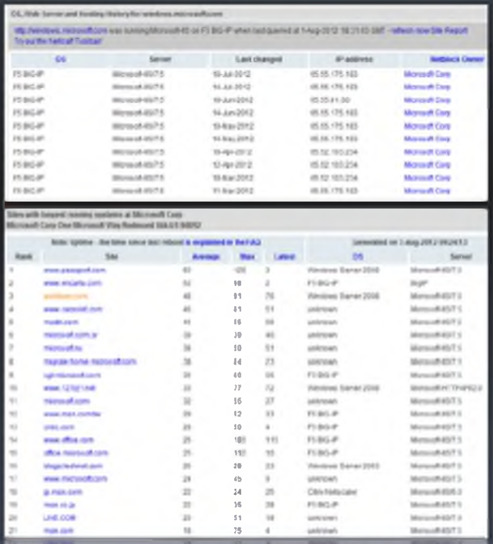
Search: site contains microsoft lookup!

example: site contains .netcraft.com

Results for microsoft

Found 232 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.microsoft.com		august 1995	microsoft corp	citrix netscaler
2.	support.microsoft.com		october 1997	microsoft corp	unknown
3.	technet.microsoft.com		august 1999	microsoft corp	citrix netscaler
4.	windows.microsoft.com		june 1998	microsoft corp	windows server 2008
5.	msdn.microsoft.com		september 1998	microsoft corp	citrix netscaler
6.	office.microsoft.com		november 1999	microsoft corp	unknown
7.	social.technet.microsoft.com		august 2008	microsoft corp	citrix netscaler
8.	answers.microsoft.com		august 2009	microsoft limited	windows server 2008
9.	www.update.microsoft.com		may 2007	microsoft corp	windows server 2008
10.	social.msdn.microsoft.com		august 2008	microsoft corp	citrix netscaler
11.	go.microsoft.com		november 2001	msn hotmail	citrix netscaler
12.	windowsupdate.microsoft.com		febuary 1999	microsoft corp	windows server 2008
13.	update.microsoft.com		febuary 2000	microsoft corp	windows server 2008
14.	[illegible]		november 2008	akamai technologies	linux
15.	search.microsoft.com		january 1997	akamai international b.v.	linux
16.	www.microsoftstore.com		november 2008	digital river ireland ltd.	f5 big-ip
17.	login.microsoftonline.com		december 2010	microsoft corp	windows server 2003
18.	ww.microsoft.com		october 2005	microsoft corp	windows server 2008



OS, Web Server and Hosting History for windows.microsoft.com

http://windows.microsoft.com was running Microsoft-IIS on F5 BIG-IP when last queried at 1-Aug-2012 18:21:03 GMT - refresh now Site Report

Try out the Netcraft Toolbar!

OS	Server	Last changed	IP address	Netblock Owner
F5 BIG-IP	Microsoft-IIS/7.5	19-Jul-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-Jul-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-Jun-2012	65.55.61.30	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-Jun-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-May-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-May-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	12-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	19-Mar-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	11-Mar-2012	65.55.175.183	Microsoft Corp

Sites with longest running systems at Microsoft Corp

Microsoft Corp One Microsoft Way Redmond WA US 98052

Note: uptime - the time since last reboot - is explained in the FAQ

Generated on 1-Aug-2012 09:24:13

Rank	Site	Average	Max	Latest	OS	Server
1	www.passport.com	61	120	3	Windows Server 2008	Microsoft-IIS/7.5
2	www.encarta.com	52	18	2	F5 BIG-IP	BigIP
3	[illegible]	48	81	76	Windows Server 2008	Microsoft-IIS/7.5
4	www.netmeeting.com	45	81	51	unknown	Microsoft-IIS/7.5
5	msdn.com	41	16	59	unknown	Microsoft-IIS/7.5
6	microsoft.com.br	39	39	40	unknown	Microsoft-IIS/7.5
7	microsoft.eu	38	10	51	unknown	Microsoft-IIS/7.5
8	[illegible]	38	14	23	unknown	Microsoft-IIS/7.5
9	[illegible]	34	40	55	F5 BIG-IP	Microsoft-IIS/7.5
10	[illegible]	33	77	72	Windows Server 2008	Microsoft-HTTPAPI/2.0
11	microsoft.com	32	16	27	unknown	Microsoft-IIS/7.5
12	www.msn.com.tw	29	12	33	F5 BIG-IP	Microsoft-IIS/7.5
13	[illegible]	25	10	4	F5 BIG-IP	Microsoft-IIS/7.5
14	www.office.com	25	188	111	F5 BIG-IP	Microsoft-IIS/7.5
15	office.microsoft.com	25	112	55	F5 BIG-IP	Microsoft-IIS/7.5
16	[illegible]	25	28	23	Windows Server 2003	Microsoft-IIS/7.5
17	www.microsoft.com	24	45	9	unknown	Microsoft-IIS/7.5
18	jp.msn.com	22	24	25	Citrix Netscaler	Microsoft-IIS/6.0
19	msn.co.jp	22	16	28	F5 BIG-IP	Microsoft-IIS/7.5
20	LIVE.COM	22	51	18	unknown	Microsoft-IIS/7.5
21	msn.com	18	75	4	unknown	Microsoft-IIS/7.5

http://news.netcraft.com

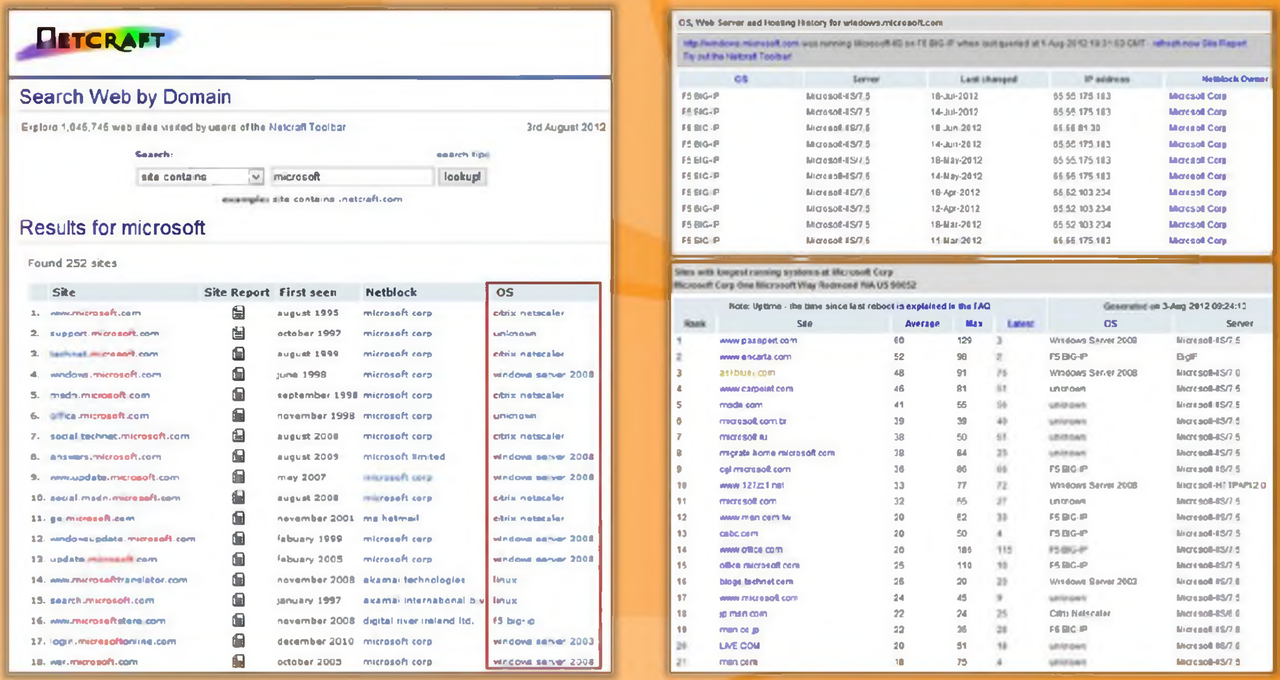
Determine the Operating System

Source: http://news.netcraft.com

So far we have collected information about IP addresses, network ranges, server names, etc. of the target network. Now it's time to find out the **OS running** on the **target network**. The technique of obtaining information about the target network OS is called **OS fingerprinting**. The Netcraft tool will help you to find out the OS running on the target network.

Let's see how Netcraft helps you deter,ome the OS of the target network.

Open the http://news.netcraft.com site in your browser and type the domain name of your target network in the What's that site running? field (here we are considering the domain name "Microsoft.com"). It displays all the **sites associated** with that domain along with the operating system running on each site.



Search Web by Domain

Explore 1,046,746 web sites visited by users of the Netcraft Toolbar — 3rd August 2012

Results for microsoft

Found 252 sites

	Site	Site Report	First seen	Netblock	OS
1.	www.microsoft.com		august 1995	microsoft corp	citrix netscaler
2.	support.microsoft.com		october 1997	microsoft corp	unknown
3.	technet.microsoft.com		august 1999	microsoft corp	citrix netscaler
4.	windows.microsoft.com		june 1998	microsoft corp	windows server 2008
5.	msdn.microsoft.com		september 1998	microsoft corp	citrix netscaler
6.	office.microsoft.com		november 1998	microsoft corp	unknown
7.	social.technet.microsoft.com		august 2008	microsoft corp	citrix netscaler
8.	answers.microsoft.com		august 2009	microsoft limited	windows server 2008
9.	www.update.microsoft.com		may 2007	microsoft corp	windows server 2008
10.	social.msdn.microsoft.com		august 2008	microsoft corp	citrix netscaler
11.	go.microsoft.com		november 2001	ms hotmail	citrix netscaler
12.	windowsupdate.microsoft.com		febuary 1999	microsoft corp	windows server 2008
13.	update.microsoft.com		febuary 2005	microsoft corp	windows server 2008
14.	www.microsofttranslator.com		november 2008	akamai technologies	linux
15.	search.microsoft.com		january 1997	akamai international b.v.	linux
16.	www.microsoftstore.com		november 2008	digital river ireland ltd.	f5 big-ip
17.	login.microsoftonline.com		december 2010	microsoft corp	windows server 2003
18.	ver.microsoft.com		october 2005	microsoft corp	windows server 2008

OS, Web Server and Hosting History for windows.microsoft.com

http://windows.microsoft.com was running Microsoft-IIS on F5 BIG-IP when last queried at 1-Aug-2012 19:31:53 GMT - refresh now Site Report
Try out the Netcraft Toolbar!

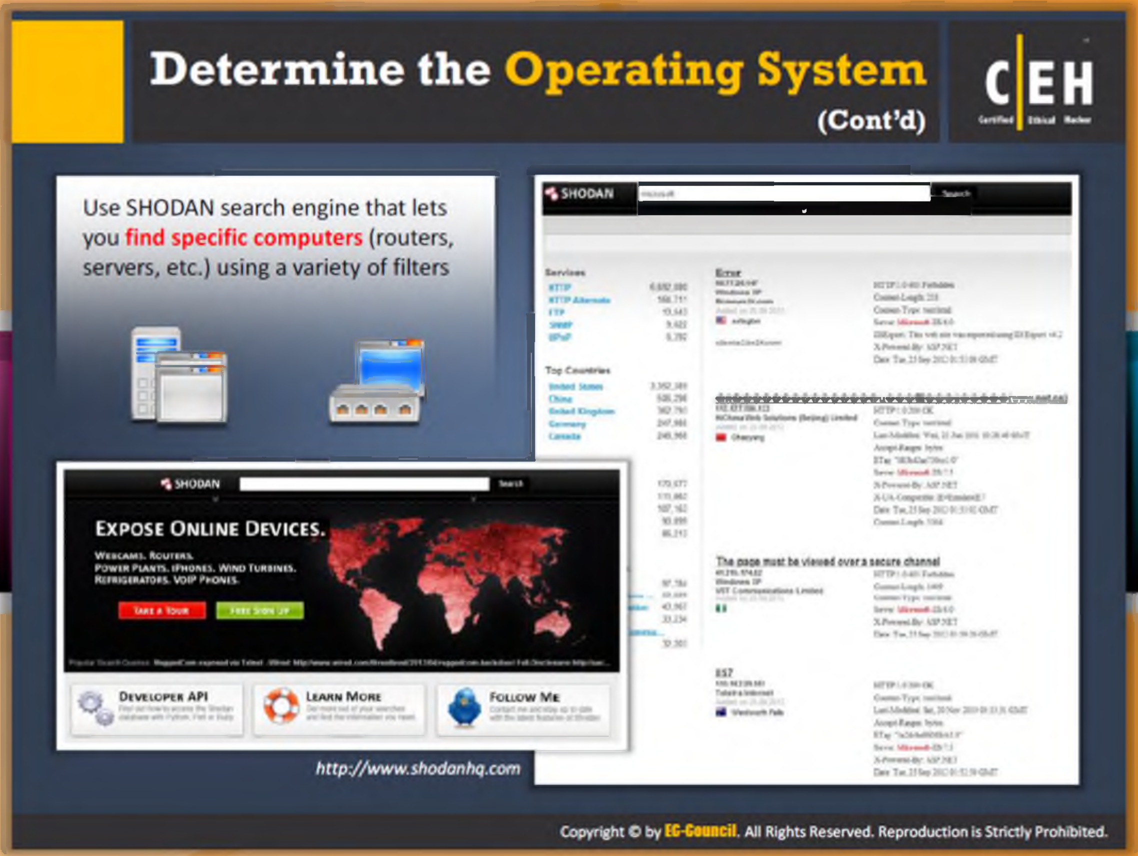
OS	Server	Last changed	IP address	Netblock Owner
F5 BIG-IP	Microsoft-IIS/7.5	18-Jul-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-Jul-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	18-Jun-2012	65.55.81.30	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-Jun-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	18-May-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	14-May-2012	65.55.175.183	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	18-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	12-Apr-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	18-Mar-2012	65.52.103.234	Microsoft Corp
F5 BIG-IP	Microsoft-IIS/7.5	11-Mar-2012	65.55.175.183	Microsoft Corp

Sites with longest running systems at Microsoft Corp
Microsoft Corp One Microsoft Way Redmond WA US 98052

Note: Uptime - the time since last reboot is explained in the FAQ
Generated on 3-Aug 2012 09:24:13

Rank	Site	Average	Max	Latest	OS	Server
1	www.passport.com	60	129	3	Windows Server 2008	Microsoft-IIS/7.5
2	www.encarta.com	52	98	2	F5 BIG-IP	BigIP
3	astbuei.com	48	91	75	Windows Server 2008	Microsoft-IIS/7.0
4	www.carpoint.com	46	81	51	unknown	Microsoft-IIS/7.5
5	msdn.com	41	55	56	unknown	Microsoft-IIS/7.5
6	microsoft.com.br	39	39	40	unknown	Microsoft-IIS/7.5
7	microsoft.ru	38	50	51	unknown	Microsoft-IIS/7.5
8	migrate.home.microsoft.com	38	84	25	unknown	Microsoft-IIS/7.5
9	cgl.microsoft.com	36	86	66	F5 BIG-IP	Microsoft-IIS/7.5
10	www.127z.1.net	33	77	72	Windows Server 2008	Microsoft-HTTPAPI/2.0
11	microsoft.com	32	65	27	unknown	Microsoft-IIS/7.5
12	www.msn.com.tw	20	62	33	F5 BIG-IP	Microsoft-IIS/7.5
13	cabc.com	20	50	4	F5 BIG-IP	Microsoft-IIS/7.5
14	www.office.com	26	186	115	F5 BIG-IP	Microsoft-IIS/7.5
15	office.microsoft.com	25	110	10	F5 BIG-IP	Microsoft-IIS/7.5
16	blogs.technet.com	26	20	23	Windows Server 2003	Microsoft-IIS/7.5
17	www.microsoft.com	24	45	9	unknown	Microsoft-IIS/7.5
18	jp.msn.com	22	24	25	Citrix Netscaler	Microsoft-IIS/6.0
19	msn.co.jp	22	36	28	F5 BIG-IP	Microsoft-IIS/7.5
20	LIVE.COM	20	51	10	unknown	Microsoft-IIS/7.0
21	msn.com	18	75	4	unknown	Microsoft-IIS/7.5

FIGURE 2.33: Netcraft showing the operating system that is in use by Microsoft



Determine the Operating System (Cont'd)

Use SHODAN search engine that lets you **find specific computers** (routers, servers, etc.) using a variety of filters

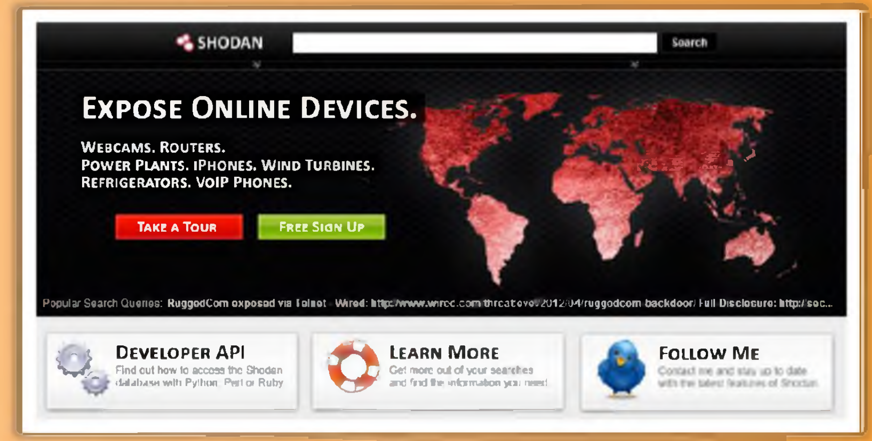
http://www.shodanhq.com

Determine the Operating System (Cont'd)

SHODAN Search Engine

Source: http://www.shodanhq.com

Use SHODAN search engine that lets you find specific computers (routers, servers, etc.) using a variety of filters.



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

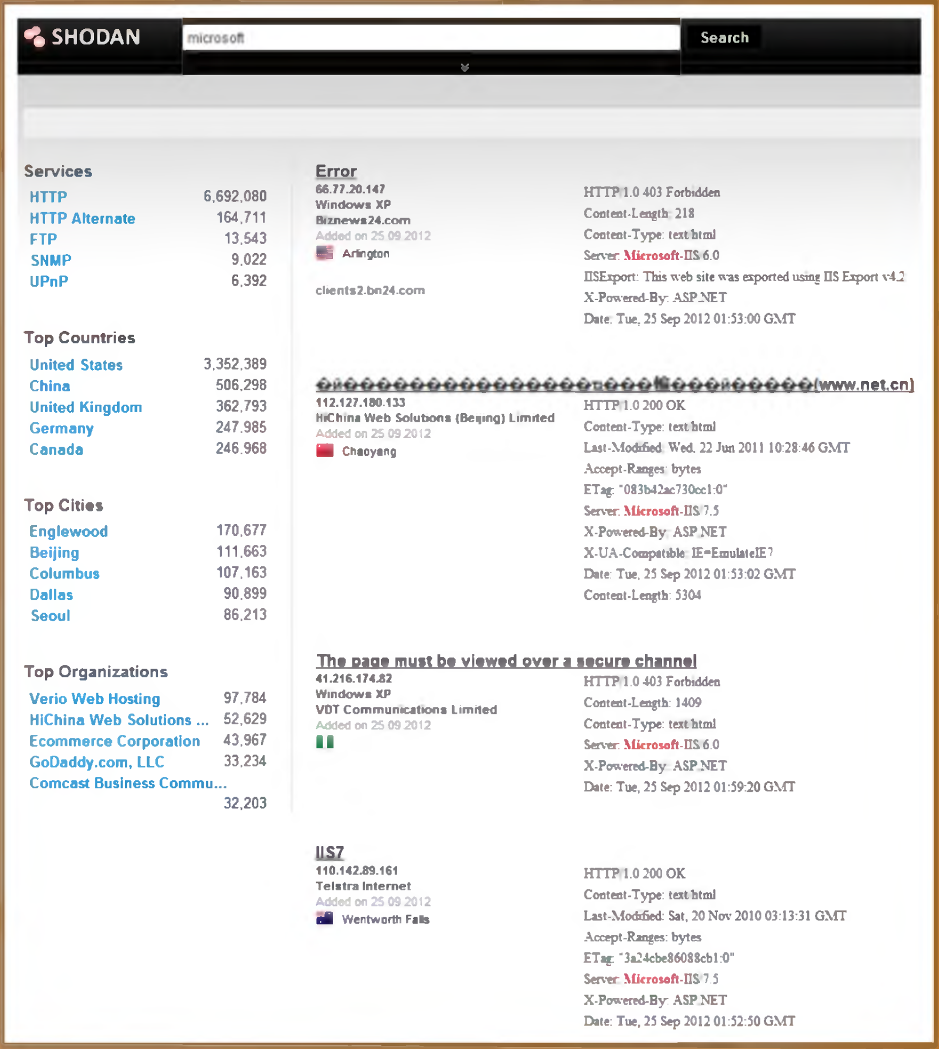
Popular Search Queries: RuggedCom exposed via Telnet - Wired: http://www.wired.com/threatlevel/2012/04/ruggedcom-backdoor/ Full Disclosure: http://sec...

