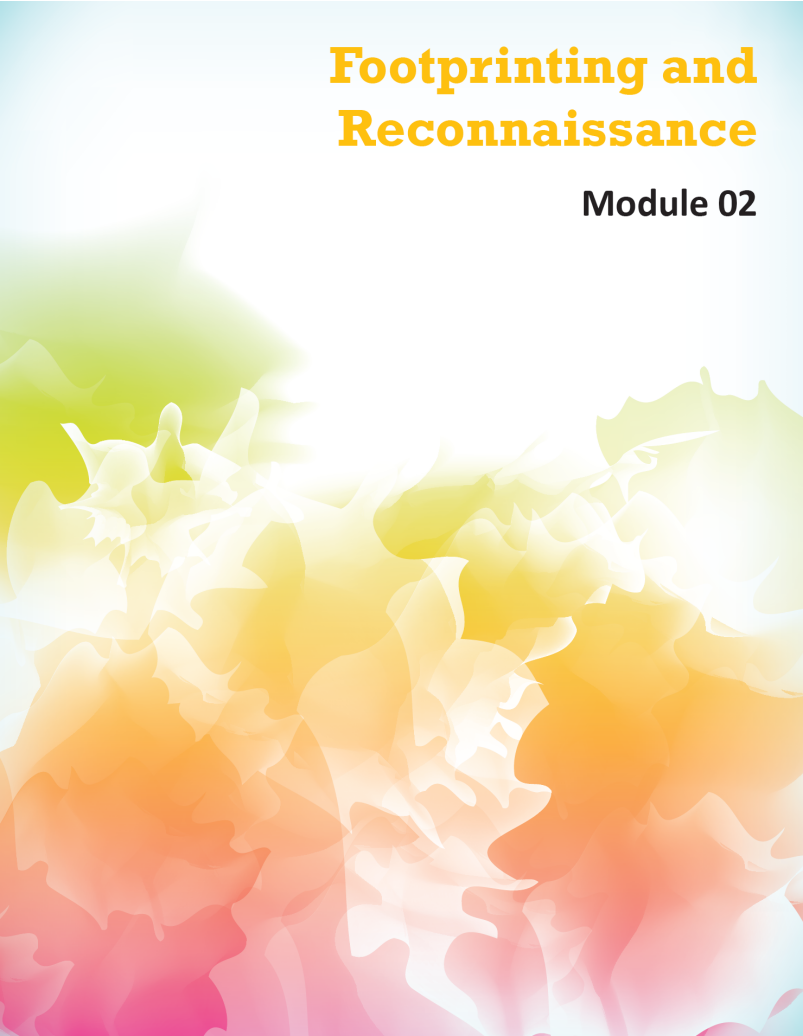
Footprinting and Reconnaissance

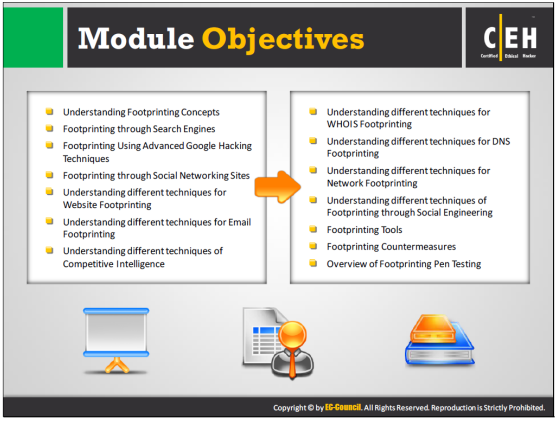
Module 02



Ethical Hacking and Countermeasures v9

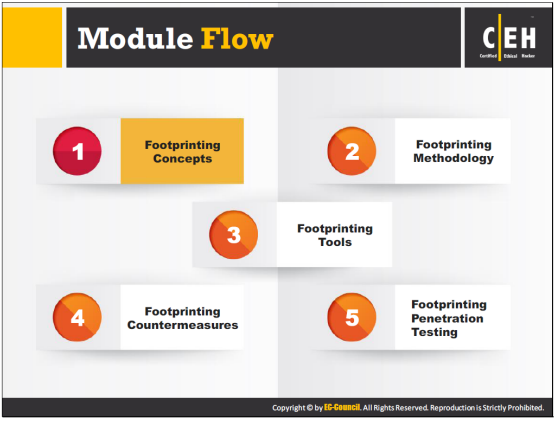
Module 02: Footprinting and Reconnaissance