DEVELOPER API
Find out how to access the Shodan database with Python, Perl or Ruby

LEARN MORE
Get more out of your searches and find the information you need

FOLLOW ME
Contact me and stay up to date with the latest features of Shodan

FIGURE 2.34: SHODAN Search Engine screenshot



Services

HTTP	6,692,080
HTTP Alternate	164,711
FTP	13,543
SNMP	9,022
UPnP	6,392

Top Countries

United States	3,352,389
China	506,298
United Kingdom	362,793
Germany	247,985
Canada	246,968

Top Cities

Englewood	170,677
Beijing	111,663
Columbus	107,163
Dallas	90,899
Seoul	86,213

Top Organizations

Verio Web Hosting	97,784
HiChina Web Solutions ...	52,629
Ecommerce Corporation	43,967
GoDaddy.com, LLC	33,234
Comcast Business Commu...	32,203

Error
66.77.20.147
Windows XP
Biznews24.com
Added on 25.09.2012
Arlington

clients2.bn24.com

```
HTTP/1.0 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
IISExport: This web site was exported using IIS Export v4.2
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 01:53:00 GMT
```

��������������������������(www.net.cn)
112.127.180.133
HiChina Web Solutions (Beijing) Limited
Added on 25.09.2012
Chaoyang

```
HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: Wed, 22 Jun 2011 10:28:46 GMT
Accept-Ranges: bytes
ETag: "083b42ac730cc1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
X-UA-Compatible: IE=EmulateIE7
Date: Tue, 25 Sep 2012 01:53:02 GMT
Content-Length: 5304
```

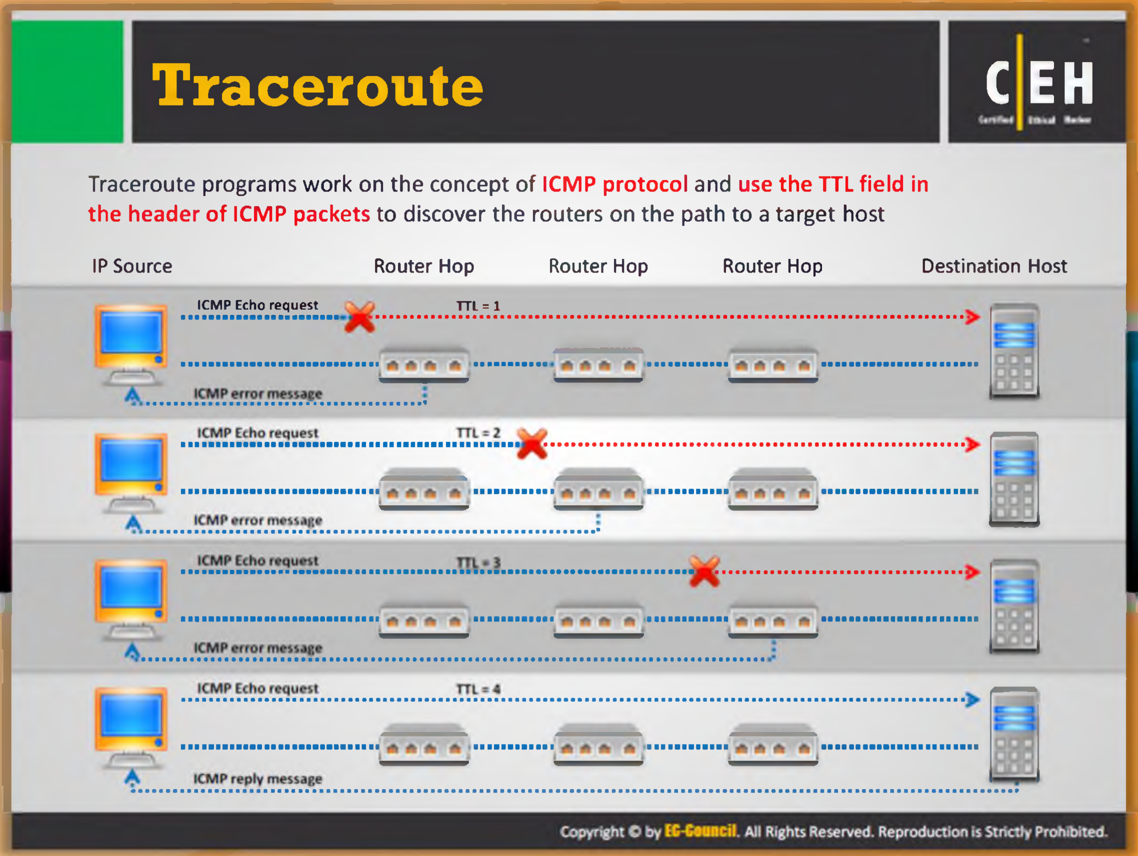
The page must be viewed over a secure channel
41.216.174.82
Windows XP
VDT Communications Limited
Added on 25.09.2012

```
HTTP/1.0 403 Forbidden
Content-Length: 1409
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 01:59:20 GMT
```

IIS7
110.142.89.161
Telstra Internet
Added on 25.09.2012
Wentworth Falls

```
HTTP/1.0 200 OK
Content-Type: text/html
Last-Modified: Sat, 20 Nov 2010 03:13:31 GMT
Accept-Ranges: bytes
ETag: "3a24cbe86088cb1:0"
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
Date: Tue, 25 Sep 2012 01:52:50 GMT
```

FIGURE 2.35: SHODAN screenshot



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

Finding the route of the target host is necessary to test against **man-in-the-middle attacks** and other relative attacks. Therefore, you need to find the route of the target host in the network. This can be accomplished with the help of the Traceroute utility provided with most operating systems. It allows you to trace the path or route through which the target host packets travel in the network.

Traceroute uses the **ICMP protocol** concept and **TTL (Time to Live)** field of IP header to find the path of the target host in the network.

The Traceroute utility can detail the path IP packets travel between two systems. It can trace the number of routers the packets travel through, the round trip time duration in transiting between two routers, and, if the routers have DNS entries, the names of the routers and their network affiliation, as well as the geographic location. It works by exploiting a feature of the Internet Protocol called **Time To Live (TTL)**. The TTL field is interpreted to indicate the maximum number of routers a packet may transit. Each router that handles a packet will decrement the TTL count field in the ICMP header by one. When the count reaches zero, the packet will be discarded and an error message will be transmitted to the originator of the packet.

It sends out a packet destined for the destination specified. It sets the TTL field in the packet to one. The first router in the path receives the packet, decrements the TTL value by one, and if the resulting TTL value is 0, it discards the packet and sends a message back to the originating host to inform it that the packet has been discarded. It records the **IP address** and **DNS name** of that router, and sends out another packet with a TTL value of two. This packet makes it through the first router, then times-out at the next router in the path. This second router also sends an error message back to the originating host. Traceroute continues to do this, and records the IP address and name of each router until a packet finally reaches the target host or until it decides that the host is unreachable. In the process, it records the time it took for each packet to travel round trip to each router. Finally, when it reaches the destination, the normal ICMP ping response will be send to the sender. Thus, this utility helps to reveal the IP addresses of the intermediate hops in the route of the target host from the source.

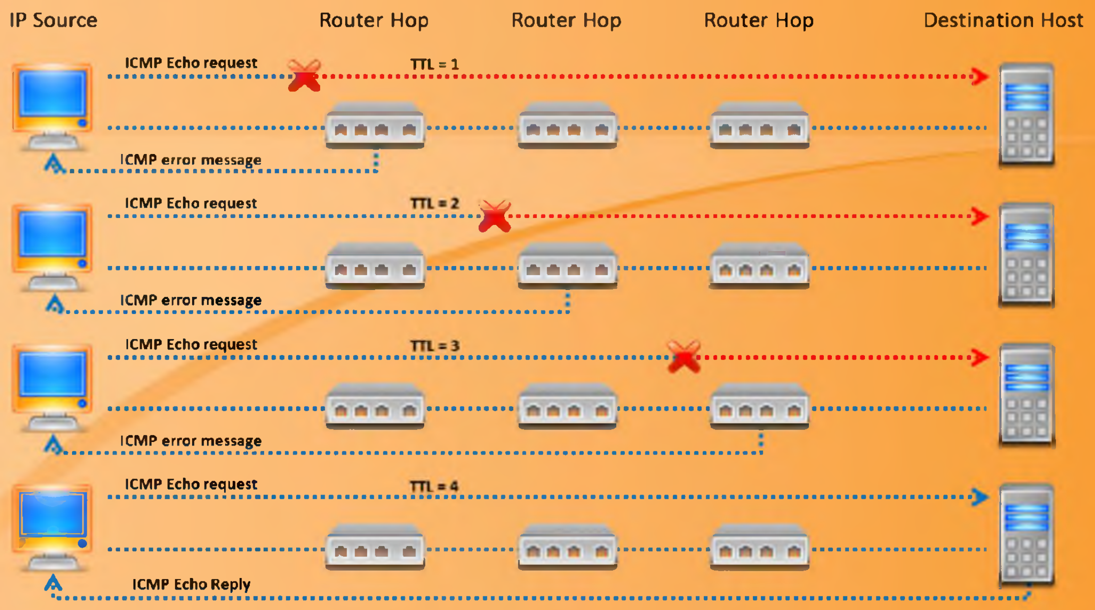


FIGURE 2.36: Working of Traceroute program

How to use the tracert command

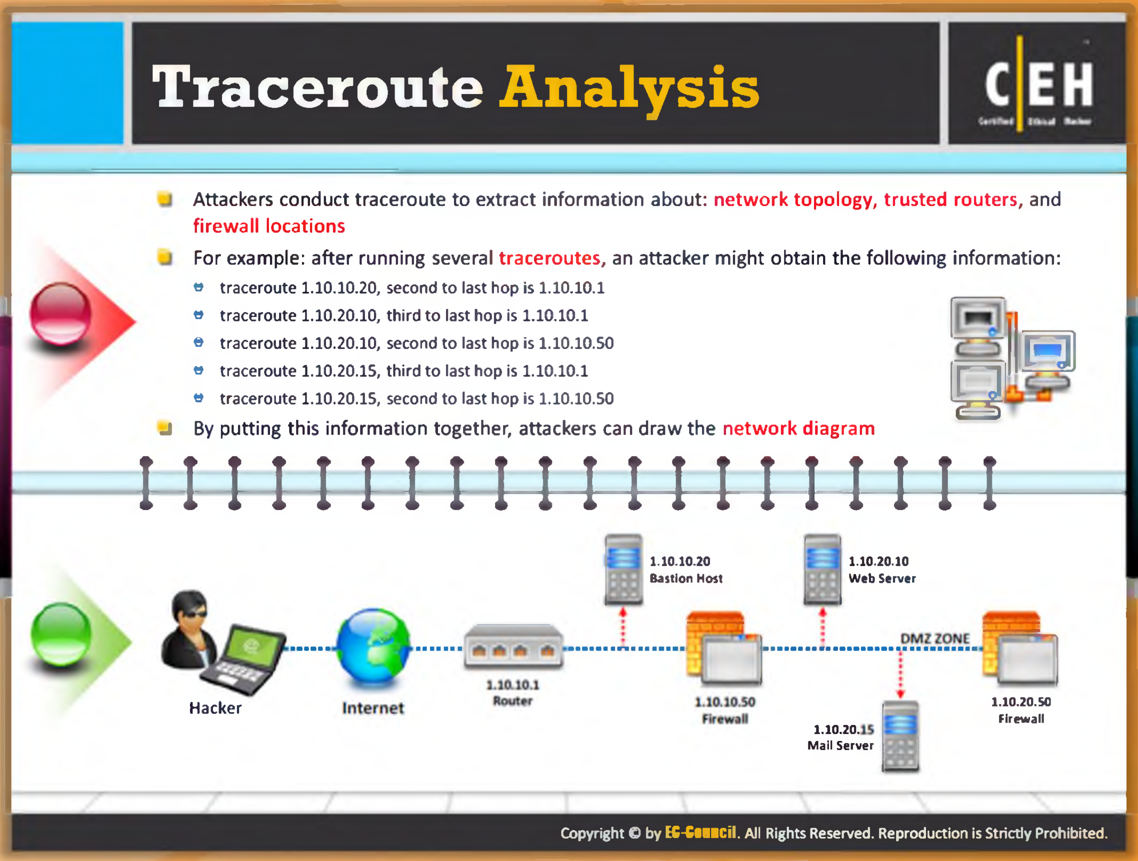
Go to the command prompt and type the `tracert` command along with destination IP address or domain name as follows:

```
C:\>tracert 216.239.36.10
```

Tracing route to ns3.google.com [216.239.36.10] over a maximum of 30 hops:

```
  1  1262 ms   186 ms   124 ms  195.229.252.10
  2  2796 ms  3061 ms  3436 ms  195.229.252.130
  3   155 ms   217 ms   155 ms  195.229.252.114
  4  2171 ms  1405 ms  1530 ms  194.170.2.57
  5  2685 ms  1280 ms   655 ms  dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
  6   202 ms   530 ms   999 ms  dxb-emix-rb.so100.emix.ae [195.229.0.230]
  7 609 ms  1124 ms  1748 ms  iar1-so-3-2-0.Thamesside.cw.net [166.63.214.65]
```

```
 8 1622 ms  2377 ms  2061 ms  eqixva-google-gige.google.com [206.223.115.21]
 9  2498 ms   968 ms   593 ms  216.239.48.193
 10  3546 ms  3686 ms  3030 ms  216.239.48.89
 11  1806 ms  1529 ms   812 ms  216.33.98.154
 12  1108 ms  1683 ms  2062 ms  ns3.google.com [216.239.36.10]
Trace complete.
```



Traceroute Analysis

- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- 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 1.10.10.1
  - 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
- By putting this information together, attackers can draw the network diagram

Traceroute Analysis

We have seen how the Traceroute utility helps you to find out the IP addresses of intermediate devices such as routers, firewalls, etc. present between source and destination. You can draw the network topology diagram by analyzing the Traceroute results. After running several traceroutes, you will be able to find out the location of a particular hop in the target network. Let's consider the following traceroute results obtained:

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

By analyzing these results, an attacker can draw the network diagram of the target network as follows:

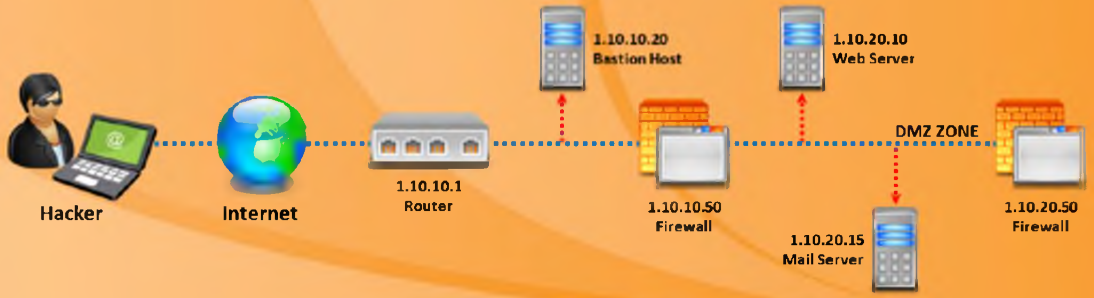
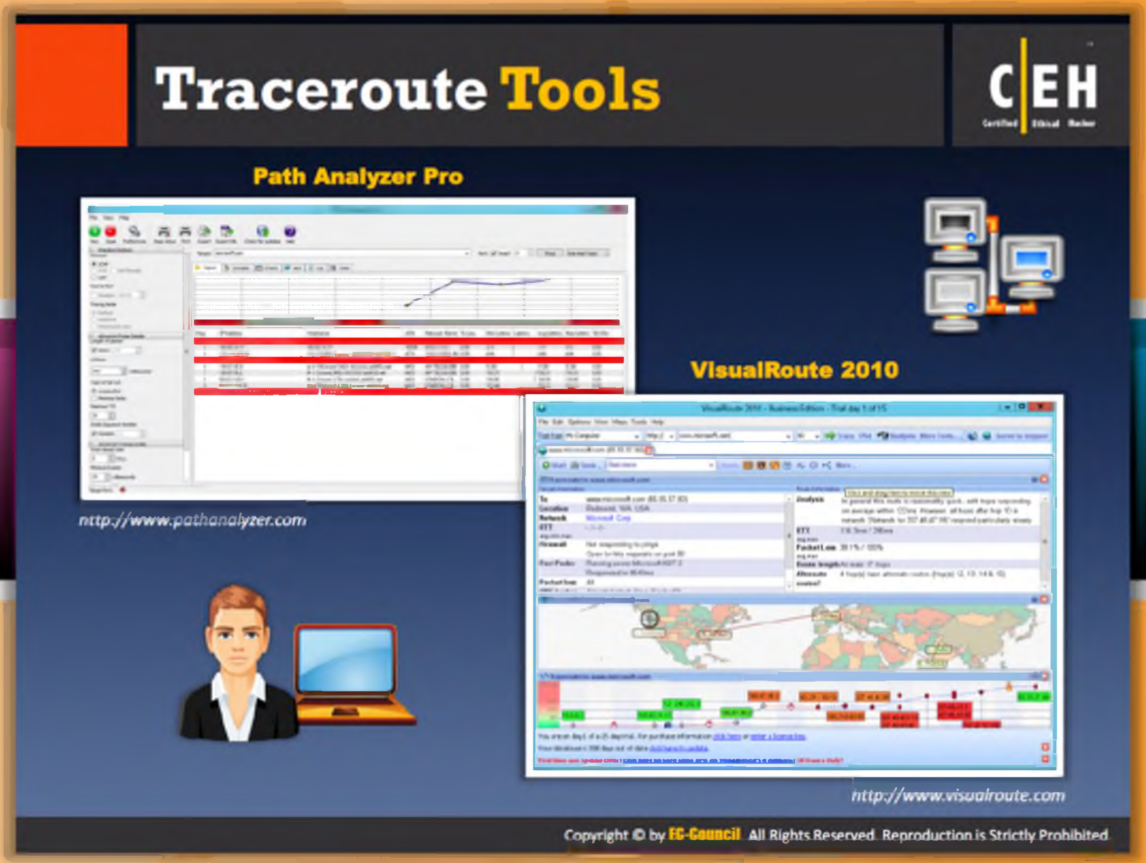


FIGURE 2.37: Diagrammatical representation of the target network



Traceroute Tools

Path Analyzer Pro

http://www.pathanalyzer.com

VisualRoute 2010

http://www.visualroute.com

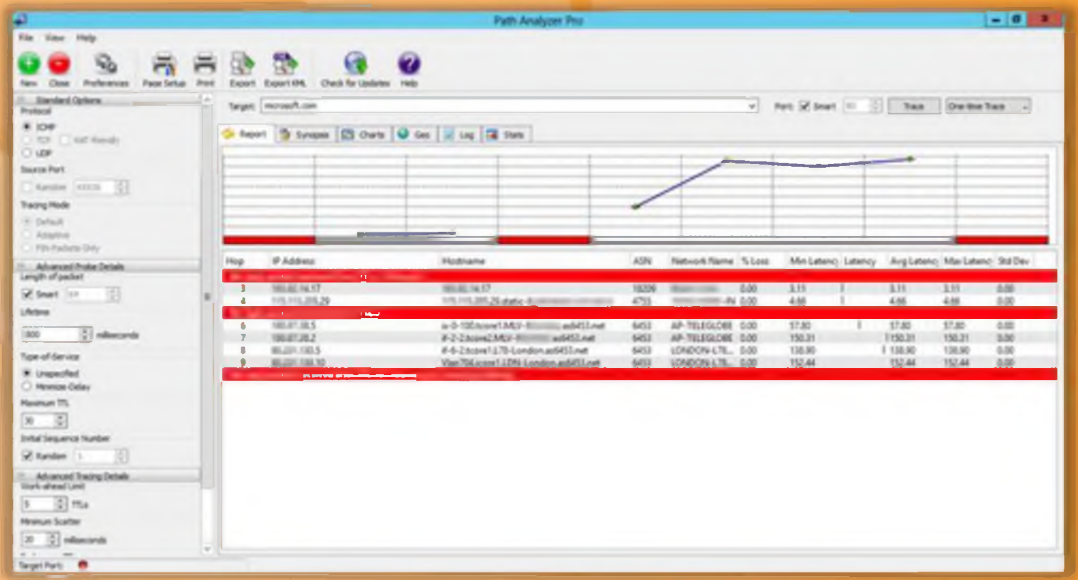
Traceroute Tools

Path Analyzer Pro and **VisualRoute 2010** are the two tools similar to Traceroute intended to traceroute the target host in a network.

Path Analyzer Pro

Source: http://www.pathanalyzer.com

Path Analyzer Pro is a **graphical-user-interface-based** trace routing tool that shows you the route from source to destination graphically. It also provides information such as the hop number, its IP address, hostname, ASN, network name, % loss, latency, avg. latency, and std. dev. about each hop in the path. You can also map the location of the IP address in the network with this tool. It allows you to detect filters, stateful firewalls, and other anomalies automatically in the network.



Hop	IP Address	Hostname	ASN	Network Name	% Loss	Min Latency	Latency	Avg Latency	Max Latency	Std Dev
3	180.82.14.17	180.82.14.17	18209	[illegible]	0.00	3.11		3.11	3.11	0.00
4	115.113.205.29	115.113.205.29.static-[illegible]	4755	[illegible]-IN	0.00	4.66		4.66	4.66	0.00
6	180.87.38.5	ix-0-100.tcore1.MLV-[illegible].as6453.net	6453	AP-TELEGLOBE	0.00	17.80		17.80	17.80	0.00
7	180.87.38.2	if-2-2.tcore2.MLV-[illegible].as6453.net	6453	AP-TELEGLOBE	0.00	150.31		150.31	150.31	0.00
8	80.231.130.5	if-6-2.tcore1.L78-London.as6453.net	6453	LONDON-L78...	0.00	138.90		138.90	138.90	0.00
9	80.231.130.10	Vlan704.icore1.LDN-London.as6453.net	6453	LONDON-L78...	0.00	152.44		152.44	152.44	0.00

FIGURE 2.38: Path Analyzer Pro screenshot

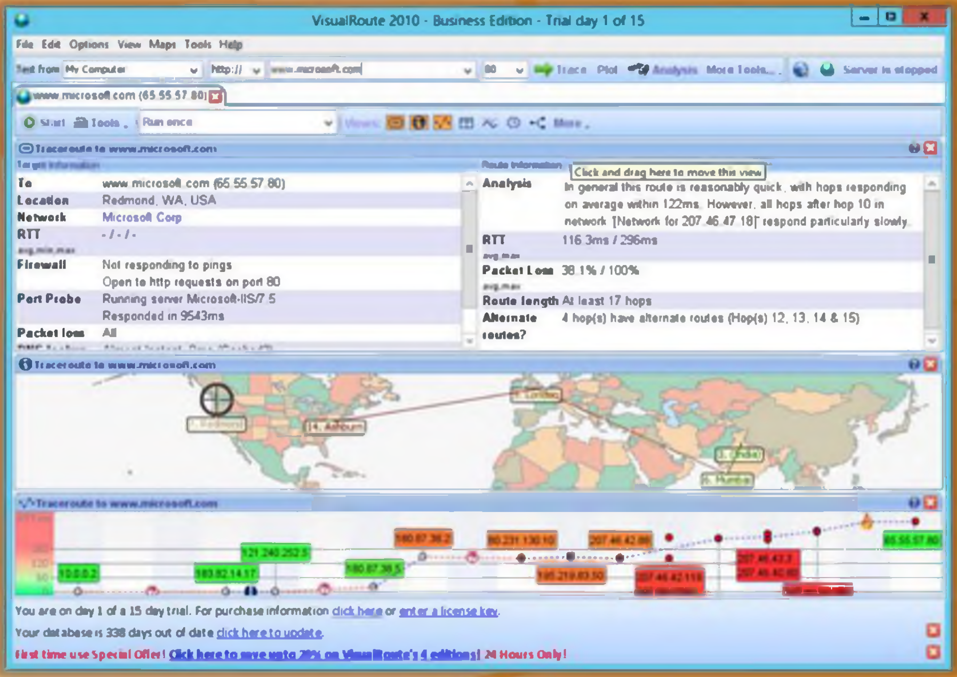
VisualRoute 2010

Source: http://www.visualroute.com

This is another graphical-user-based tracing tool that displays **hop-by-hop analysis**. It enables you to identify the geographical location of the routers, servers, and other IP devices. It is able to provide the **tracing information** in three forms: as an overall analysis, in a data table, and as a geographical view of the routing. The data table contains information such as hop number, IP address, node name, geographical location, etc. about each hop in the route.