Exam 312-50



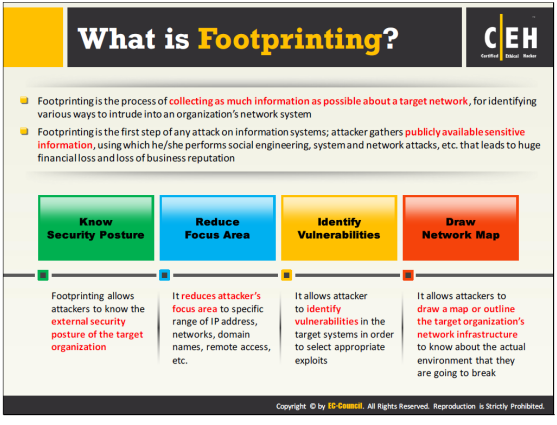
Footprinting is a first step in the evaluation of the security posture of the target organization's IT infrastructure. Through footprinting and reconnaissance, one can gather maximum information about the computer system or a network and about devices connected to that network. In other words, footprinting gives the blueprint of the security profile for an organization, and should be undertaken in a methodological manner.

This module starts with an introduction to footprinting concepts and provides an insight into footprinting methodology. Later the module discusses footprinting tools and countermeasures. The module ends with an overview of penetration (pen) testing steps that an ethical hacker should follow to perform the security assessment of a target.



Ethical hacking is legal in nature and conducted in order to evaluate the security of a target organization's IT infrastructure with their consent. Footprinting is the first step in ethical hacking, where an attacker tries to gather information about a target.

The footprinting concepts section familiarizes you with footprinting, why footprinting is necessary, and the objectives of 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.

After you complete the footprinting process in a methodological manner, you will obtain the blueprint of the security profile of the target organization. Here the term "blueprint" refers to the unique system profile of the target organization acquired by footprinting.

There is no single methodology for footprinting, as you can trace information in various ways. However, this activity is important, as you need to gather all crucial information about the target organization before beginning the hacking phase. You should carry out footprinting in an organized manner.

You can collect information about the target organization 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. Track physical location and perform social engineering

Using this information, we will discuss how to find and exploit vulnerabilities in detail.

Footprinting Threats

Attackers perform footprinting as the first step of any attack on information systems. In the footprinting phase, attackers try to collect valuable system-level information such as account details, operating system and other software versions, server names, database schema details, etc. 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, the hackers gather crucial information from willing employees who are unaware of the hackers' intent.

- **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 vulnerabilities in the target system and then exploit those vulnerabilities. Attackers can then take control over a target system or the entire network.

- **Information Leakage**

  Information leakage can pose a threat to any organization. If sensitive information of an organization falls into the hands of attackers, they can build an attack plan based on the information, or use it for monetary benefit.

- **Privacy Loss**

  With the help of footprinting, hackers are able to access the systems and networks of the organization and even escalate the privileges up to admin levels, resulting in the loss of privacy maintained by the organization.

- **Corporate Espionage**

  Corporate espionage is one of the major threats to organizations, 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 target organization.

- **Business Loss**

  Footprinting has a major effect on organizations 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.

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 through the

organization's security perimeter. As mentioned previously, footprinting methodology makes it easy 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 gives the complete profile of the organization's security posture. Hackers can analyze this report to figure out loopholes in the security posture of the target organization and then build a hacking plan accordingly.

- **Reduce Focus Area**

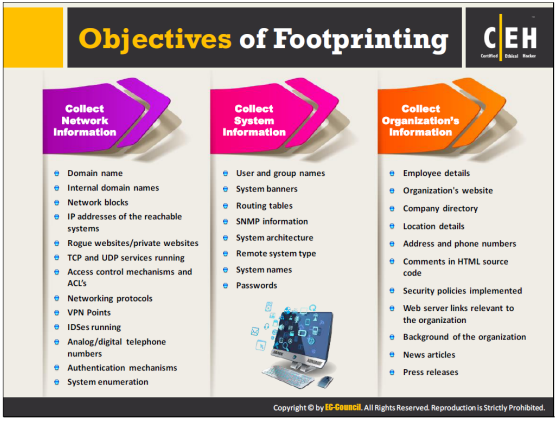
  By using a combination of tools and techniques, attackers can take an unknown entity (for example, XYZ Organization) and reduce it to a specific range of domain names, network blocks, and individual IP addresses of systems directly connected to the Internet, as well as many other details pertaining to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

- **Identify Vulnerabilities**

  A detailed footprint provides maximum information about the target organization. Attackers can build their own information database about security weaknesses of the target organization. This database helps in finding the easiest way to break through the organization's security perimeter.