Features:

- Hop-by-hop traceroutes
- Reverse tracing
- Historical analysis
- Packet loss reporting
- Reverse DNS
- Ping plotting
- Port probing
- Firefox and IE plugin



To	www.microsoft.com (65.55.57.80)
Location	Redmond, WA, USA
Network	Microsoft Corp
RTT avg,min,max	- / - / -
Firewall	Not responding to pings Open to http requests on port 80
Port Probe	Running server Microsoft-IIS/7.5 Responded in 9543ms
Packet loss	All

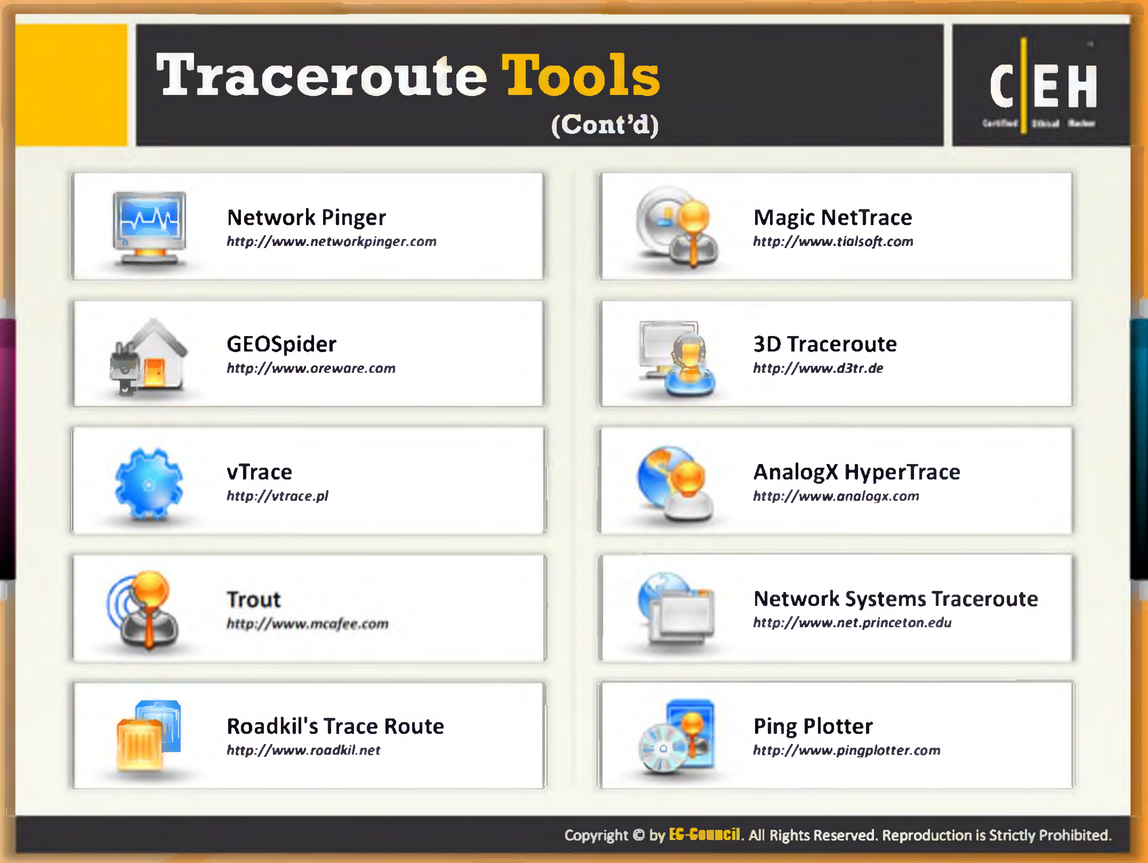
Analysis	In general this route is reasonably quick, with hops responding on average within 122ms. However, all hops after hop 10 in network [Network for 207.46.47.18]" respond particularly slowly.
RTT avg,max	116.3ms / 296ms
Packet Loss avg,max	38.1% / 100%
Route length	At least 17 hops
Alternate routes?	4 hop(s) have alternate routes (Hop(s) 12, 13, 14 & 15)

You are on day 1 of a 15 day trial. For purchase information click here or enter a license key.

Your database is 338 days out of date click here to update.

First time use Special Offer! Click here to save upto 20% on VisualRoute's 4 editions! 24 Hours Only!

FIGURE 2.39: VisualRoute 2010 screenshot



Traceroute Tools (Cont'd)

Network Pinger
http://www.networkpinger.com

Magic NetTrace
http://www.tialsoft.com

GEOSpider
http://www.oreware.com

3D Traceroute
http://www.d3tr.de

vTrace
http://vtrace.pl

AnalogX HyperTrace
http://www.analogx.com

Trout
http://www.mcafee.com

Network Systems Traceroute
http://www.net.princeton.edu

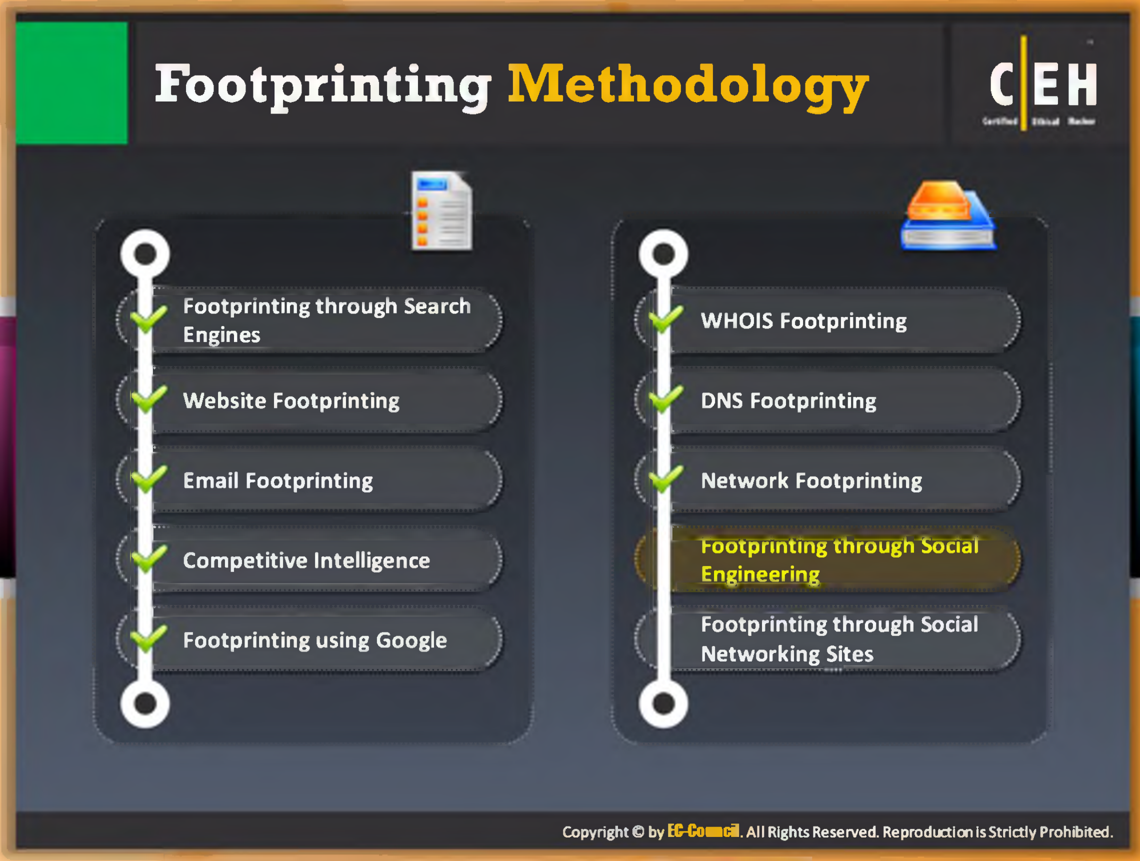
Roadkil's Trace Route
http://www.roadkil.net

Ping Plotter
http://www.pingplotter.com

Traceroute Tools (Cont'd)

A few more traceroute tools similar to Path Analyzer Pro and VisualRoute 2010 are listed as follows:

- Network Pinger available at http://www.networkpinger.com
- GEOSpider available at http://www.oreware.com
- vTrace available at http://vtrace.pl
- Trout available at http://www.mcafee.com
- Roadkil's Trace Route available at http://www.roadkil.net
- Magic NetTrace available at http://www.tialsoft.com
- 3D Traceroute available at http://www.d3tr.de
- AnalogX HyperTrace available at http://www.analogx.com
- Network Systems Traceroute available at http://www.net.princeton.edu
- Ping Plotter available at http://www.pingplotter.com



Footprinting Methodology

C|EH

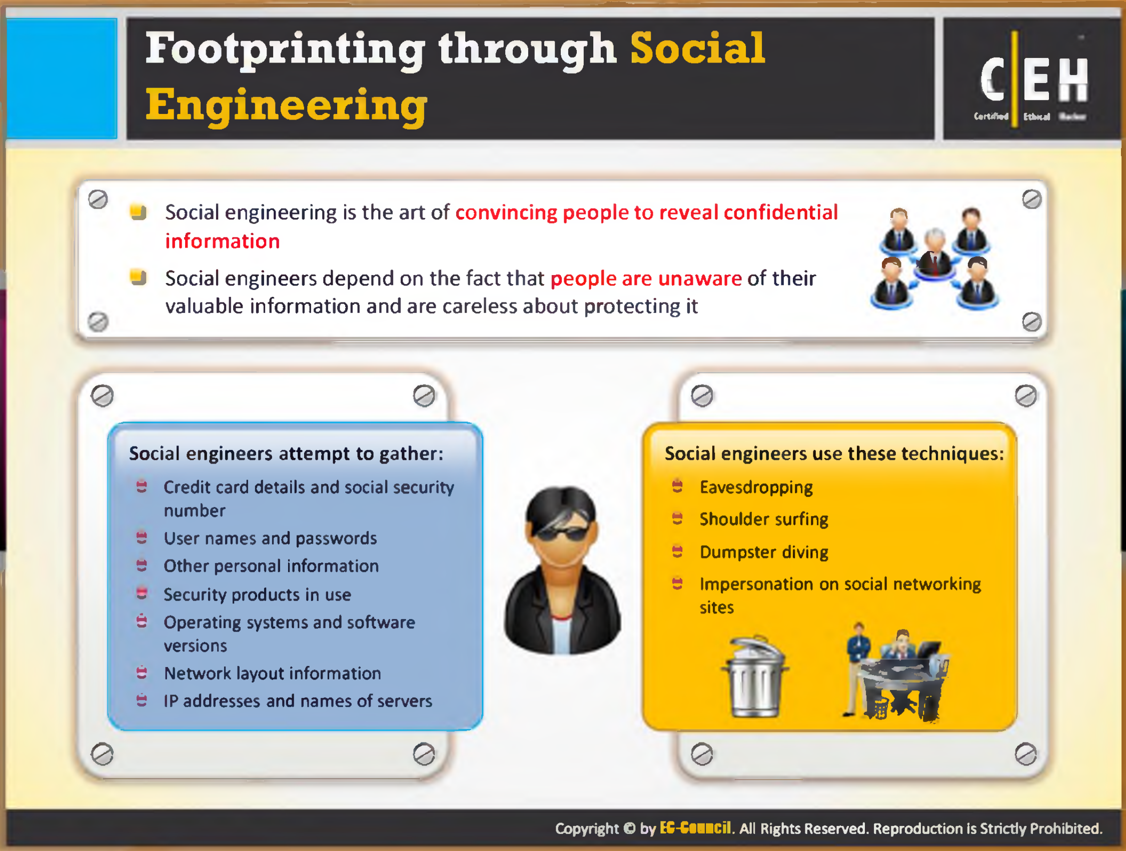
- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google

- ✓ WHOIS Footprinting
- ✓ DNS Footprinting
- ✓ Network Footprinting
- Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

So far we have discussed various techniques of gathering information either with the help of online resources or tools. Now we will discuss footprinting through **social engineering**, the art of grabbing information from people by manipulating them.

This section covers the social engineering concept and techniques used to gather information.



Footprinting through Social Engineering

- Social engineering is the art of convincing people to reveal confidential information
- Social engineers depend on the fact that people are unaware of their valuable information and are careless about protecting it

Social engineers attempt to gather:

- Credit card details and social security number
- User names and passwords
- Other personal information
- Security products in use
- Operating systems and software versions
- Network layout information
- IP addresses and names of servers

Social engineers use these techniques:

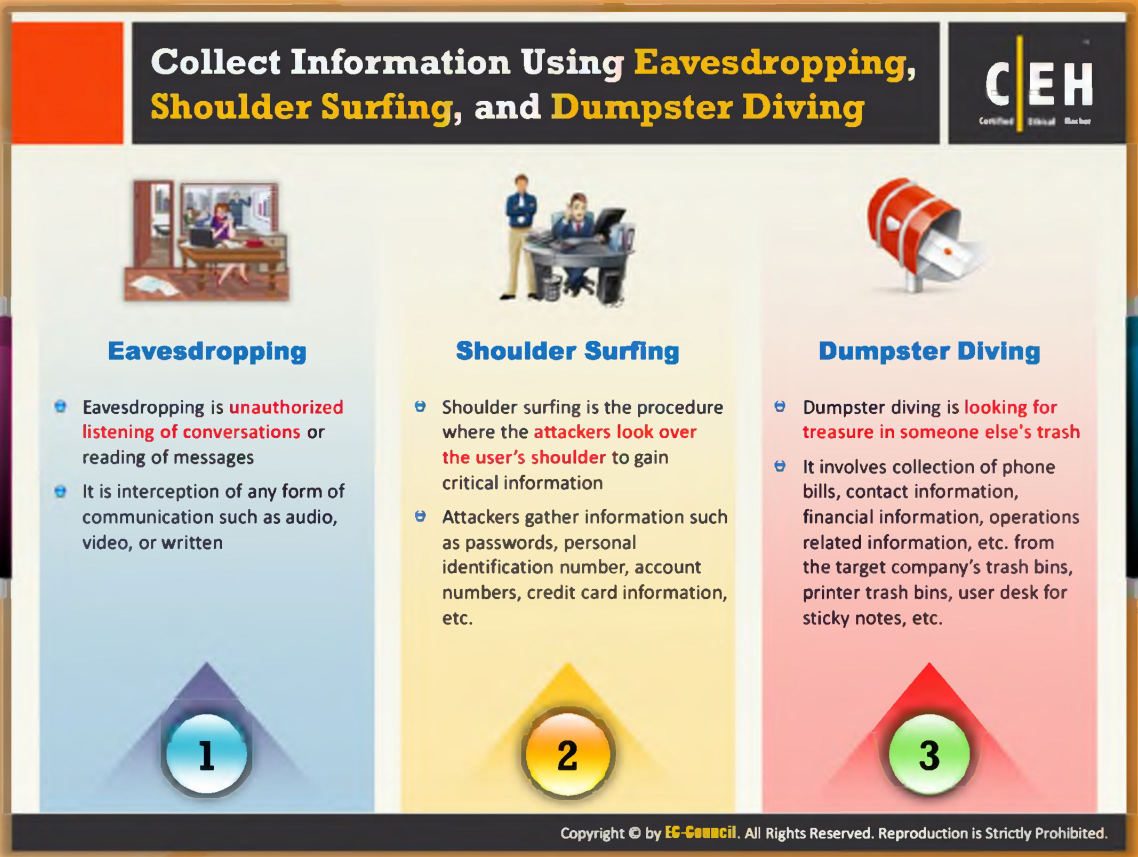
- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation on social networking sites

Footprinting through Social Engineering

Social engineering is a totally non-technical process in which an attacker tricks a person and obtains confidential information about the target in such a way that the target is unaware of the fact that someone is stealing his or her confidential information. The attacker actually plays a cunning game with the target to obtain confidential information. The attacker takes advantage of the helping nature of people and their weakness to provide confidential information.

To perform social engineering, you first need to gain the confidence of an authorized user and then trick him or her into revealing confidential information. The basic goal of social engineering is to obtain required confidential information and then use that information for hacking attempts such as gaining unauthorized access to the system, identity theft, industrial espionage, network intrusion, commit frauds, etc. The information obtained through social engineering may include credit card details, social security numbers, usernames and passwords, other personal information, operating systems and software versions, IP addresses, names of servers, network layout information, and much more. Social engineers use this information to hack a system or to commit fraud.

Social engineering can be performed in many ways such as eavesdropping, shoulder surfing, dumpster diving, impersonation on social networking sites, and so on.



Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Eavesdropping

- Eavesdropping is unauthorized listening of conversations or reading of messages
- It is interception of any form of communication such as audio, video, or written

Shoulder Surfing

- Shoulder surfing is the procedure where the attackers look over the user's shoulder to gain critical information
- Attackers gather information such as passwords, personal identification number, account numbers, credit card information, etc.

Dumpster Diving

- Dumpster diving is looking for treasure in someone else's trash
- It involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

Collect Information using Eavesdropping, Shoulder Surfing, and Dumpster Diving

As mentioned previously eavesdropping, shoulder surfing, and dumpster driving are the three techniques used to collect information from people using social engineering. Let's discuss these social engineering techniques to understand how they can be performed to obtain confidential information.

Eavesdropping

Eavesdropping is the act of secretly listening to the conversations of people over a phone or videoconference without their consent. It also includes reading secret messages from communication media such as instant messaging or fax transmissions. Thus, it is basically the act of intercepting communication without the consent of the communicating parties. The attacker gains confidential information by tapping the phone conversation, and intercepting audio, video, or written communication.

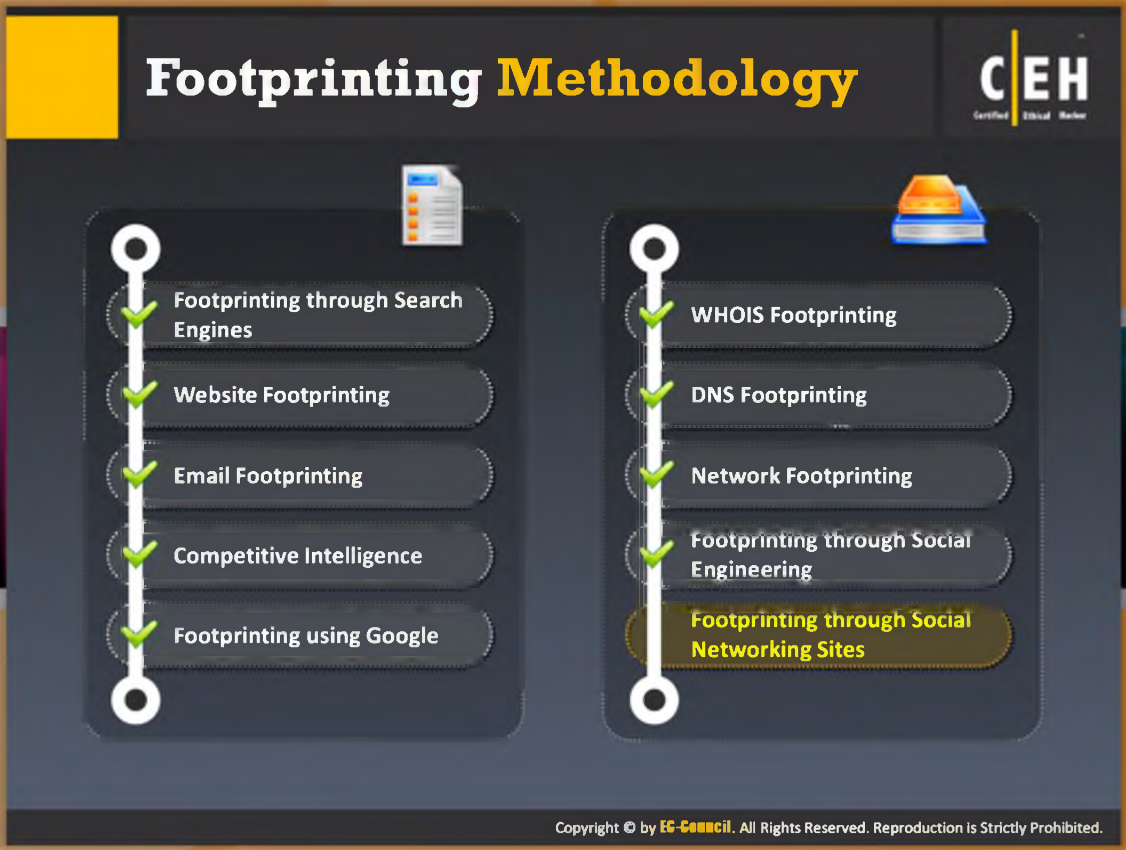
Shoulder Surfing

With this technique, an attacker stands behind the victim and secretly observes the victim's activities on the computer such keystrokes while entering usernames, passwords, etc.

This technique is commonly used to gain passwords, PINs, security codes, account numbers, credit card information, and similar data. It can be performed in a crowded place as it is relatively easy to stand behind the victim without his or her knowledge.

Dumpster Diving

This technique is also known as **trashing**, where the attacker looks for information in the target company's dumpster. The attacker may **gain vital information** such as phone bills, contact information, financial information, operations-related information, printouts of source codes, printouts of sensitive information, etc. from the target company's trash bins, printer trash bins, and sticky notes at users' desks, etc. The obtained information can be helpful for the attacker to commit attacks.



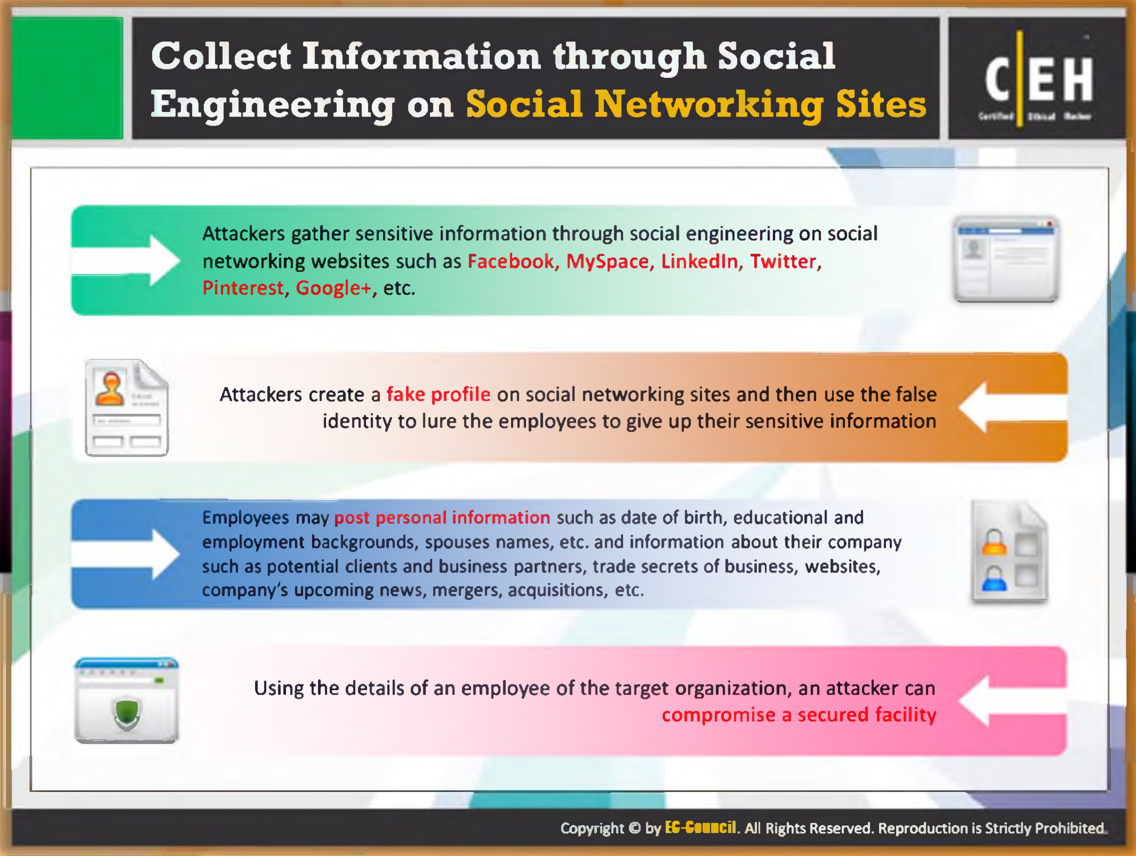
Footprinting Methodology

- ✓ Footprinting through Search Engines
- ✓ Website Footprinting
- ✓ Email Footprinting
- ✓ Competitive Intelligence
- ✓ Footprinting using Google
- ✓ WHOIS Footprinting
- ✓ DNS Footprinting
- ✓ Network Footprinting
- ✓ Footprinting through Social Engineering
- Footprinting through Social Networking Sites

Footprinting Methodology

Though footprinting through social networking sites sounds similar to footprinting through social engineering, there are some differences between the two methods. In footprinting through social engineering, the attacker tricks people into revealing information whereas in footprinting through social networking sites, the attacker gathers information available on social networking sites. Attackers can even use social networking sites as a medium to perform social engineering attacks.

This section explains how and what information can be collected from social networking sites by means of social engineering.



Collect Information through Social Engineering on Social Networking Sites

CEH
Certified Ethical Hacker

Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Attackers create a fake profile on social networking sites and then use the false identity to lure the employees to give up their sensitive information

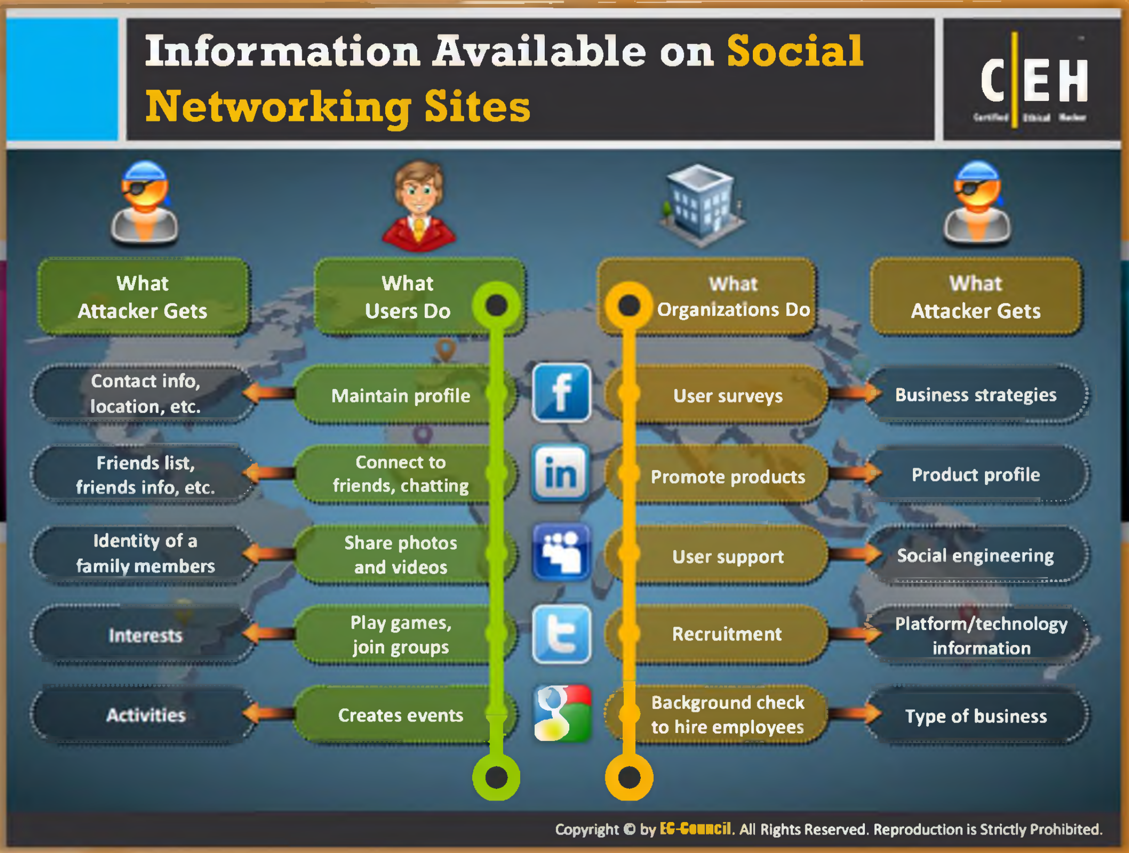
Employees may post personal information such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.

Using the details of an employee of the target organization, an attacker can compromise a secured facility

Collect Information through Social Engineering on Social Networking Sites

Social networking sites are the online services, platforms, or sites that allow people to connect with each other and to build social relations among people. The use of social networking sites is increasing rapidly. Examples of social networking sites include Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, and so on. Each social networking site has its own purpose and features. One site may be intended to connect friends, family, etc. and another may be intended to share professional profiles, etc. These social networking sites are open to everyone. Attackers may take advantage of these to grab sensitive information from users either by browsing through users' public profiles or by creating a fake profile and tricking user to believe him or her as a genuine user. These sites allow people to stay connected with others, to maintain professional profiles, and to share the information with others. On social networking sites, people may post information such as date of birth, educational information, employment backgrounds, spouse's names, etc. and companies may post information such as potential partners, websites, and upcoming news about the company.

For an attacker, these social networking sites can be great sources to find information about the target person or the company. These sites help an attacker to collect only the information uploaded by the person or the company. Attackers can easily access public pages of these accounts on the sites. To obtain more information about the target, attackers may create a fake account and use social engineering to lure the victim to reveal more information. For example, the attacker can send a friend request to the target person from the **fake account**; if the victim accepts the request, then the attacker can access even the restricted pages of the target person on that website. Thus, social networking sites prove to be a valuable information resource for attackers.



Information Available on Social Networking Sites

What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile
Identity of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

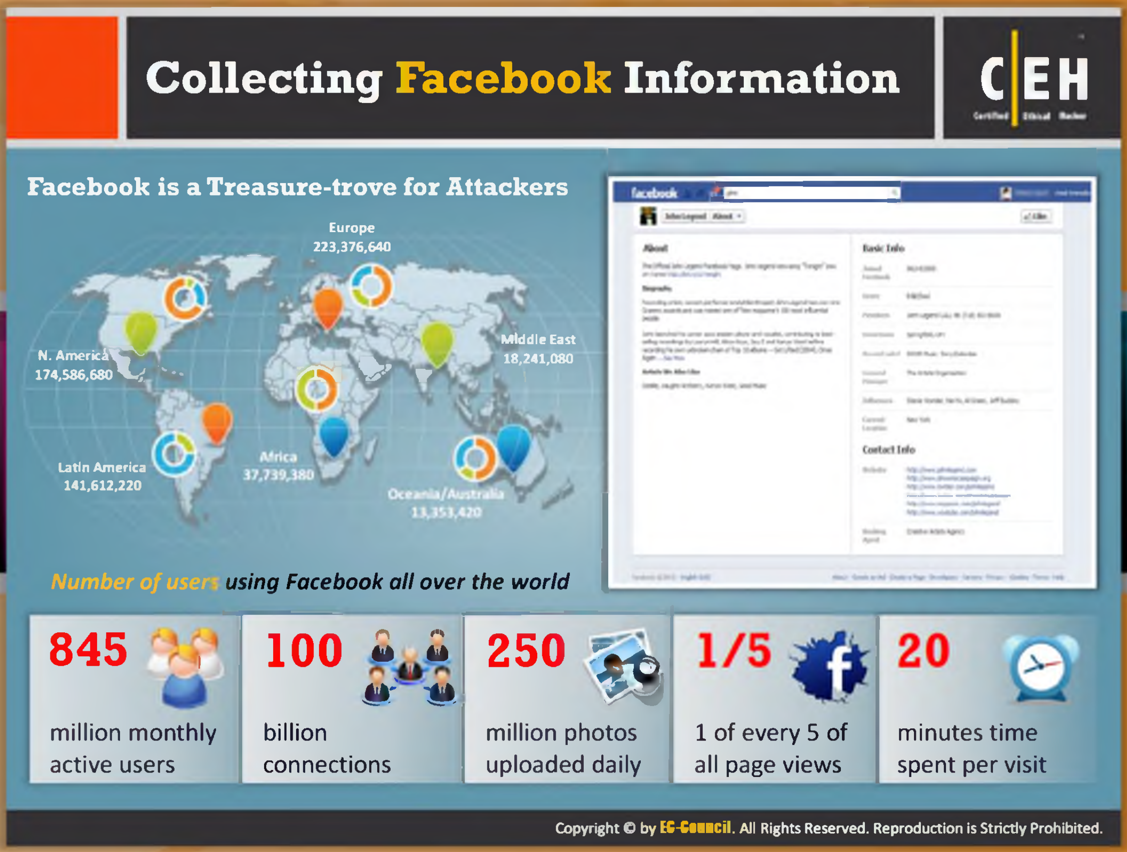
Information Available on Social Networking Sites

So far, we have discussed how an attacker can grab information from social networking sites; now we will discuss what information an attacker can get from social networking sites.

People usually maintain profiles on social networking sites in order to provide basic information about them and to get connected with others. The profile generally contains information such as name, contact information (mobile number, email ID), friends' information, information about family members, their interests, activities, etc. People usually connect to friends and chat with them. Attackers can gather sensitive information through their chats. Social networking sites also allow people to share photos and videos with their friends. If the people don't set their privacy settings for their albums, then attackers can see the pictures and videos shared by the victim. Users may join groups to plays games or to share their views and interests. Attackers can grab information about a victim's interests by tracking their groups and then can trap the victim to reveal more information. Users may create events to notify other users of group about upcoming occasions. With these events, attackers can reveal the victim's activities. Like individuals, organizations also use social networking sites to connect with people, promote their products, and to gather feedback about their products or services, etc. The activities of an organization on the social networking sites and the respective information that an **attacker** can grab are as follows:

What Organizations Do	What Attacker Gets
User surveys	Business strategies
Promote products	Product profile
User support	Social engineering
Background check to hire employees	Type of business

TABLE 2.1: What organizations Do and What Attacker Gets



Collecting Facebook Information

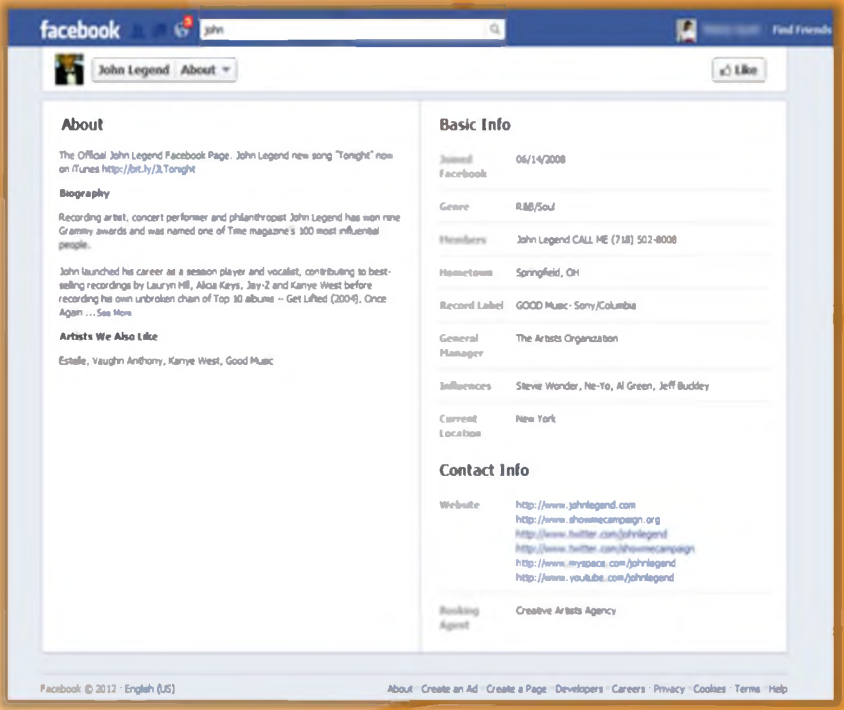
Facebook is a Treasure-trove for Attackers

Number of users using Facebook all over the world

845 million monthly active users	**100** billion connections	**250** million photos uploaded daily	**1/5** 1 of every 5 of all page views	**20** minutes time spent per visit

Collecting Facebook Information

Facebook is one of the world's largest social networking sites, having more than 845 million monthly active users all over the world. It allows people to create their personal profile, add friends, exchange instant messages, create or join various groups or communities, and much more. An attacker can grab all the information provided by the victim on Facebook. To grab information from Facebook, the attacker should have an active account. The attacker should login to his/her account, and search for either the target person or organization profile. Browsing the target person's profile may reveal a lot of useful information such as phone number, email ID, friend information, educational details, professional details, his interests, photos, and much more. The attacker can use this information for further hacking planning, such as social engineering, to reveal more information about the target.



About

The Official John Legend Facebook Page. John Legend new song "Tonight" now on iTunes http://bit.ly/JLTonight

Biography

Recording artist, concert performer and philanthropist John Legend has won nine Grammy awards and was named one of Time magazine's 100 most influential people.

John launched his career as a session player and vocalist, contributing to best-selling recordings by Lauryn Hill, Alicia Keys, Jay-Z and Kanye West before recording his own unbroken chain of Top 10 albums -- Get Lifted (2004), Once Again ... See More

Artists We Also Like

Estelle, Vaughn Anthony, Kanye West, Good Music

Basic Info

Joined Facebook	06/14/2008
Genre	R&B/Soul
Members	John Legend CALL ME (718) 502-8008
Hometown	Springfield, OH
Record Label	GOOD Music - Sony/Columbia
General Manager	The Artists Organization
Influences	Stevie Wonder, Ne-Yo, Al Green, Jeff Buckley
Current Location	New York

Contact Info

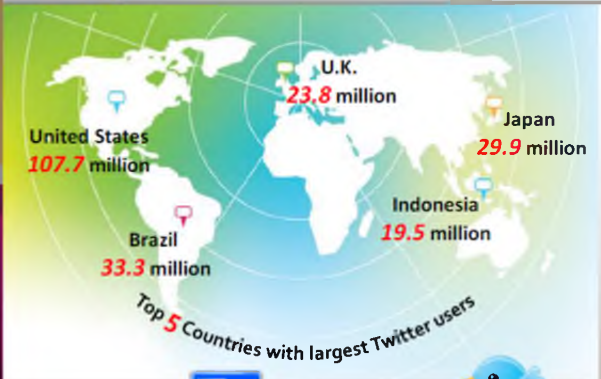
Website	http://www.johnlegend.com http://www.showmecampaign.org http://www.twitter.com/johnlegend http://www.twitter.com/showmecampaign http://www.myspace.com/johnlegend http://www.youtube.com/johnlegend
Booking Agent	Creative Artists Agency

Facebook © 2012 · English (US)

About · Create an Ad · Create a Page · Developers · Careers · Privacy · Cookies · Terms · Help

FIGURE 2.40: Facebook screenshot

Collecting Twitter Information

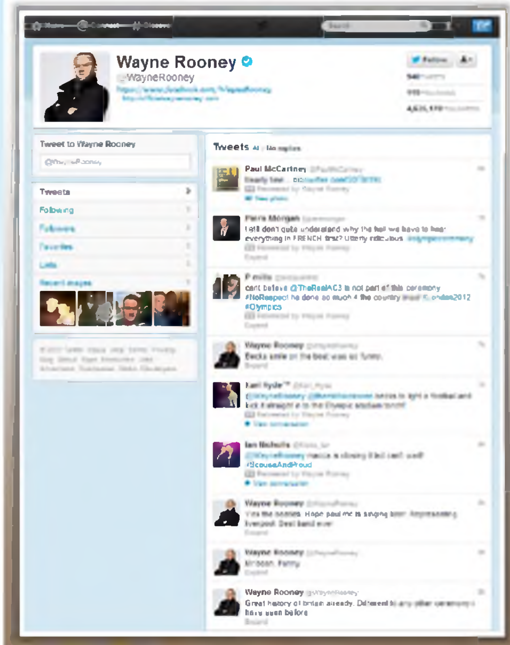


465 million accounts

350 million tweets a day

76% Twitter users now post status updates

55% Twitter users access the platform via their mobile



Wayne Rooney
@WayneRooney

Tweet to Wayne Rooney

Tweets

Paul McCartney

Piers Morgan
I still dont quite understand why the hell we have to hear everything in FRENCH first? Utterly ridiculous

P mills
cant believe @TheRealAC3 is not part of this ceremony #NoRespect he done so much 4 the country #London2012 #Olympics

Wayne Rooney
Becks smile on the boat was so funny.

Karl Hyde™

Ian Nicholls
#ScouseAndProud

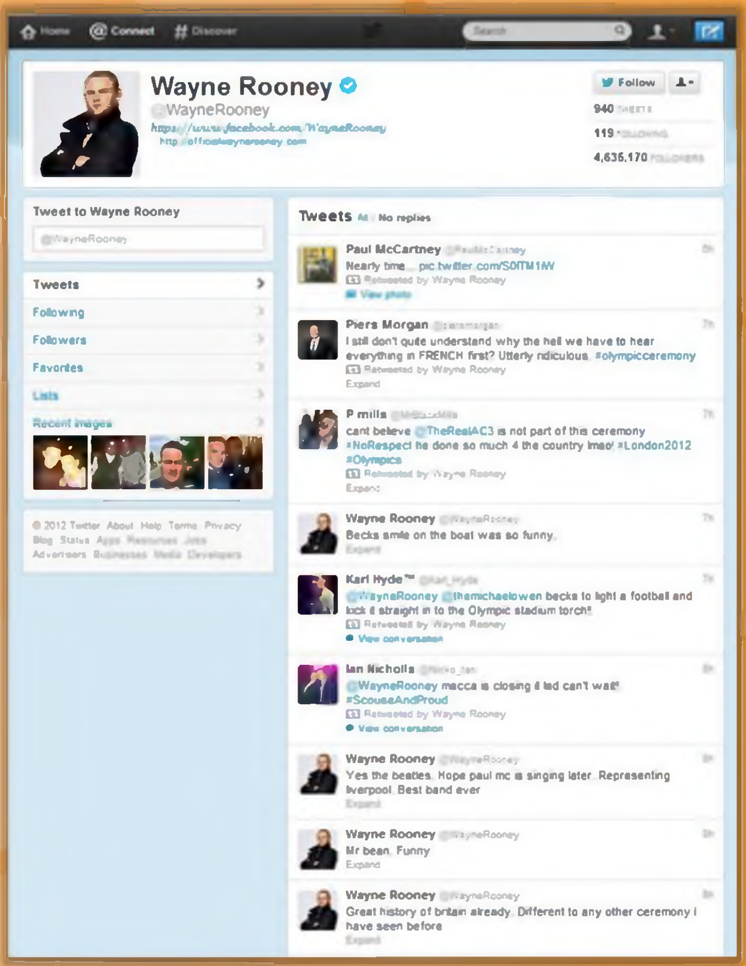
Wayne Rooney

Wayne Rooney
Mr bean. Funny

Wayne Rooney
Great history of britain already. Different to any other ceremony i have seen before

Collecting Twitter Information

Twitter is another popular **social networking site** used by people to send and read **text-based messages**. It allows you to follow your friends, experts, favorite celebrities, etc. This site also can be a great source for an attacker to get information about the target person. This is helpful in extracting information such as personal information, friend information, activities of the target posted as tweets, whom the target is following, the followers of the user, **photos uploaded**, etc. The attacker may get meaningful information from the target user's tweets.