- **Draw Network Map**

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

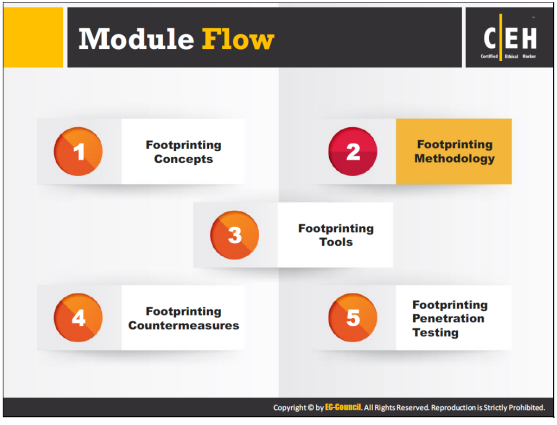


The major objectives of footprinting include collecting the target's network information, system information, and the organizational information. By carrying out footprinting at various network levels, you can gain information such as network blocks, network services and applications, system architecture,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

Collect Network Information: An attacker performs whois database analysis, trace routing, etc. to gather network information. Thereafter the attacker may gain access to sensitive data or may attack the network.

Collect System Information: Prior to performing an attack, an attacker must identify the vulnerabilities to exploit in order to gain access to a system. Once the attacker gains system access, he can use various tools and utilities to perform illegal activities such as stealing sensitive data, attacking other systems, sending forged emails from the system, etc.

Collect Organization's Information: An attacker can obtain information about an organization from its website. In addition, they can query the target's domain name against the whois database and get valuable information such as location, people's names, phone numbers, etc. The information can then identify key employees in the company and launch social engineering attacks to extract sensitive data about the organization.



Now that you are familiar with footprinting concepts and threats, we will discuss footprinting methodology. The footprinting methodology section discusses various techniques used to collect information about the target organization from different sources.

Footprinting methodology is a procedure for collecting information about a target organization from all available sources. It involves gathering information about a target organization such as URLs, locations, establishment details, number of employees, the specific range of domain names, contact information, etc. Attackers collect this information from various publicly accessible sources such as search engines, whois databases, etc.

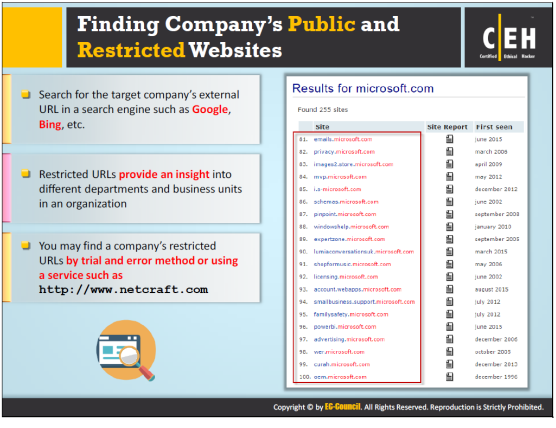
Search engines are the main information sources to find valuable information about a target organization.

Examples of search engines include Google, Yahoo, and Bing.

A search engine searches for information on the World Wide Web. It returns a list of Search Engine Results Pages (SERPs). Many search engines can extract target organization 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. Attackers sometimes discover even the network diagrams, which enable them to launch an attack.

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.

As an ethical hacker, if you find any deleted pages/information about your company in SERPs or search engine cache, then request search engine to remove the page/information from their indexed cache.



A company's public and restricted URLs provide a lot of useful information to the attacker.

A public website is designed to show the presence of an organization on the Internet. It is available for free access and is accessible by anyone. It is designed to attract customers and partners. It may contain information such as organization history, services and products, and contact information for the organization. The target organization's external URL can be located with the help of search engines such as Google or Bing.

A restricted website is available to only a few people. The people may be employees of an organization, members of a department, etc. Access restrictions can be applied based on the IP address, domain or subnet, username, and password. The restricted URL helps to access the private functions of an organization. Most organizations use common formats for restricted URLs. Therefore, a hacker who knows the external URL of a company can often discover the restricted URL through trial and error, or by using a service such as netcraft.com. These restricted URLs provide insight into different departments and business units in an organization.