Home
Connect
Discover
Search
Follow

Wayne Rooney
@WayneRooney
https://www.facebook.com/WayneRooney
http://officialwaynerooney.com

940 TWEETS
119 FOLLOWING
4,636,170 FOLLOWERS

Tweet to Wayne Rooney
@WayneRooney

Tweets
Following
Followers
Favorites
Lists
Recent images
© 2012 Twitter About Help Terms Privacy
Blog Status Apps Resources Jobs
Advertisers Businesses Media Developers

Tweets All / No replies

Paul McCartney
Nearly time... pic.twitter.com/S0ITM1WV
Retweeted by Wayne Rooney
View photo

Piers Morgan
I still don't quite understand why the hell we have to hear everything in FRENCH first? Utterly ridiculous. #olympicceremony
Retweeted by Wayne Rooney
Expand

P mills
cant believe @TheRealAC3 is not part of this ceremony #NoRespect he done so much 4 the country lmao! #London2012 #Olympics
Retweeted by Wayne Rooney
Expand

Wayne Rooney @WayneRooney
Becks smile on the boat was so funny.
Expand

Karl Hyde™ @Karl_Hyde
@WayneRooney @themichaelowen becks to light a football and kick it straight in to the Olympic stadium torch!!
Retweeted by Wayne Rooney
View conversation

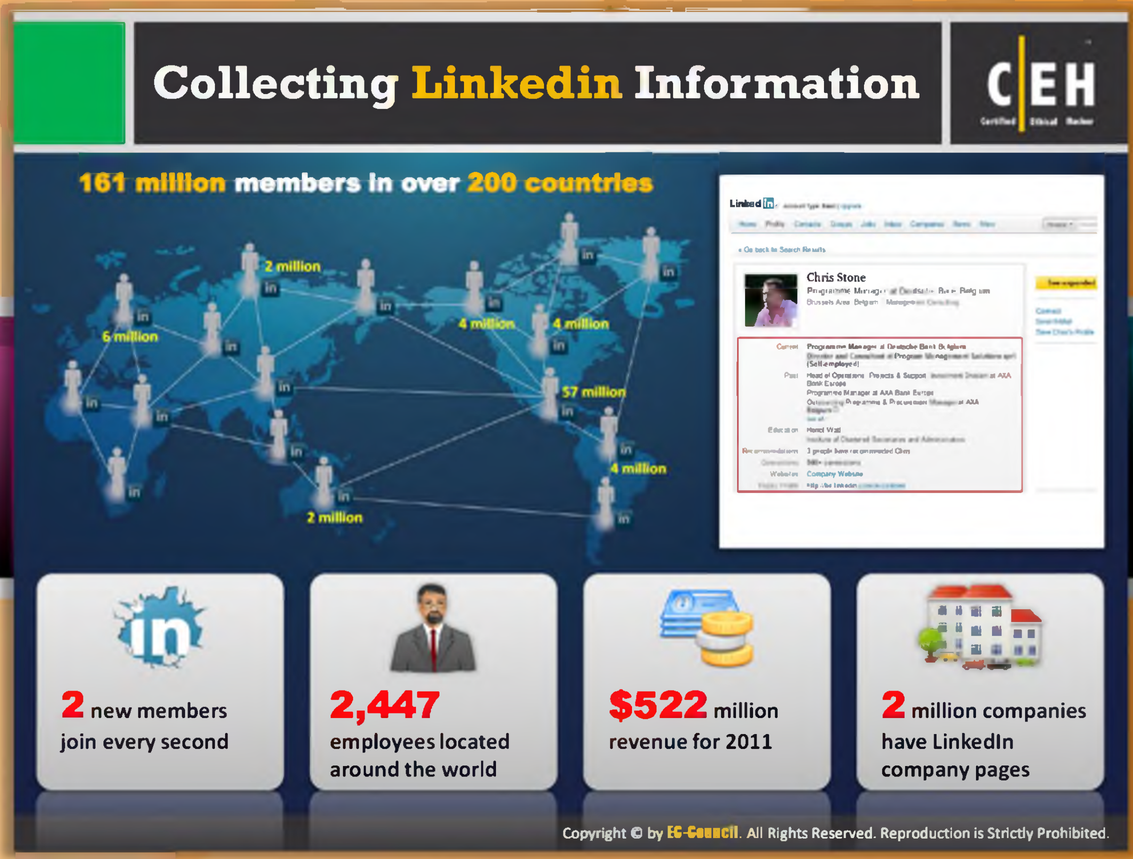
Ian Nicholls
@WayneRooney macca is closing it lad can't wait! #ScouseAndProud
Retweeted by Wayne Rooney
View conversation

Wayne Rooney @WayneRooney
Yes the beatles. Hope paul mc is singing later. Representing liverpool. Best band ever
Expand

Wayne Rooney @WayneRooney
Mr bean. Funny
Expand

Wayne Rooney @WayneRooney
Great history of britain already. Different to any other ceremony I have seen before
Expand

FIGURE 2.41: Twitter showing user's tweets



Collecting Linkedin Information

161 million members in over 200 countries

Linked in

« Go back to Search Results

Chris Stone
Programme Manager at Deutsche Bank Belgium
Brussels Area, Belgium | Management Consulting

Current: Programme Manager at Deutsche Bank Belgium; Director and Consultant at Program Management Solutions sprl (Self-employed)
Past: Head of Operations, Projects & Support, Investment Division at AXA Bank Europe; Programme Manager at AXA Bank Europe; Outsourcing Programme & Procurement Manager at AXA Belgium
Education: Heriot Watt; Institute of Chartered Secretaries and Administrators
Recommendations: 3 people have recommended Chris
Connections: 500+ connections
Websites: Company Website
Public Profile: http://be.linkedin.com/[illegible]

2 new members join every second

2,447 employees located around the world

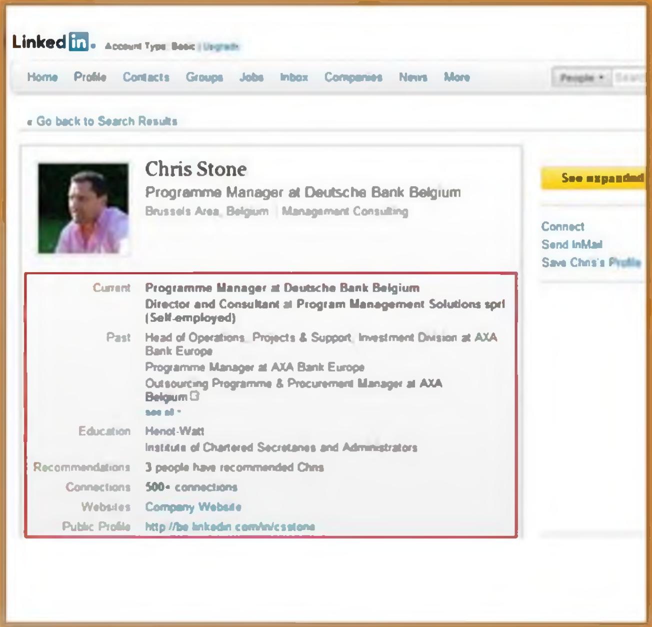
$522 million revenue for 2011

2 million companies have LinkedIn company pages

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting LinkedIn Information

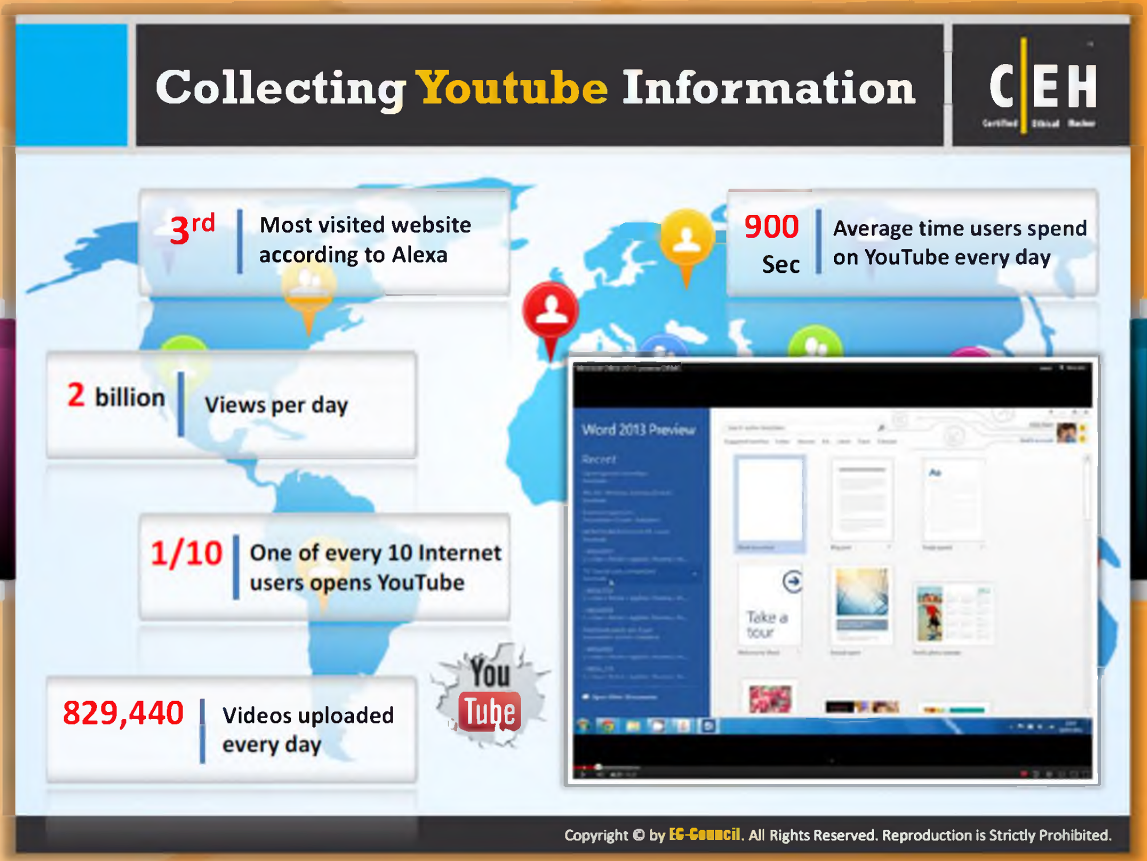
Similar to Facebook and Twitter, LinkedIn is another social networking site for professionals. It allows people to create and manage their professional profile and identity. It allows its users to build and engage with their professional network. Hence, this can be a great information resource for the attacker. The attacker may get information such as current employment details, past employment details, education details, contact details, and much more about the target person. The attacker can collect all this information with the footprinting process.



Chris Stone
Programme Manager at Deutsche Bank Belgium
Brussels Area, Belgium | Management Consulting

Current	Programme Manager at Deutsche Bank Belgium Director and Consultant at Program Management Solutions sprl (Self-employed)
Past	Head of Operations, Projects & Support, Investment Division at AXA Bank Europe Programme Manager at AXA Bank Europe Outsourcing Programme & Procurement Manager at AXA Belgium see all
Education	Heriot-Watt Institute of Chartered Secretaries and Administrators
Recommendations	3 people have recommended Chris
Connections	500+ connections
Websites	Company Website
Public Profile	http://be.linkedin.com/in/csstone

FIGURE 2.42: LinkedIn showing user's professional profile and identity



Collecting Youtube Information

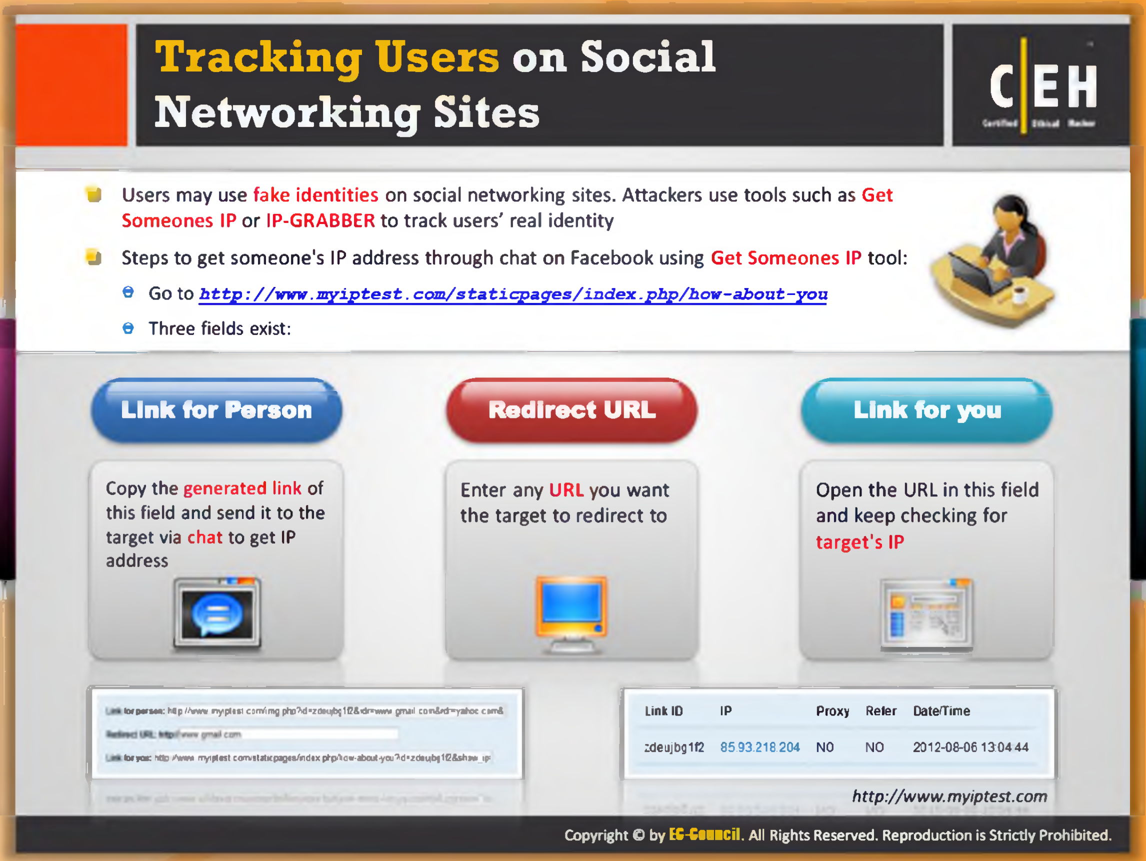
3rd	Most visited website according to Alexa
900 Sec	Average time users spend on YouTube every day
2 billion	Views per day
1/10	One of every 10 Internet users opens YouTube
829,440	Videos uploaded every day

CEH
Certified Ethical Hacker
You Tube
Word 2013 Preview

Collecting YouTube Information

YouTube is a **website** that allows you to upload, view, and share videos all over the world. The attacker can search for the videos related to the target and may collect information from them.

FIGURE 2.43: Youtube showing videos related to target



Tracking Users on Social Networking Sites

- Users may use fake identities on social networking sites. Attackers use tools such as Get Someones IP or IP-GRABBER to track users' real identity
- Steps to get someone's IP address through chat on Facebook using Get Someones IP tool:
  - Go to http://www.myiptest.com/staticpages/index.php/how-about-you
  - Three fields exist:

Link for Person: Copy the generated link of this field and send it to the target via chat to get IP address

Redirect URL: Enter any URL you want the target to redirect to

Link for you: Open the URL in this field and keep checking for target's IP

Link for person: http://www.myiptest.com/img.php?d=zdeujbg1f2&rdr=www.gmail.com&rd=yahoo.com&
Redirect URL: http://www.gmail.com
Link for you: http://www.myiptest.com/staticpages/index.php/how-about-you?d=zdeujbg1f2&show_ip

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

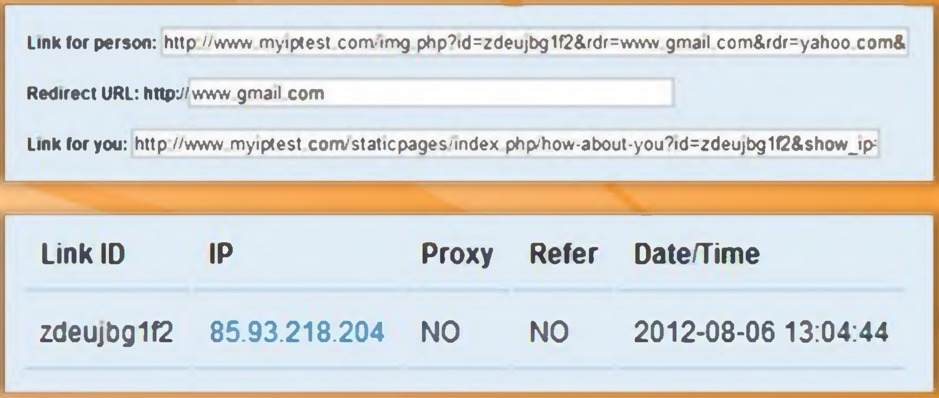
http://www.myiptest.com

Tracking Users on Social Networking Sites

In order to protect themselves from Internet fraud and attacks, people with little knowledge about Internet crimes may use fake identities on social networking sites. In such cases, you will not get exact information about the target user. So to determine the real identity of the target user, you can use tools such as Get Someone's IP or IP-GRABBER to track users' real identities.

If you want to trace the identity of particular user, then do the following:

- Open your web browser, paste the URL, and press Enter: http://www.myiptest.com/staticpages/index.php/how-about-you
- Notice the three fields at the bottom of the web page, namely **Link for person, Redirect URL: http://**, and **Link for you**.
  - To get real IP address of the target, copy the generated link of the **Link for person** field and send it to the target via chat.
  - Enter any **URL** you want the target to redirect to in **the Redirect link: http://** field.
  - Open the URL present in the **Link for you** field in another window, to monitor the target's IP address details and additional details.



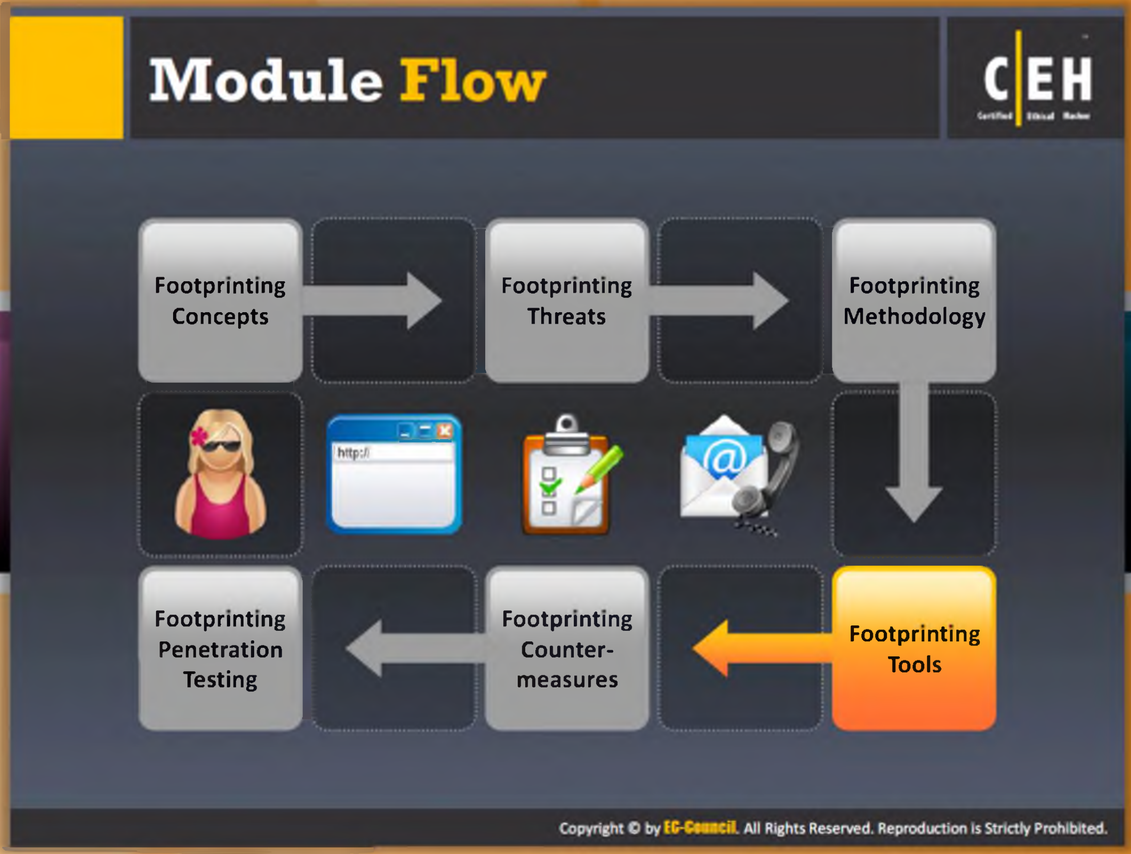
Link for person: http://www.myiptest.com/img.php?id=zdeujbg1f2&rdr=www.gmail.com&rdr=yahoo.com&

Redirect URL: http:// www.gmail.com

Link for you: http://www.myiptest.com/staticpages/index.php/how-about-you?id=zdeujbg1f2&show_ip=

Link ID	IP	Proxy	Refer	Date/Time
zdeujbg1f2	85.93.218.204	NO	NO	2012-08-06 13:04:44

FIGURE 2.44: Tracing identity of user's



Module Flow

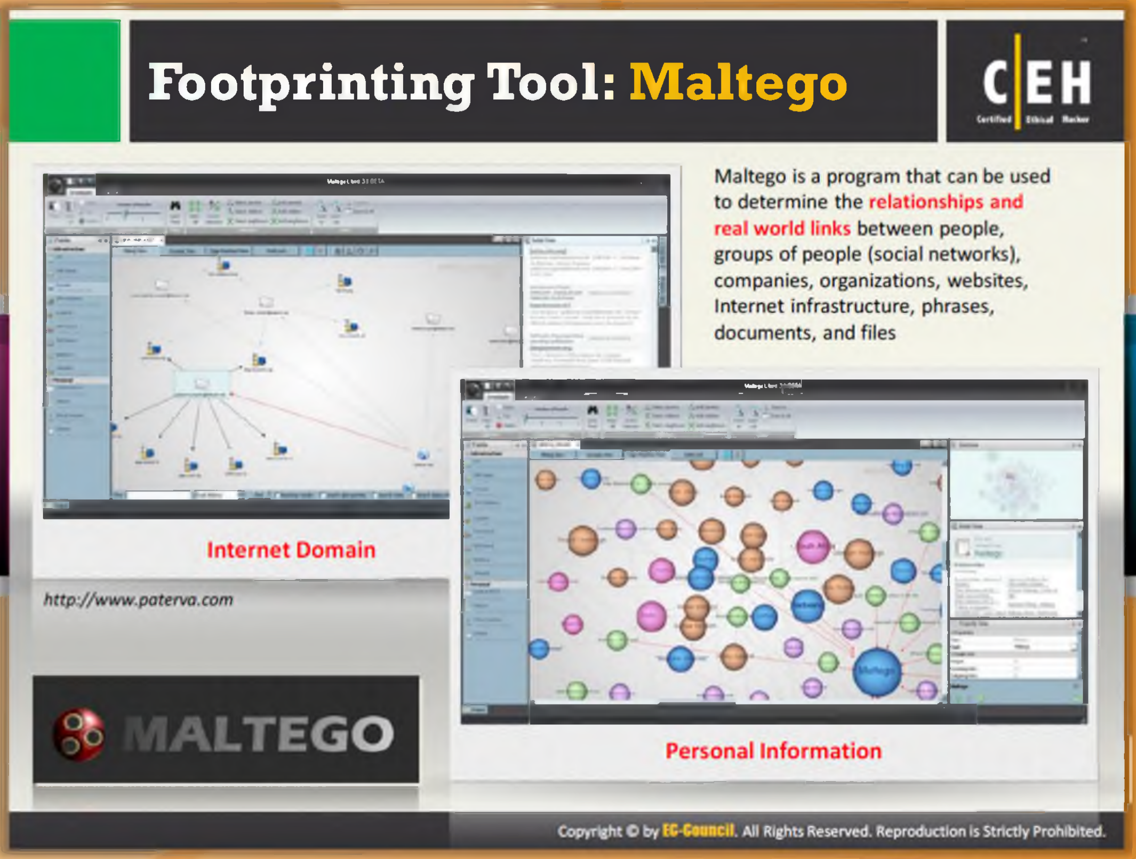
Footprinting Concepts → Footprinting Threats → Footprinting Methodology → Footprinting Tools → Footprinting Countermeasures → Footprinting Penetration Testing

Module Flow

Footprinting can be performed with the help of tools. Many organizations offer tools that make information gathering an easy job. These tools ensure the maximum

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

This section describes tools intended for grabbing information from various sources.



Footprinting Tool: Maltego

Maltego is a program that can be used to determine the relationships and real world links between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files

Internet Domain

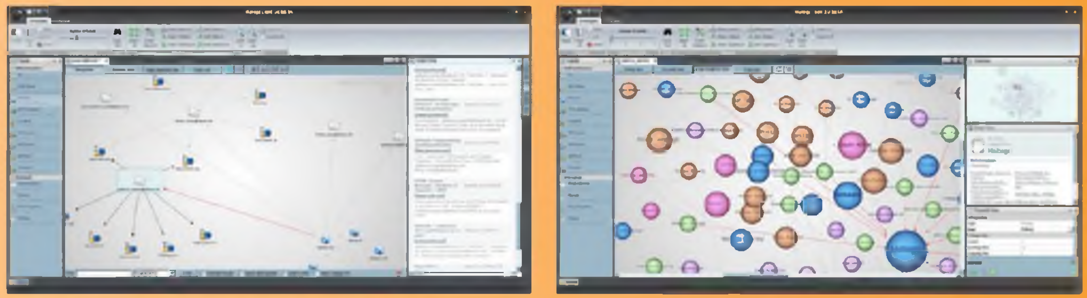
http://www.paterva.com

Personal Information

Footprinting Tool: Maltego

Source: http://paterva.com

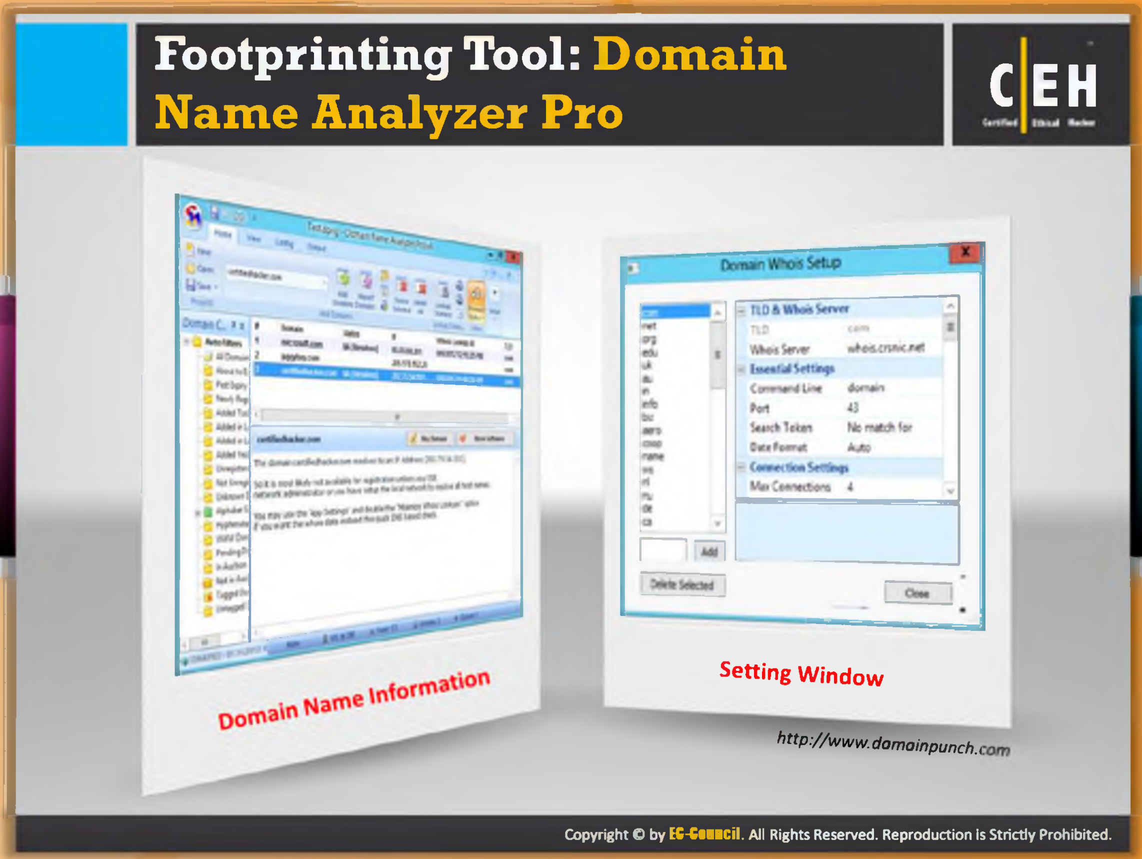
Maltego is an open source **intelligence** and **forensics application**. It can be used for the information gathering phase of all **security-related work**. Maltego is a platform developed to deliver a clear threat picture to the environment that an organization owns and operates. It can be used to determine the relationships and real-world links between people, social networks, companies, organizations, websites, Internet infrastructure (domains, DNS names, Netblocks, IP addresses), phrases, affiliations, documents, and files.



Internet Domain

Personal Information

FIGURE 2.45: Maltego showing Internet Domain and personal information



Footprinting Tool: Domain Name Analyzer Pro

Domain Name Information

Setting Window

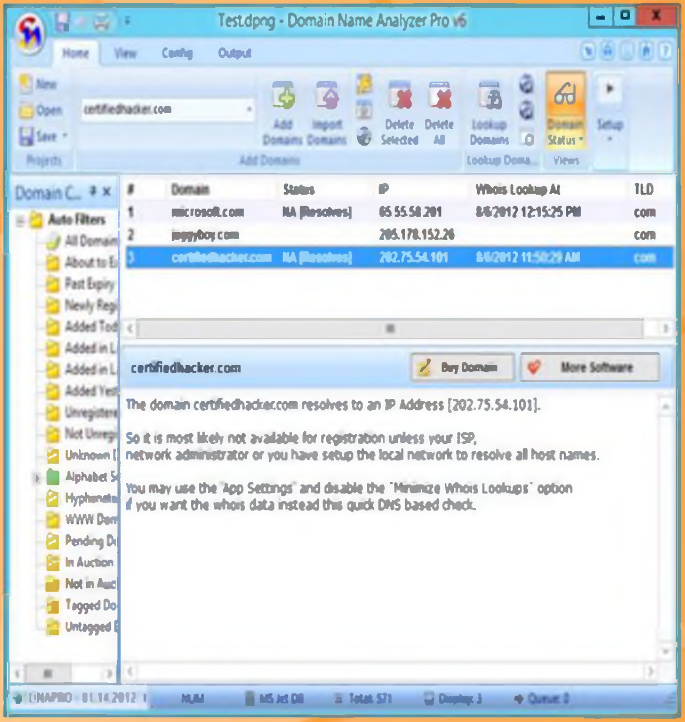
http://www.domainpunch.com

Footprinting Tool: Domain Name Analyzer Pro

Source: http://www.domainpunch.com

Domain Name Analyzer Professional is **Windows software** for finding, managing, and maintaining multiple domain names. It supports the display of additional data (expiry and creation dates, name server information), tagging domains, secondary whois lookups (for thin model whois TLDs like COM, NET, TV).

The following is a screenshot of the Domain Name **Analyzer Pro** tool showing domain name information:



#	Domain	Status	IP	Whois Lookup At	TLD
1	microsoft.com	NA [Resolves]	65.55.58.201	8/6/2012 12:15:25 PM	com
2	juggyboy.com		205.178.152.26		com
3	certifiedhacker.com	NA [Resolves]	202.75.54.101	8/6/2012 11:50:29 AM	com

certifiedhacker.com

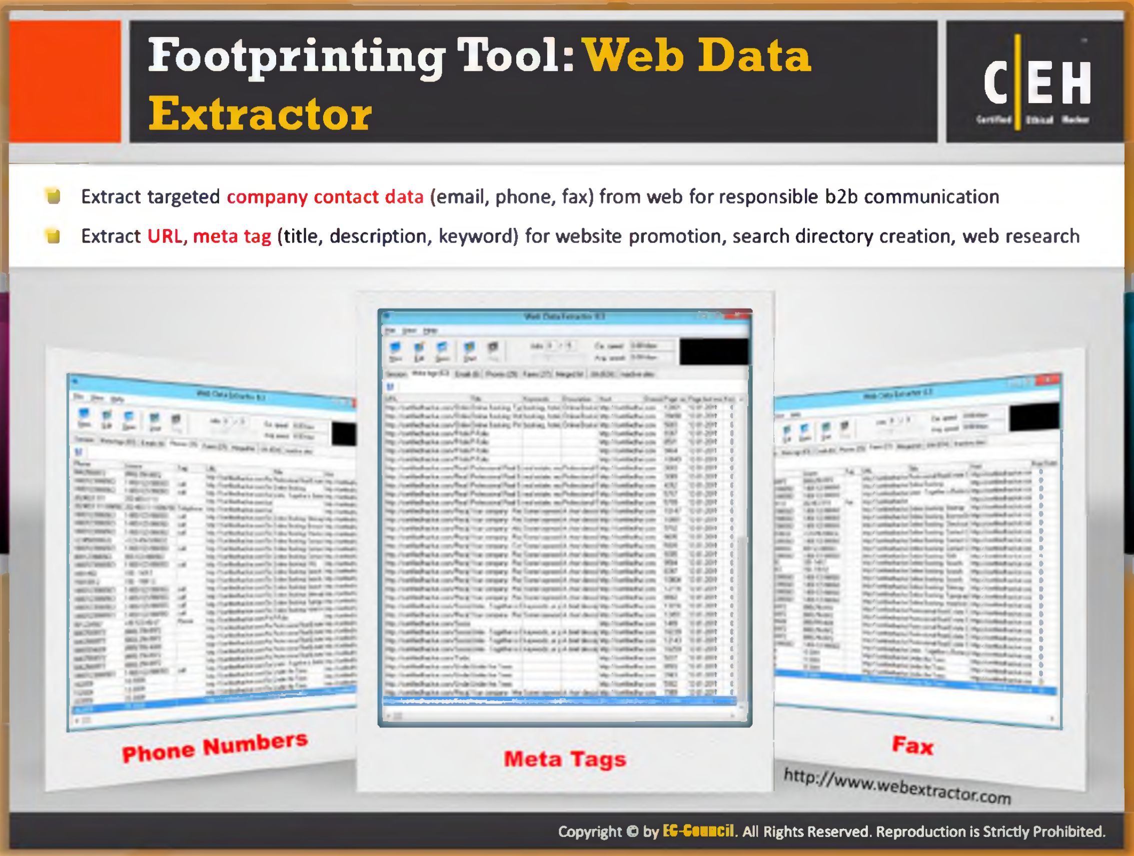
The domain certifiedhacker.com resolves to an IP Address [202.75.54.101].

So it is most likely not available for registration unless your ISP,
network administrator or you have setup the local network to resolve all host names.

You may use the 'App Settings' and disable the 'Minimize Whois Lookups' option
if you want the whois data instead this quick DNS based check.

Domain Name Information

FIGURE 2.46: Domain Name Analyzer Pro software showing Domain Name Information



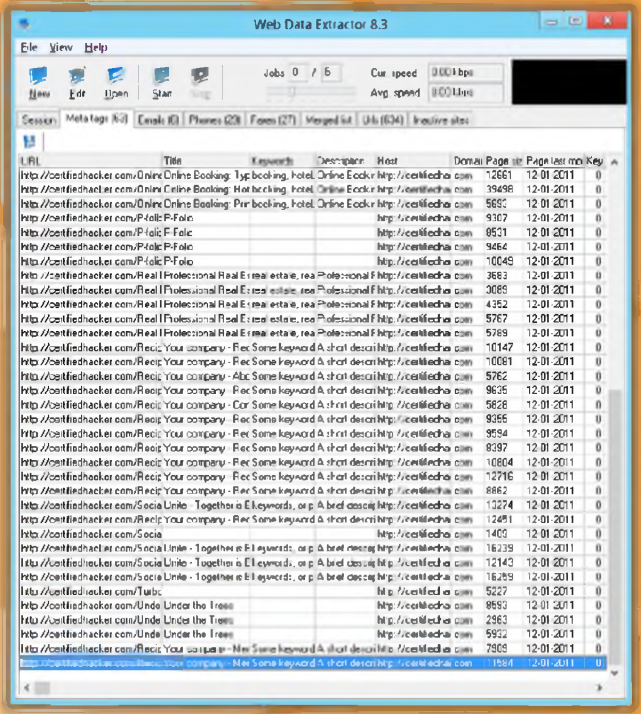
Footprinting Tool: Web Data Extractor

- Extract targeted company contact data (email, phone, fax) from web for responsible b2b communication
- Extract URL, meta tag (title, description, keyword) for website promotion, search directory creation, web research

Footprinting Tool: Web Data Extractor

Source: http://www.webextractor.com

Web Data Extractor is a **data extractor tool**. It extracts targeted company contact data (email, phone, and fax) from the web, extracts the **URL** and **meta tag** (title, desc, keyword) for website promotion, searches directory creation, etc. The following is a screenshot of the **Web Data Extractor** showing meta tags:



Jobs 0 / 5

Cur. speed 0.00 kbps

Avg. speed 0.00 kbps

URL	Title	Keywords	Description	Host	Domai	Page siz	Page last mo	Key
http://certifiedhacker.com/Onlin	Online Booking: Typ	booking, hotel	Online Bookir	http://certifiedha	com	12661	12-01-2011	0
http://certifiedhacker.com/Onlin	Online Booking: Hot	booking, hotel	Online Bookir	http://certifiedha	com	39498	12-01-2011	0
http://certifiedhacker.com/Onlin	Online Booking: Pr	booking, hotel	Online Bookir	http://certifiedha	com	5693	12-01-2011	0
http://certifiedhacker.com/P-foli	P-Folio			http://certifiedha	com	9307	12-01-2011	0
http://certifiedhacker.com/P-foli	P-Folio			http://certifiedha	com	8531	12-01-2011	0
http://certifiedhacker.com/P-foli	P-Folio			http://certifiedha	com	9464	12-01-2011	0
http://certifiedhacker.com/P-foli	P-Folio			http://certifiedha	com	10049	12-01-2011	0
http://certifiedhacker.com/Real I	Professional Real E	real estate, rea	Professional F	http://certifiedha	com	3683	12-01-2011	0
http://certifiedhacker.com/Real I	Professional Real E	real estate, rea	Professional F	http://certifiedha	com	3089	12-01-2011	0
http://certifiedhacker.com/Real I	Professional Real E	real estate, rea	Professional F	http://certifiedha	com	4352	12-01-2011	0
http://certifiedhacker.com/Real I	Professional Real E	real estate, rea	Professional F	http://certifiedha	com	5767	12-01-2011	0
http://certifiedhacker.com/Real I	Professional Real E	real estate, rea	Professional F	http://certifiedha	com	5789	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	10147	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	10081	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Abc	Some keyword	A short descri	http://certifiedha	com	5762	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	9635	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Cor	Some keyword	A short descri	http://certifiedha	com	5828	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	9355	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	9594	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	8397	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	10804	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	12716	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	8862	12-01-2011	0
http://certifiedhacker.com/Socia	Unite - Together is E	keywords, or p	A brief descri	http://certifiedha	com	13274	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - Rec	Some keyword	A short descri	http://certifiedha	com	12451	12-01-2011	0
http://certifiedhacker.com/Socia				http://certifiedha	com	1409	12-01-2011	0
http://certifiedhacker.com/Socia	Unite - Together is E	keywords, or p	A brief descri	http://certifiedha	com	16239	12-01-2011	0
http://certifiedhacker.com/Socia	Unite - Together is E	keywords, or p	A brief descri	http://certifiedha	com	12143	12-01-2011	0
http://certifiedhacker.com/Socia	Unite - Together is E	keywords, or p	A brief descri	http://certifiedha	com	16259	12-01-2011	0
http://certifiedhacker.com/Turbo				http://certifiedha	com	5227	12-01-2011	0
http://certifiedhacker.com/Unde	Under the Trees			http://certifiedha	com	8593	12-01-2011	0
http://certifiedhacker.com/Unde	Under the Trees			http://certifiedha	com	2963	12-01-2011	0
http://certifiedhacker.com/Unde	Under the Trees			http://certifiedha	com	5932	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - New	Some keyword	A short descri	http://certifiedha	com	7909	12-01-2011	0
http://certifiedhacker.com/Recip	Your company - New	Some keyword	A short descri	http://certifiedha	com	11584	12-01-2011	0

FIGURE 2.47: Web Data Extractor showing meta tags

Additional Footprinting Tools

Prefix WhoIs
http://pwhois.org

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

NetScanTools Pro
http://www.netscantools.com

BingIng
http://www.blueinfy.com

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

Spiderzilla
http://spiderzilla.mozdev.org

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

Sam Spade
http://www.majorgeeks.com

DNS DIGGER
http://www.dnsdigger.com

Robtex
http://www.robtex.com

Additional Footprinting Tools

In addition to the footprinting tools mentioned previously, a few more tools are listed as follows:

- Prefix WhoIs available at http://pwhois.org
- NetScanTools Pro available at http://www.netscantools.com
- Tctrace available at http://www.phenoelit-us.org
- Autonomous System Scanner (ASS) available at http://www.phenoelit-us.org
- DNS DIGGER available at http://www.dnsdigger.com
- Netmask available at http://www.phenoelit-us.org
- Binging available at http://www.blueinfy.com
- Spiderzilla available at http://spiderzilla.mozdev.org
- Sam Spade available at http://www.majorgeeks.com
- Robtex available at http://www.robtex.com

Additional Footprinting Tools (Cont'd)

C|EH Certified Ethical Hacker

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

SpiderFoot
http://www.binarypool.com

Domain Research Tool
http://www.domainresearchtool.com

CallerIP
http://www.callerippro.com

ActiveWhois
http://www.johnru.com

Zaba Search
http://www.zabasearch.com

yoName
http://yoname.com

GeoTrace
http://www.nabber.org

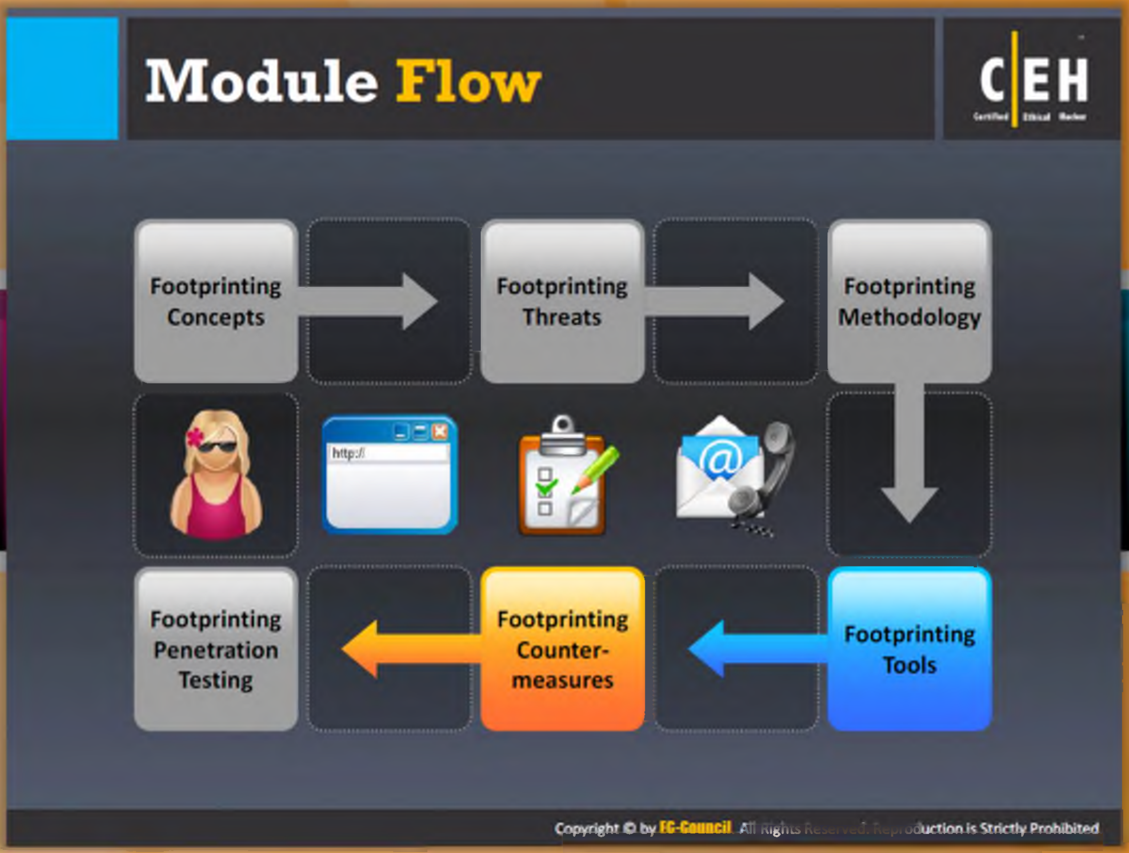
Ping-Probe
http://www.ping-probe.com

DomainHostingView
http://www.nirsoft.net

Additional Footprinting Tools (Cont'd)

Additional footprinting tools that are helpful in gathering information about the target person or organization are listed as follows:

- Dig Web Interface available at http://www.digwebinterface.com
- Domain Research Tool available at http://www.domainresearchtool.com
- ActiveWhois available at http://www.johnru.com
- yoName available at http://yoname.com
- Ping-Probe available at http://www.ping-probe.com
- SpiderFoot available at http://www.binarypool.com
- CallerIP available at http://www.callerippro.com
- Zaba Search available at http://www.zabasearch.com
- GeoTrace available at http://www.nabber.org
- DomainHostingView available at http://www.nirsoft.net



Module Flow

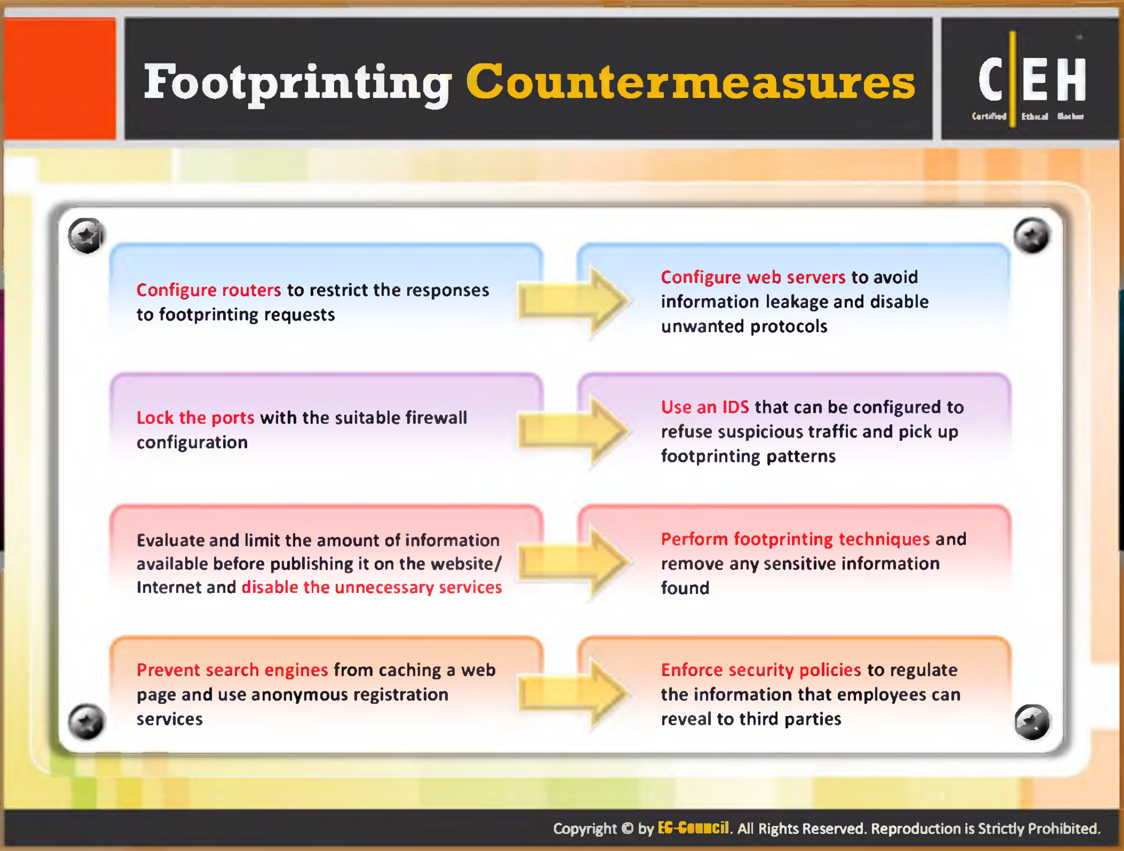
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited

Module Flow

So far we have discussed the importance of footprinting, various ways in which footprinting can be performed, and the tools that can be used for footprinting. Now we will discuss the countermeasures to be applied in order to avoid sensitive information disclosure.