Tools to Search Restricted URLs

Tools to search restricted URLs include:

Netcraft

Source: *http://www.netcraft.com*

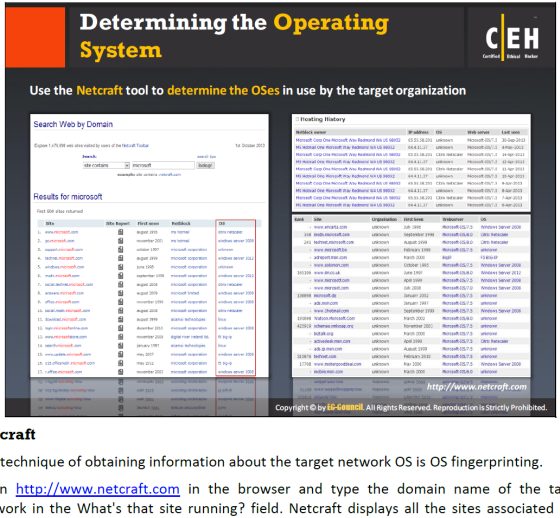
Netcraft provides internet security services including anti-fraud and anti-phishing services, application testing and PCI scanning. They also analyse many aspects of the internet, including

the market share of web servers, operating systems, hosting providers and SSL certificate authorities

Link Extractor

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

Link Extractor is a utility that allows the user to choose between external and internal URLs, and will return a plain list of URLs linked to or an html list. This utility can be used to extract links of a target organization.

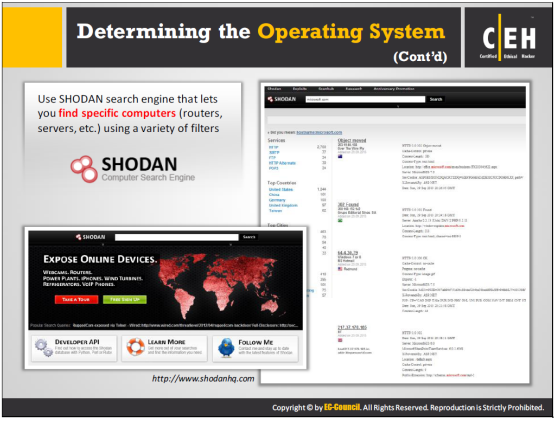


Netcraft

The technique of obtaining information about the target network OS is OS fingerprinting.

Open http://www.netcraft.com in the browser and type the domain name of the target network in the What's that site running? field. Netcraft displays all the sites associated with that domain along with the operating system running at each site.

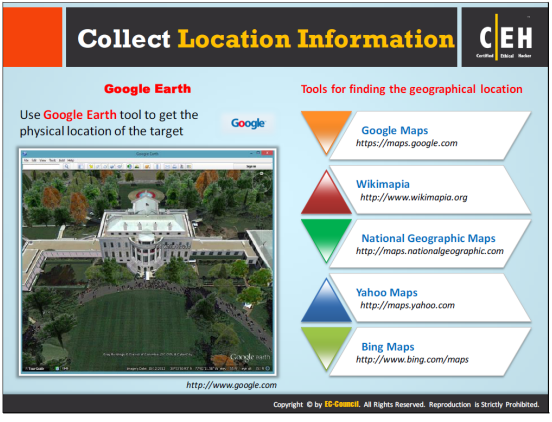
Source: *http://www.netcraft.com*



Shodan Search Engine

Shodan is the computer search engine that searches the Internet for computers. It allows the user to find devices based on city, country, latitude/longitude, hostname, operating system, and IP address. It also allows the user to search for known vulnerabilities and exploits across Exploit DB, Metasploit, CVE, OSVDB, and Packetstorm with a single interface.

Source: *http://www.shodanhq.com*



Information such as physical location of the organization plays a vital role in the hacking process. Attackers can obtain this information using footprinting. In addition to physical location, a hacker 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 more information about the target organization. Once the attackers know location of the target, they can obtain detailed satellite images of the location using various sources available on the Internet such as Google Earth, Google Maps, etc. Attackers can use this information to gain unauthorized access to buildings, wired and wireless networks, systems, etc.

Example: earth.google.com

The Google Earth tool allows you to find and explore any location on the earth. It can even access 3D images that depict most of the Earth in high-resolution detail.

Location Finding Tools

Tools to find the geographical location of a target include:

Google Maps

Source: *https://maps.google.com*

Google Maps provides a Street View feature that provides you with a series of displays images of buildings, as well as 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.

Wikimapia

Source: http://www.wikimapia.org

"WikiMapia is an open-content collaborative mapping project, aimed at marking all geographical objects in the world and providing a useful description of them." It aims to create and maintain a free, complete, multilingual, and up-to-date map of the whole world. Wikimapia intends to contain detailed information about every place on Earth.

It provides a Google Maps API-based interactive web map that consists of user-generated information layered on top of Google Maps satellite imagery and other resources. The navigation interface provides scrolling and zoom functionality similar to that of Google Maps.

National Geographic Maps

Source: http://maps.nationalgeographic.com

National Geographic Maps is responsible for illustrating the world through the art and science of mapmaking. It provides interactive maps, outline maps, satellite imagery, and information on how to interact with and create one's own maps.

Yahoo! Maps

Source: http://maps.yahoo.com

Yahoo! Maps is an online mapping portal provided by Yahoo! It emphasizes local online maps and driving directions, though international maps are available. Yahoo! Maps is available with the Yahoo! search engine to offer detailed information about businesses and points of interest on a map, although the business profiles in Yahoo! are not as extensive as that of Google. Features like traffic conditions and easy map upload by email or text message make Yahoo! Maps a competitive site for users of online maps.

Bing Maps

Source: http://www.bing.com/maps

Bing Maps is a web mapping service provided as a part of Microsoft's Bing suite of search engines and powered by the Bing Maps for Enterprise framework. The user can use the search box that appears at the top of Bing Maps to locate places, businesses, landmarks, and people. Search results include addresses, contact information, and reviews for businesses and landmarks.

People Search on Social Networking Sites

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 contain information that users provide in their profiles. These websites help to directly or indirectly relate people to each other through various fields such as common interests, work location, educational communities, etc.

Social networking sites allow people to share information quickly and effectively, as they can update these sites in real time. The sites allow updating facts about upcoming or current events, recent announcements and invitations, and so on. Social networking sites are a great platform for searching for people and their related information. Through people searching on social networking services, an attacker 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 registering on the site; this makes people searching on social networking sites an easy task. A user can search a person using name, email, or address. Some sites allow users to check whether or not an account is active, which then provides information on the status of the person being searched.

Examples of Social Networking Sites:

LinkedIn

Source: *http://www.linkedin.com*

LinkedIn is a social networking website for professionals. It allows a user to find people by name, keyword, company, school, etc. Searching for people on LinkedIn returns information such as name, position, organization name, current location, and educational qualifications.

Facebook

Source: *http://www.facebook.com*

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

FIGURE 2.1: Screenshot of Social Networking Service - Facebook

Twitter

Source: *http://twitter.com*

Twitter is a social networking service that allows people to send and read text messages (tweets). People increasingly use Twitter to share advice, news, concerns, opinions, rumors, facts, etc. Posted tweets are public and are available for mining.

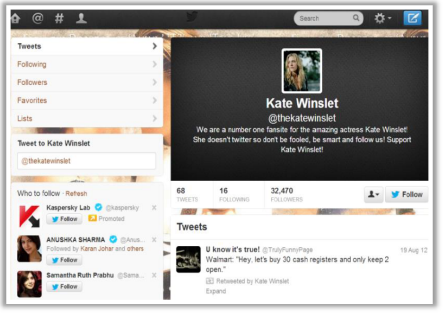


FIGURE 2.2: Screenshot of Social Networking Service - Twitter

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. A hacker can retrieve a lot of useful information about users of this site and use it to hack their systems.

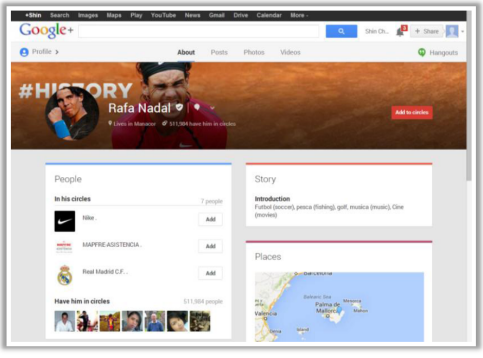


FIGURE 2.3: Screenshot of Social Networking Service - Google+

People Search on People Search Services

A user can use public record websites to find information about email addresses, phone numbers, house addresses, and other information. Using this information a hacker can try to obtain bank details, credit card details, past history, etc. There are many people search online services available that help find people. Examples of such people search services include pipl, AnyWho, etc.

pipl

Source: *https://pipl.com*

pipl is an online people search tool to find other users through their name, email, username or phone number. It has an Identity Resolution engine that focuses on finding the right person and provides accurate results for people search.