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	Footprinting Penetration Testing

This section lists various footprinting countermeasures to be applied at various levels.



Footprinting Countermeasures

CEH
Certified Ethical Hacker

Configure routers to restrict the responses to footprinting requests → Configure web servers to avoid information leakage and disable unwanted protocols

Lock the ports with the suitable firewall configuration → Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns

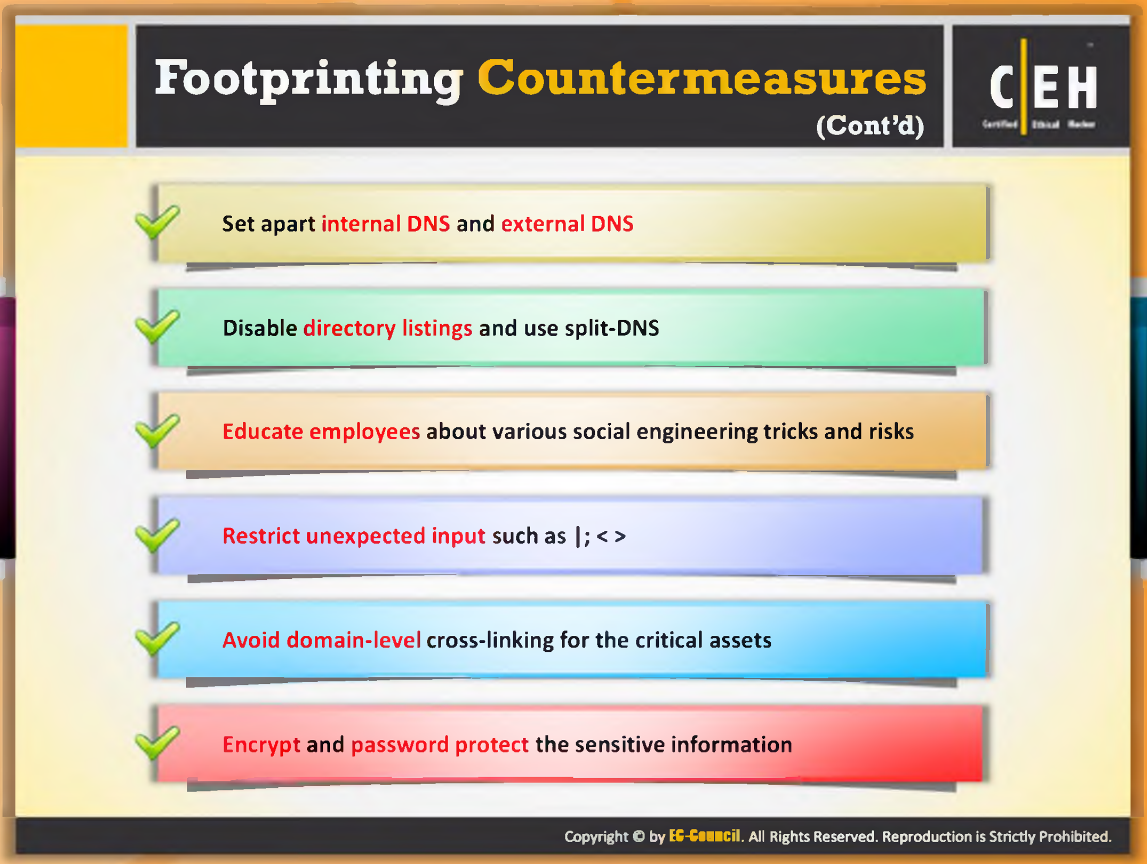
Evaluate and limit the amount of information available before publishing it on the website/ Internet and disable the unnecessary services → Perform footprinting techniques and remove any sensitive information found

Prevent search engines from caching a web page and use anonymous registration services → Enforce security policies to regulate the information that employees can reveal to third parties

Footprinting Countermeasures

Footprinting countermeasures are the measures or actions taken to counter or offset information disclosure. A few footprinting countermeasures are listed as follows:

- Configure routers to restrict the responses to footprinting requests.
- Lock the ports with suitable firewall configuration.
- Evaluate and limit the amount of information available before publishing it on the website/Internet and disable the unnecessary services.
- Prevent search engines from caching a webpage and use anonymous registration services.
- Configure web servers to avoid information leakage and disable unwanted protocols.
- Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns.
- Perform footprinting techniques and remove any sensitive information found.
- Enforce security policies to regulate the information that employees can reveal to third parties.



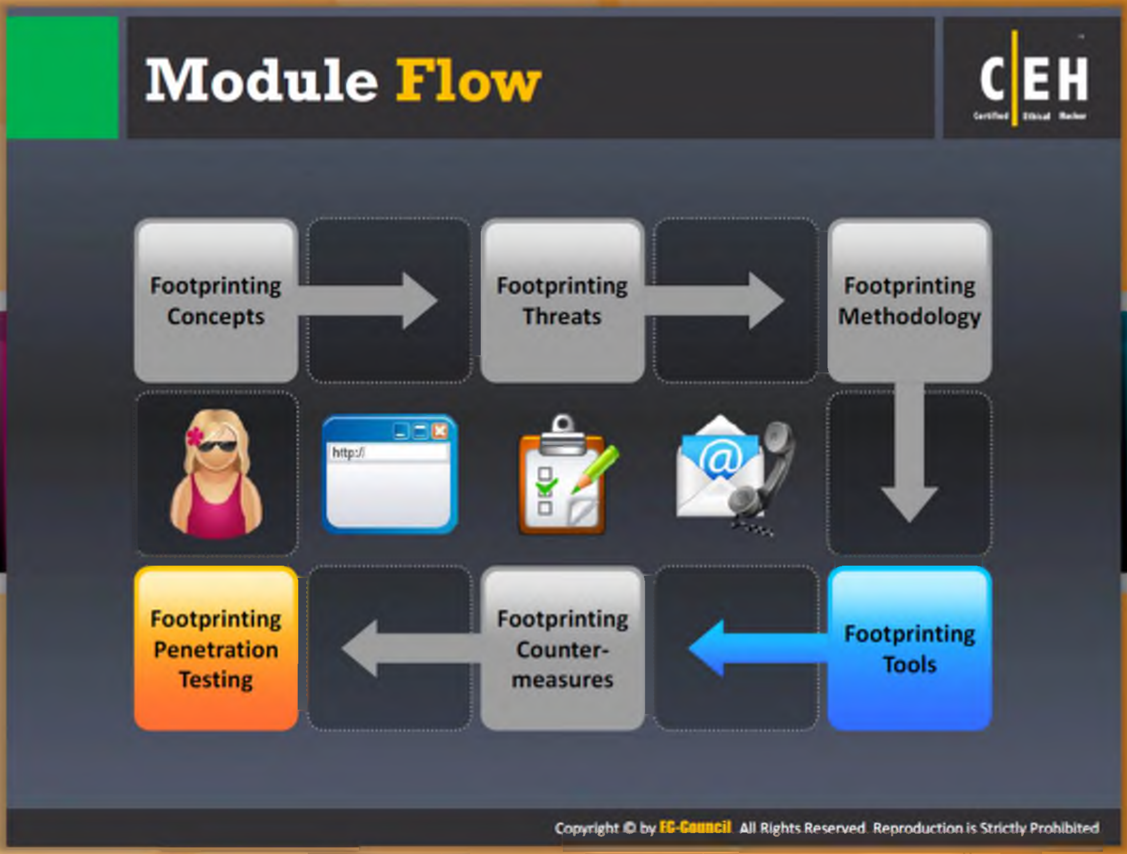
Footprinting Countermeasures (Cont'd)

- ✓ Set apart internal DNS and external DNS
- ✓ Disable directory listings and use split-DNS
- ✓ Educate employees about various social engineering tricks and risks
- ✓ Restrict unexpected input such as |; < >
- ✓ Avoid domain-level cross-linking for the critical assets
- ✓ Encrypt and password protect the sensitive information

Footprinting Countermeasures (Cont'd)

In addition to the countermeasures mentioned previously, you can apply the following countermeasures as well:

- Set apart the internal DNS and external DNS.
- Disable directory listings and use split-DNS.
- Educate employees about various **social engineering tricks** and risks.
- Restrict unexpected input such as |; < >.
- Avoid domain-level cross-linking for critical assets.
- Encrypt and password protect sensitive information.
- Do not enable protocols that are not required.
- Always use TCP/IP and IPSec filters.
- Configure IIS against banner grabbing.



Module Flow

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far we discussed all the necessary techniques and tools to test the security of a system or network. Now it is the time to put all those **techniques** into practice. Testing the security of a system or network using similar techniques as that of an attacker with adequate permissions is known as **penetration testing**. The penetration test should be conducted to check whether an attacker is able to reveal sensitive information in response to footprinting attempts.

Footprinting Concepts	Footprinting Tools
Footprinting Threats	Footprinting Countermeasures
Footprinting Methodology	**Footprinting Penetration Testing**

Penetration testing is an evaluation method of system or network security. In this evaluation method, the **pen tester** acts as a malicious outsider and simulates an attack to find the security loopholes.

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 the Internet and other publicly accessible sources

Footprinting pen testing helps administrator to:

Prevent information leakage

Prevent social engineering attempts

Prevent DNS record retrieval from publically available servers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

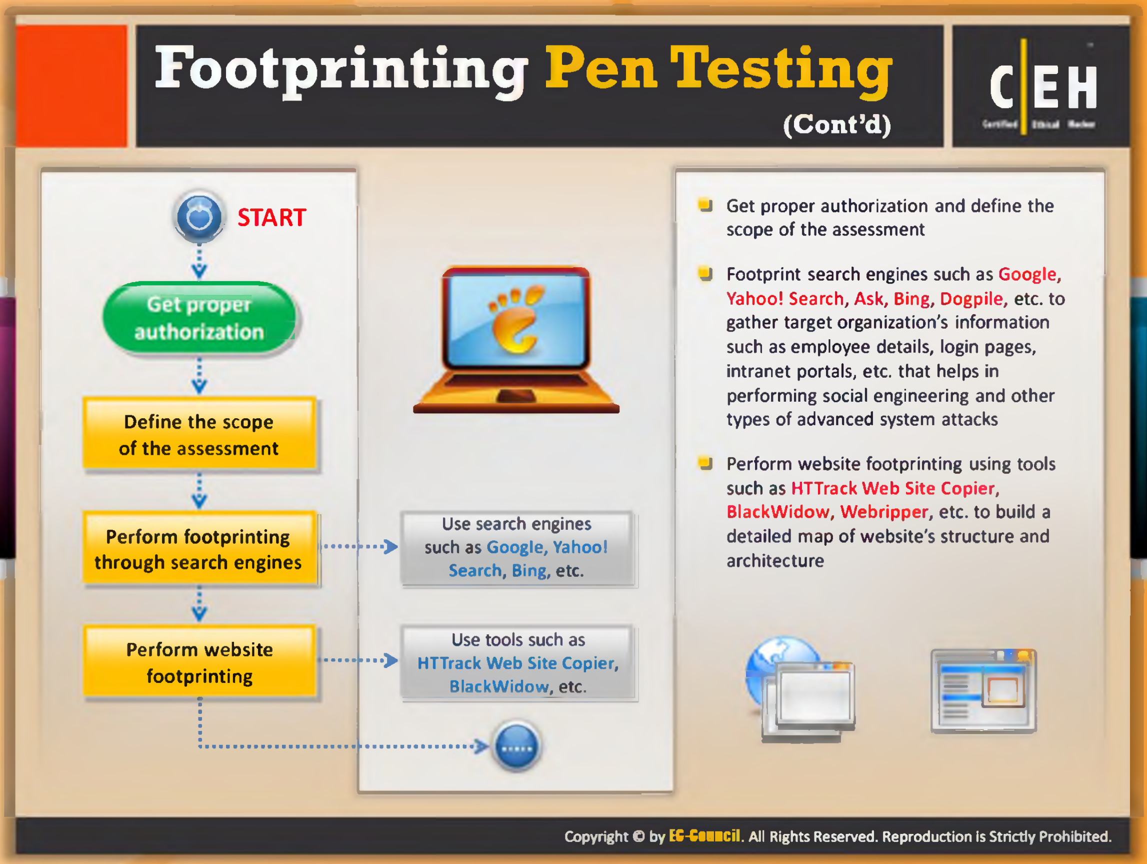
Footprinting Pen Testing

A footprinting pen test is used to determine an organization's publicly available information on the Internet such as network architecture, operating systems, applications, and users. In this method, the pen tester tries to gather publicly available sensitive information of the target by pretending to be an attacker. The target may be a specific host or a network.

The pen tester can perform any attack that an attacker could perform. The pen tester should try all possible ways to gather as much information as possible in order to ensure maximum scope of footprinting pen testing. If the pen tester finds any sensitive information on any publicly available information resource, then he or she should enter the information and the respective source in the report.

The major advantages of conducting penetration testing include:

- It gives you the chance to prevent DNS record retrieval from publically available servers.
- It helps you to avoid information leakage.
- It prevents social engineering attempts.



Footprinting Pen Testing (Cont'd)

START

Get proper authorization

Define the scope of the assessment

Perform footprinting through search engines → Use search engines such as Google, Yahoo! Search, Bing, etc.

Perform website footprinting → Use tools such as HTTrack Web Site Copier, BlackWidow, etc.

- Get proper authorization and define the scope of the assessment
- Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering and other types of advanced system attacks
- Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of website's structure and architecture

Footprinting Pen Testing (Cont'd)

Penetration testing is a procedural way of testing the security in various steps. Steps should be followed one after the other in order to ensure maximum scope of testing. Here are the steps involved in footprinting pen testing:

Step 1: Get proper authorization

Pen testing should be performed with permission. Therefore, the very first step in a footprinting pen test is to get proper authorization from the concerned people, such as administrators.

Step 2: Define the scope of the assessment

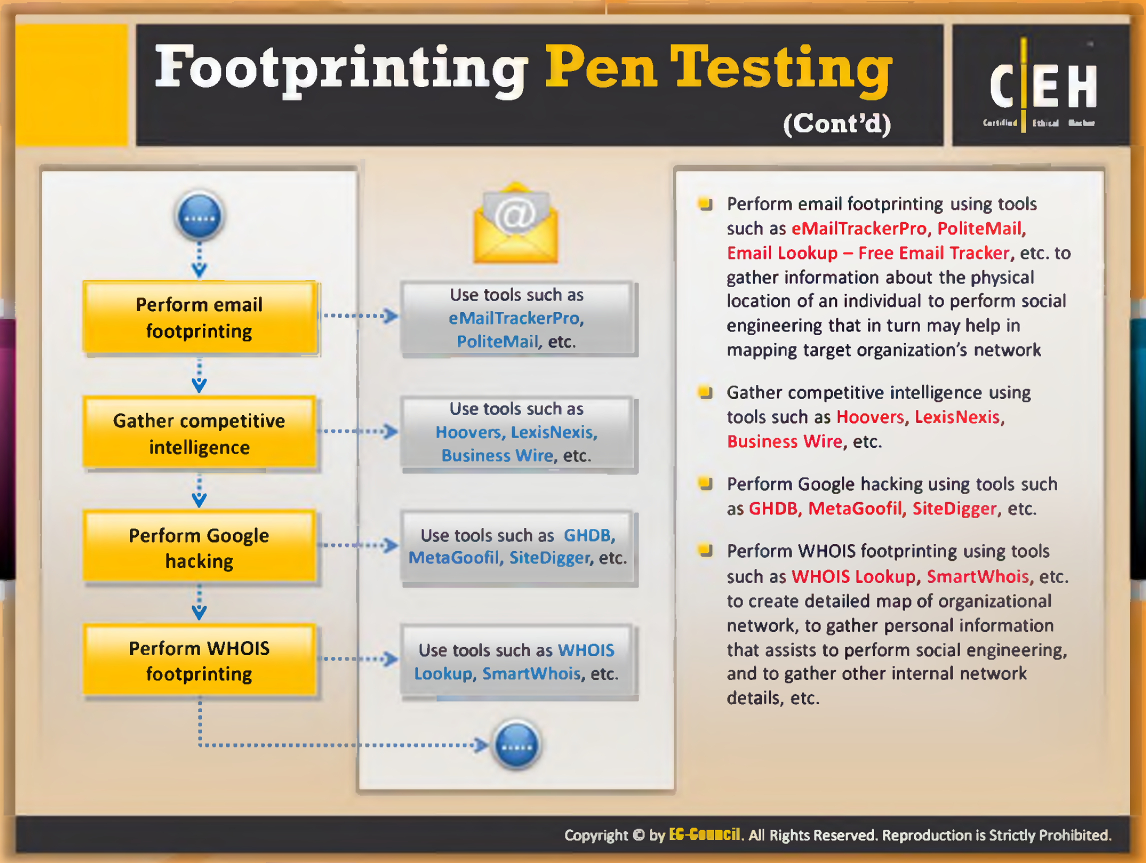
Defining the scope of the security assessment is the prerequisite for penetration testing. Defining the scope of assessment determines the range of systems in the network to be tested and the resources that can be used to test, etc. It also determines the pen tester's limitations. Once you define the scope, you should plan and gather sensitive information using various footprinting techniques.

Step 3: Perform footprinting through search engines

Footprint search engines such as Google, Yahoo! Search, Ask, Bing, Dogpile, etc. to gather the target organization's information such as employee details, login pages, intranet portals, etc. that can help in performing social engineering and other types of **advanced system attacks**.

Step 4: Perform website footprinting

Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, Webripper, etc. to build a detailed map of the **website's structure and architecture**.



Footprinting Pen Testing (Cont'd)

C|EH
Certified Ethical Hacker

Perform email footprinting → Use tools such as eMailTrackerPro, PoliteMail, etc.

Gather competitive intelligence → Use tools such as Hoovers, LexisNexis, Business Wire, etc.

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

Perform WHOIS footprinting → Use tools such as WHOIS Lookup, SmartWhois, etc.

- Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup – Free Email Tracker, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping target organization's network
- Gather competitive intelligence using tools such as Hoovers, LexisNexis, Business Wire, etc.
- Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc.
- Perform WHOIS footprinting using tools such as WHOIS Lookup, SmartWhois, etc. to create detailed map of organizational network, to gather personal information that assists to perform social engineering, and to gather other internal network details, etc.

Footprinting Pen Testing (Cont'd)

Step 5: Perform email footprinting

Perform email footprinting using tools such as eMailTrackerPro, PoliteMail, Email Lookup – Free Email Tracker, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping the target organization's network.

Step 6: Gather competitive intelligence

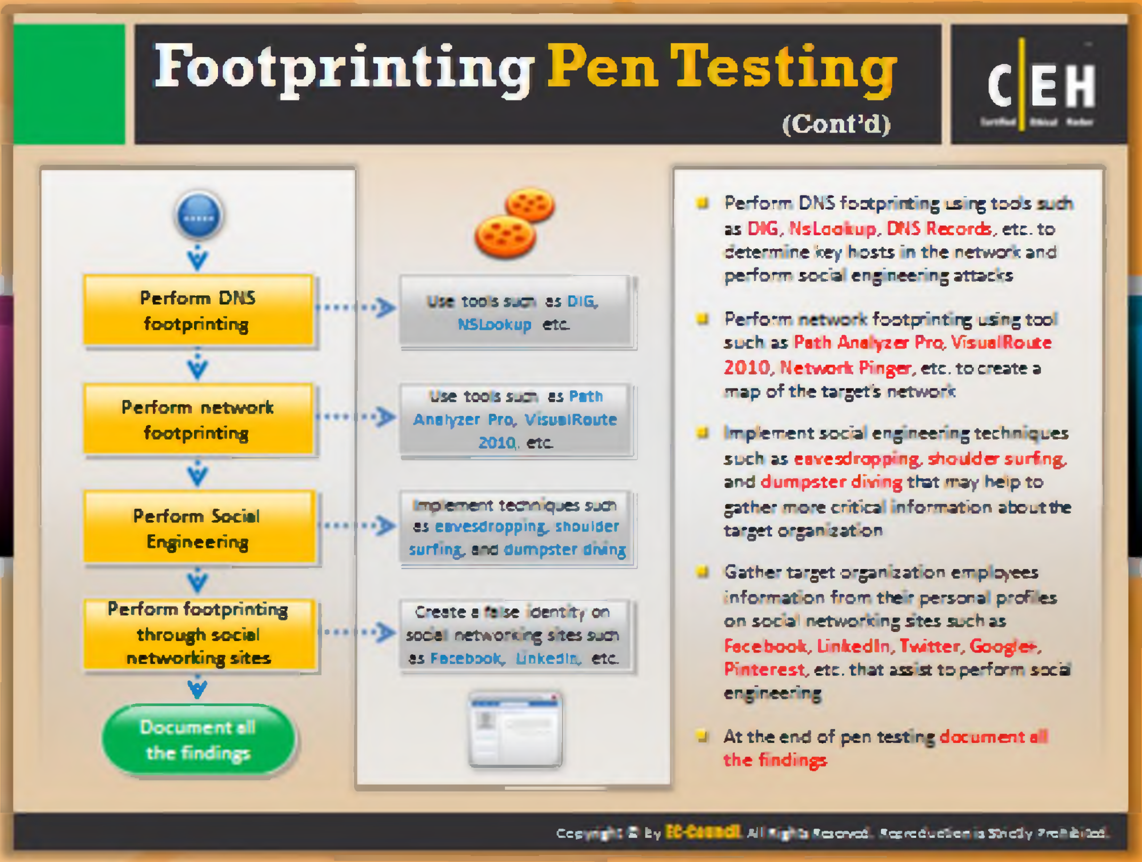
Gather competitive intelligence using tools such as Hoovers, SEC Info, Business Wire, etc. These tools help you to extract a competitor's information such as its establishment, location of the company, progress analysis, higher authorities, product analysis, marketing details, and much more.