Many individuals use people search online services to find information about other people. Generally, people search online services provide people's names, addresses, and contact details. Some people search online services may also reveal the type of work an individual does, businesses owned by a person, contact numbers, company email addresses, cell phone numbers, fax numbers, dates of birth, personal e-mail addresses, etc. This information proves to be highly beneficial for attackers to launch attacks.

Some of the people search online services include:

AnyWho

Source: *http://www.anywho.com*

AnyWho provides an online white pages directory that lists people by name, address or phone number. For best results, one needs to include both the first and last name. If present, input the ZIP Code as well.

US Search

Source: *http://www.ussearch.com*

US Search can find people anywhere in the US. It helps to search people and their contact information by name, address, or phone number. It provides detailed information about a person that includes current address, phone numbers, address history, email, social networking profiles, household members, home values, optional background an criminal checks, etc.

Intelius

Source: http://www.intelius.com

Intelius helps to find people info with people search, reverse phone lookup, and background check services. People search reports delivered by Intelius include name, address, aliases, phone numbers, address history, age and date of birth, relatives, etc.

411

Source: http://www.411.com

411 is a directory assistance site used to find businesses, people, reverse phone, reverse address, area, and zip codes.

PeopleFinders

Source: http://www.peoplefinders.com

PeopleFinders helps to find people by name, phone number, address, or email to obtain public records about them. People search information fetched by PeopleFinders includes address, phone number, friends, family, former classmates, etc.

PeopleSmart

Source: http://www.peoplesmart.com

PeopleSmart is a comprehensive people search and lookup site that offers a variety of information from reverse phone lookups to background checks. Users can initiate searches for people by giving their name, email, phone number and address. It assists consumers, businesses, and professionals in finding contact information, reverse phone lookups, email searches, background checks, social networking profiles, criminal records, etc.

Veromi

Source: http://www.veromi.net

Veromi.net helps to find people and learn more about them via background reports, people searches and other public records reports. Searches are performed by name, address or phone number. The site returns information that includes name, date of birth, address, phone number, possible relatives, etc.

PrivateEye

Source: http://www.privateeye.com

Private Eye allows a user to find people and learn more about them by entering name, address or phone number. The report delivered includes full name, date of birth, age, address history, phone numbers, aliases, possible relatives, etc.

People Search Now

Source: http://www.peoplesearchnow.com

PeopleSearchNow helps users find people in the United States. It is a comprehensive people search service that provides high-quality information, from basic contact information to in-

depth background checks. It gives information such as name, phone number, address, email ID, aliases, relatives, etc.

Public Background Checks

Source: *http://www.publicbackgroundchecks.com*

Public Background Checks searches for people by name, address, and phone number. It provides information such as addresses, phone numbers, dates of birth, relatives, property records, address history, business records, property information, etc.

Attackers who seek access to personal information or financial information often target financial data such as bank or credit card details. Financial services such as Google Finance, Yahoo! Finance, etc., 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 other. Financial firms rely on web services to perform transactions and grant users access to their accounts. Attackers can obtain sensitive and private information about these firms and users by using malware, exploiting software design flaws, breaking authentication mechanisms, service flooding, brute force attack, phishing, etc.

Google Finance

Source: *https://www.google.com/finance*

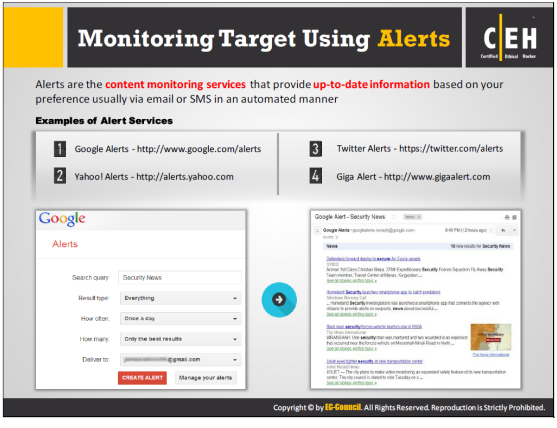
Google finance service features business and enterprise headlines for many corporations, including their financial decisions and major news events. Stock information is available, as are stock price charts that contain marks for major news events and corporate actions. The site also aggregates Google news and Google blog search articles about each corporation.

Yahoo! Finance

Source: *http://finance.yahoo.com*

Yahoo! Finance provides financial information and commentary with a focus on US markets. The website offers information such as stock quotes, stock exchange rates, corporate press releases and financial reports, original programming video clips, and message boards. It also offers some online tools for personal finance management. Yahoo! Finance Worldwide offers similar features for international finance markets.

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. Many organizations' websites provide recruiting information on a job posting page that in turn reveals hardware, network-related information and technologies used by the company (e.g., firewall, Internal server type, OS used, network appliances, etc.). In addition, the website may have a key employee list with email addresses. All this information may prove to be beneficial for an attacker. For example, if an organization advertises a Network Administrator job, it posts the requirements related to that position.



Alerts are content monitoring services that provide automated up-to-date information based on user preference, usually via email or SMS. To receive alerts, a user must register on the website and provide either an email address or phone number. Attackers can gather updated information about the target periodically from the alert services and use it for further attacks.

Google Alerts

Source: *http://www.google.com/alerts*

Google Alerts 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, keeping current on a competitor or industry, getting the latest on a celebrity or event, and keeping tabs on sports teams.

Yahoo! Alerts

Source: *http://alerts.yahoo.com*

A registered Yahoo user can use Yahoo! Alerts to receive alerts via email, Yahoo Messenger, or a mobile device. Yahoo! Alerts allows monitoring of the web through Yahoo search for new content related to a set of keywords or search criteria.

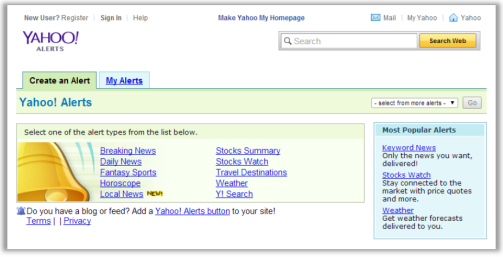


FIGURE 2.4: Screenshot of Yahoo! Alerts for Monitoring Target

Twitter Alerts

Source: *https://twitter.com/alerts*

Twitter Alerts helps users get important and accurate information from credible organizations during emergencies, natural disasters or when other communications services are not accessible. Twitter Alerts appear on subscribers' phones as push and/or SMS notifications when authoritative accounts mark Tweets as alerts.

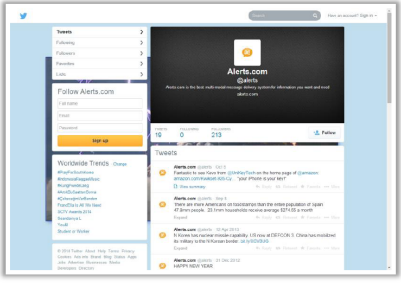


FIGURE 2.5: Screenshot of Twitter Alerts for Monitoring Target

Giga Alert

Source: *http://www.gigaalert.com*

Giga Alert is a leading automated search and web intelligence solution for monitoring professional interests online. It tracks the web for personalized topics and sends new results by daily email. It helps to manage reputation, monitor competitors, and generate critical leads for an organization. It also helps track mentions of the organization's name, member names, website, or any people or projects that are important.

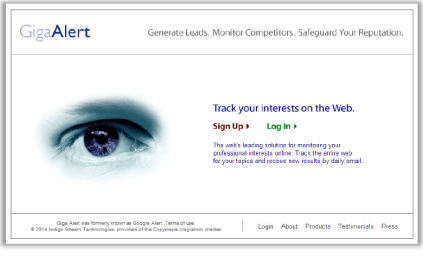
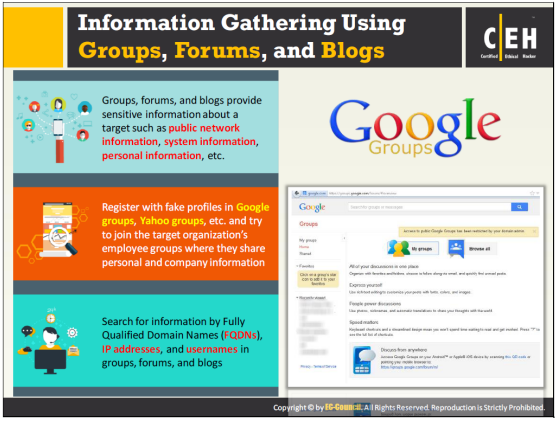