Step 7: Perform Google hacking

Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc. It determines the security loopholes in the code and configuration of the websites. Google hacking is usually done with the help of advanced Google operators that locate specific strings of text such as versions of vulnerable web applications.

Step 8: Perform WHOIS footprinting

Perform the WHOIS **footprinting technique** to extract information about particular domains. You can get information such as domain name, IP address, domain owner name, registrant name, and their contact details including phone numbers, email IDs, etc. Tools such as SmartWhois, CountryWhois, Whois Pro, and ActiveWhois will help you to extract this information. You can use this information to perform **social engineering** to obtain more information.



Footprinting Pen Testing (Cont'd)

C|EH
Perform DNS footprinting
Use tools such as DIG, NSLookup etc.
Perform network footprinting
Use tools such as Path Analyzer Pro, VisualRoute 2010, etc.
Perform Social Engineering
Implement techniques such as eavesdropping, shoulder surfing, and dumpster diving
Perform footprinting through social networking sites
Create a false identity on social networking sites such as Facebook, LinkedIn, etc.
Document all the findings

- Perform DNS footprinting using tools such as DIG, NsLookup, DNS Records, etc. to determine key hosts in the network and perform social engineering attacks
- Perform network footprinting using tool such as Path Analyzer Pro, VisualRoute 2010, Network Pinger, etc. to create a map of the target's network
- Implement social engineering techniques such as eavesdropping, shoulder surfing, and dumpster diving that may help to gather more critical information about the target organization
- Gather target organization employees information from their personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. that assist to perform social engineering
- At the end of pen testing document all the findings

Footprinting Pen Testing (Cont'd)

Step 9: Perform DNS footprinting

Perform DNS footprinting using tools such as DIG, NsLookup, DNS Records, etc. to determine key hosts in the network and perform **social engineering attacks**. Resolve the domain name to learn about its IP address, DNS records, etc.

Step 11: Perform network footprinting

Perform network footprinting using tools such as Path Analyzer Pro, VisualRoute 2010, Network Pinger, etc. to create a map of the target's network. Network footprinting allows you to reveal the network range and other **network information** of the target network. Using all this information, you can draw the network diagram of the target network.

Step 12: Perform social engineering

Implement social engineering techniques such as **eavesdropping**, **shoulder surfing**, and dumpster diving that may help to gather more critical information about the target organization. Through social engineering you can gather **target organization's** employee details, phone numbers, contact address, email address, etc. You can use this information to reveal even more information.

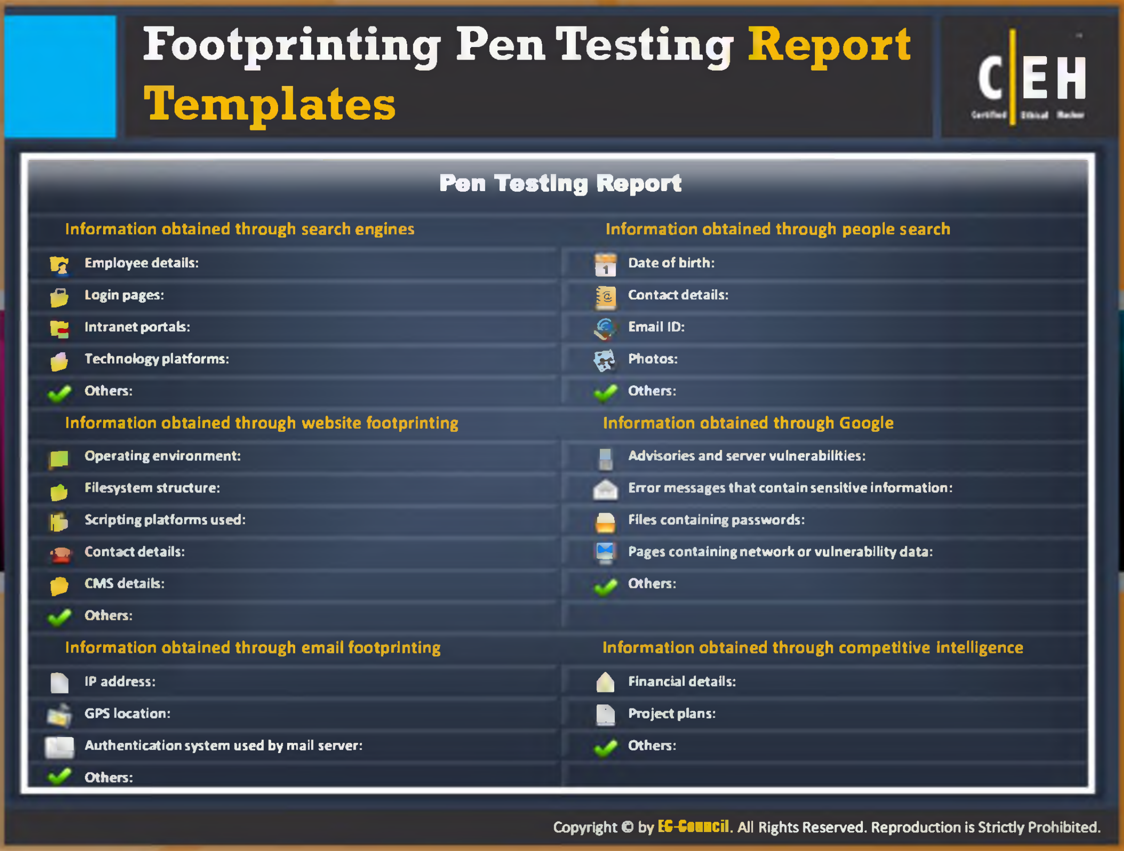
Step 13: Perform footprinting through social networking sites

Perform footprinting through social networking sites on the employees of the **target organization** obtained in footprinting through social engineering. You can gather information from their personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. that assists in **performing social engineering**. You can also use people search engines to obtain information about target person.

Step 14: Document all the findings

After implementing all the **footprinting techniques**, collect and document all the information obtained at every stage of testing. You can use this document to study, understand, and analyze the security posture of the target organization. This also enables you to find security loopholes. Once you find security loopholes, you should suggest respective countermeasures to the loopholes.

The following is a summary of footprinting **penetration testing**.



Footprinting Pen Testing Report Templates

Pen Testing Report

Information obtained through search engines

- Employee details:
- Login pages:
- Intranet portals:
- Technology platforms:
- ✓ Others:

Information obtained through website footprinting

- Operating environment:
- Filesystem structure:
- Scripting platforms used:
- Contact details:
- CMS details:
- ✓ Others:

Information obtained through email footprinting

- IP address:
- GPS location:
- Authentication system used by mail server:
- ✓ Others:

Information obtained through people search

- Date of birth:
- Contact details:
- Email ID:
- Photos:
- ✓ Others:

Information obtained through Google

- Advisories and server vulnerabilities:
- Error messages that contain sensitive information:
- Files containing passwords:
- Pages containing network or vulnerability data:
- ✓ Others:

Information obtained through competitive intelligence

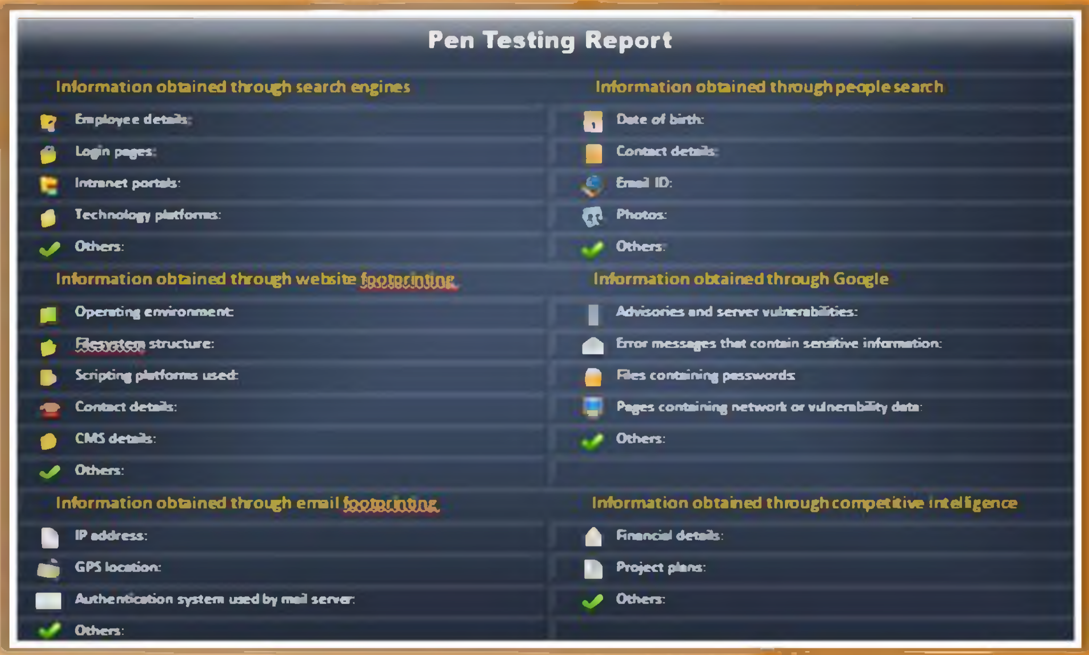
- Financial details:
- Project plans:
- ✓ Others:

Footprinting Pen Testing Report Templates

Pen Testing Report

Penetration testing is usually conducted to enhance the **security perimeter** of an organization. As a pen tester you should gather sensitive information such as server details, the operating system, etc. of your target by conducting footprinting. Analyze the system and network defenses by breaking into its security with **adequate permissions** (i.e., ethically) without causing any damage. Find the loopholes and weaknesses in the network or system security. Now explain all the **vulnerabilities** along with respective countermeasures in a report, i.e., the pen testing report. The pen testing report is a report obtained after performing network penetration tests or security audits. It contains all the details such as types of tests performed, the **hacking techniques** used, and the results of hacking activity. In addition, the report also contains the highlights of security risks and vulnerabilities of an organization. If any vulnerability is identified during any test, the details of the cause of vulnerability along with the countermeasures are suggested. The report should always be kept **confidential**. If this information falls into the hands of attacker, he or she may use this information to launch attacks.

The pen testing report should contain the following details:



Pen Testing Report

Information obtained through search engines

- Employee details:
- Login pages:
- Intranet portals:
- Technology platforms:
- Others:

Information obtained through people search

- Date of birth:
- Contact details:
- Email ID:
- Photos:
- Others:

Information obtained through website footprinting

- Operating environment:
- Filesystem structure:
- Scripting platforms used:
- Contact details:
- CMS details:
- Others:

Information obtained through Google

- Advisories and server vulnerabilities:
- Error messages that contain sensitive information:
- Files containing passwords:
- Pages containing network or vulnerability data:
- Others:

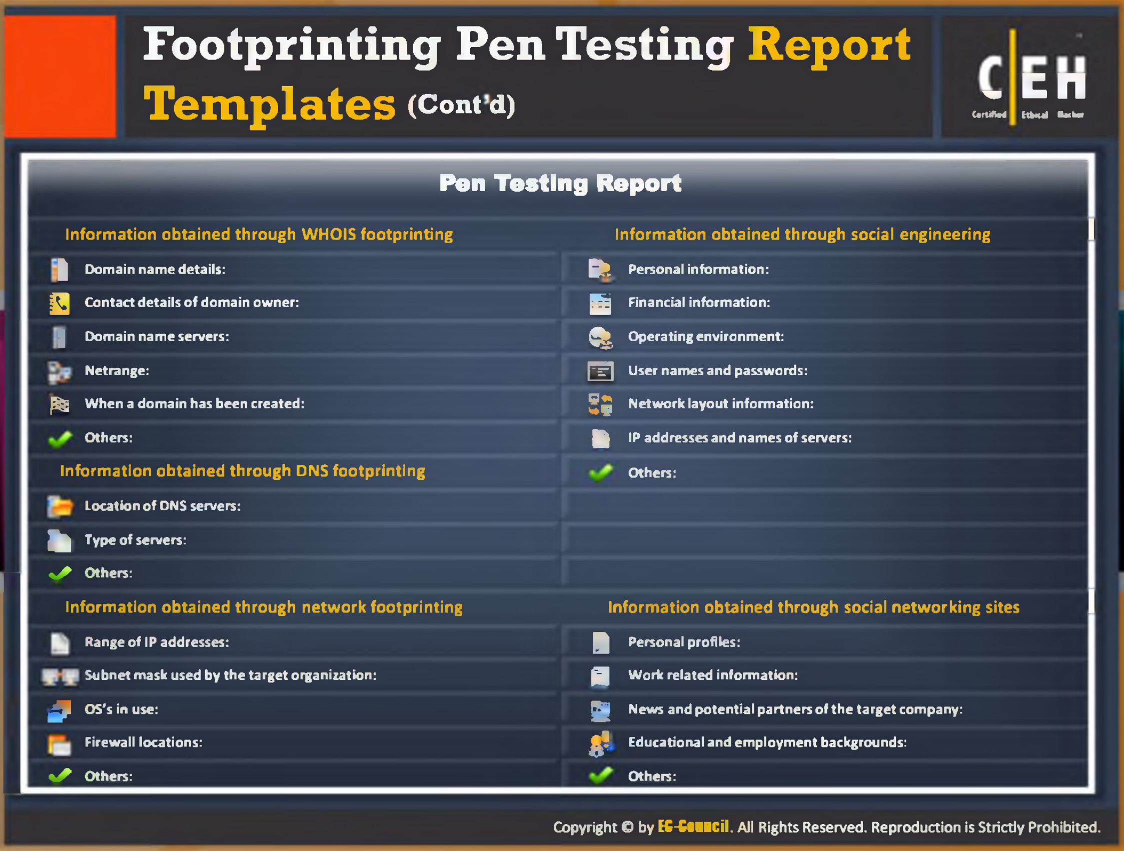
Information obtained through email footprinting

- IP address:
- GPS location:
- Authentication system used by mail server:
- Others:

Information obtained through competitive intelligence

- Financial details:
- Project plans:
- Others:

FIGURE 2.48: Pen Testing Report



Footprinting Pen Testing Report Templates (Cont'd)

Pen Testing Report

Information obtained through WHOIS footprinting

- Domain name details:
- Contact details of domain owner:
- Domain name servers:
- Netrange:
- When a domain has been created:
- ✓ Others:

Information obtained through DNS footprinting

- Location of DNS servers:
- Type of servers:
- ✓ Others:

Information obtained through social engineering

- Personal information:
- Financial information:
- Operating environment:
- User names and passwords:
- Network layout information:
- IP addresses and names of servers:
- ✓ Others:

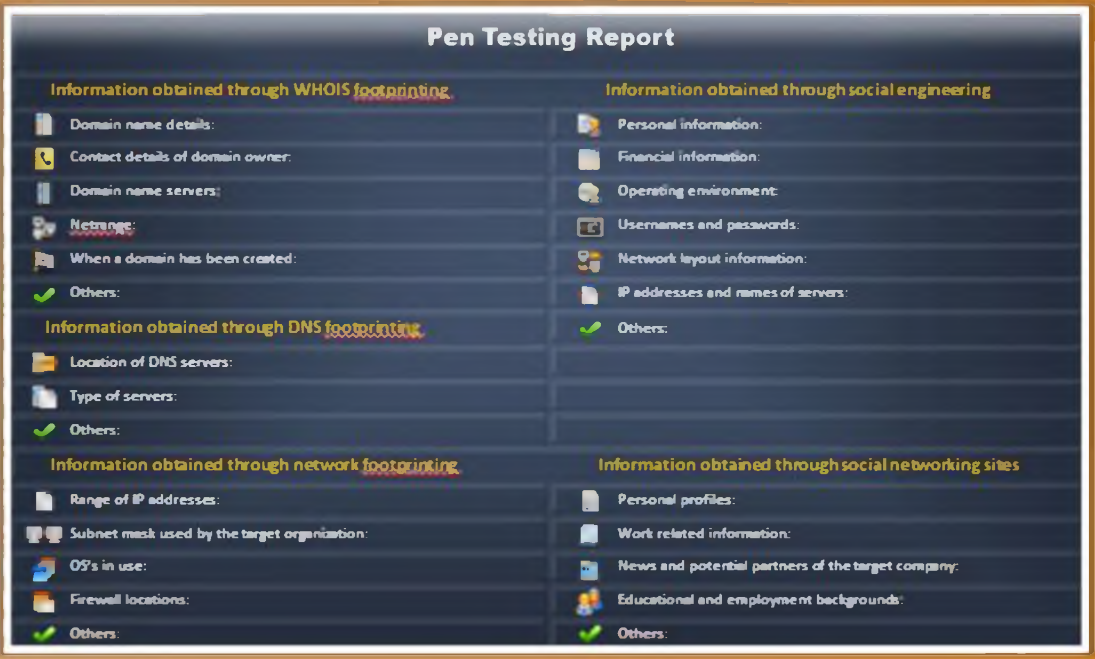
Information obtained through network footprinting

- Range of IP addresses:
- Subnet mask used by the target organization:
- OS's in use:
- Firewall locations:
- ✓ Others:

Information obtained through social networking sites

- Personal profiles:
- Work related information:
- News and potential partners of the target company:
- Educational and employment backgrounds:
- ✓ Others:

Footprinting Pen Testing Report Templates (Cont'd)



Pen Testing Report

Information obtained through WHOIS footprinting

- Domain name details:
- Contact details of domain owner:
- Domain name servers:
- Netrange:
- When a domain has been created:
- ✓ Others:

Information obtained through DNS footprinting

- Location of DNS servers:
- Type of servers:
- ✓ Others:

Information obtained through social engineering

- Personal information:
- Financial information:
- Operating environment:
- Usernames and passwords:
- Network layout information:
- IP addresses and names of servers:
- ✓ Others:

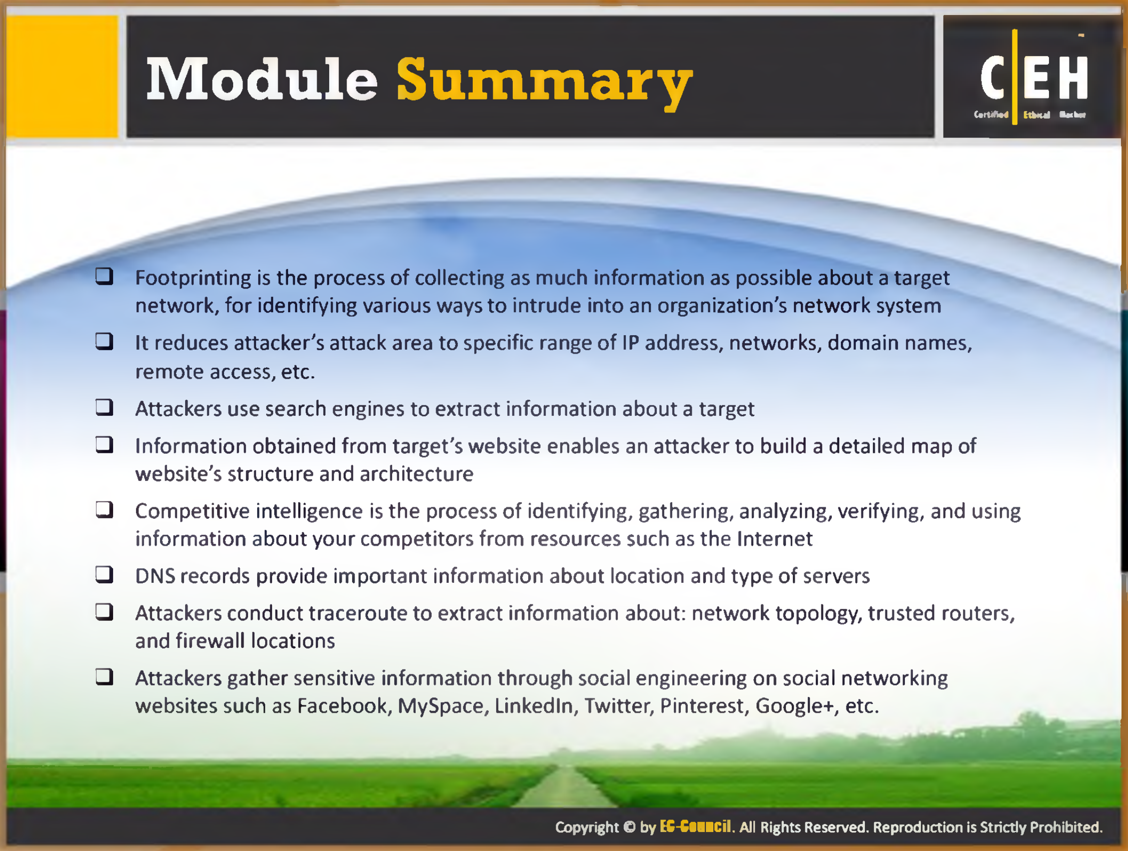
Information obtained through network footprinting

- Range of IP addresses:
- Subnet mask used by the target organization:
- OS's in use:
- Firewall locations:
- ✓ Others:

Information obtained through social networking sites

- Personal profiles:
- Work related information:
- News and potential partners of the target company:
- Educational and employment backgrounds:
- ✓ Others:

FIGURE 2.49: Pen Testing Report showing information obtained through footprinting and social engineering



Module Summary

CEH
Certified Ethical Hacker

- ❑ Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system
- ❑ It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- ❑ Attackers use search engines to extract information about a target
- ❑ Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture
- ❑ Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet
- ❑ DNS records provide important information about location and type of servers
- ❑ Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations
- ❑ Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

Module Summary

- Footprinting refers to uncovering and collecting as much information as possible about a target of attack.
- It reduces attacker's attack area to specific range of IP address, networks, domain names, remote access, etc.
- Attackers use search engines to extract information about a target.
- Information obtained from target's website enables an attacker to build a detailed map of website's structure and architecture.
- Competitive intelligence is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet.
- DNS records provide important information about location and type of servers.
- Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations.
- Attackers gather sensitive information through social engineering on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.