FIGURE 2.6: Screenshot of Giga Alert for Monitoring Target

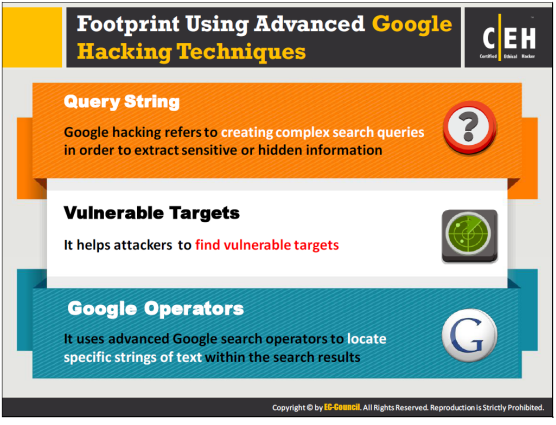


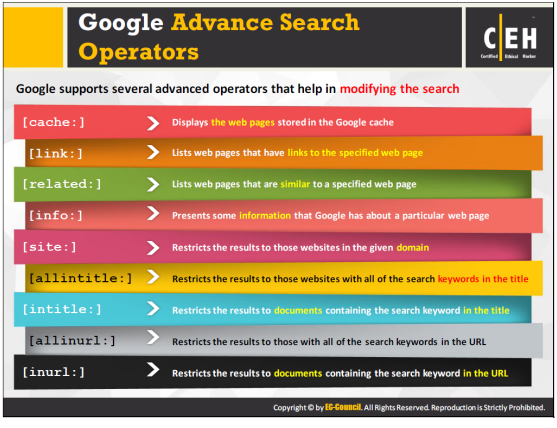
Many Internet users use blogs, groups, and forums for knowledge sharing purposes. Therefore, attackers focus on groups, forums, and blogs to find information about a target organization and its people. Organizations do not monitor the exchange of information that employees reveal to other users in forums, blogs, and group discussions. Attackers see this as an advantage and collect sensitive information about the target such as public network information, system information, employee personal information, etc. Attackers might register with fake profiles in Google groups, Yahoo groups, etc. and try to join the target organization's employee groups, where they might share personal and company information. Attackers might also search for information in groups, forums, and blogs by Fully Qualified Domain Names (FQDNs), IP addresses, and usernames.

Employee information that an attacker can gather from groups, forums, and blogs might include:

- Full name of the employee
- Place of work and residence
- Home telephone, cell number, or office number
- Personal and organizational email address
- Pictures of the employee residence or work location that include identifiable information
- Pictures of employee awards and rewards or upcoming goals

Though Google is a search engine, the process of footprinting using Advanced Google Hacking Techniques differs from the process of footprinting through search engines. Footprinting using Advanced Google Hacking Techniques gathers information by Google hacking, a hacking technique to locate specific strings of text within search results using an advanced operator in the Google search engine.





Advanced Google Hacking refers to the art of creating complex search engine queries. Proper queries 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. Attackers can use the 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. When a query without advanced search operators is specified, Google traces for the search terms in any part of the webpage that includes the title, text, URL, etc. In order to confine a search, Google offers advanced search operators. Advanced search operators help to narrow down the search query and get the most relevant and accurate output.

The syntax to use an advanced search operator: operator: **search_term**

Note: Do not enter any spaces between the operator and the query.

Some of the popular Google advanced search operators include:

- **Site**: This operator restricts search results to the specified site or domain.

  For example, the [games site: www.juggyboy.com] query gives information on games from the juggyboy site.

- **allinurl**: This operator restricts results to only those pages containing all the query terms specified in the URL.

For example, the [allinurl: google career] query returns only those pages containing the words "google" and "career" in the URL.

- **Inurl**: This operator restricts the results to only those pages containing the word specified in the URL.

  For example, the [inurl: copy site:www.google.com] query returns only those pages in Google site in which the URL has the word "copy."

- **allintitle**: This operator restricts results to only those pages containing all the query terms specified in the title.

  For example, the [allintitle: detect malware] query returns only those pages containing the words "detect" and "malware" in the title.

- **intitle**: This operator restricts results to only those pages containing the specified term in the title.

  For example, the [malware detection intitle:help] query returns only those pages that have the term "help" in the title, and "malware" and "detection" terms anywhere within the page.

- **Inanchor**: This operator restricts results to only those pages containing the query terms specified in the anchor text on links to the page.

  For example, the [Anti-virus inanchor:Norton] query returns only those pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus."

- **Allinanchor**: This operator restricts results to only those pages containing all query terms specified in the anchor text on links to the page.

  For example, the [allinanchor: best cloud service provider] query returns only those pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider."

- **Cache**: This operator displays Google's cached version of a web page, instead of the current version of the web page.

  For example, [cache:www.eff.org] will show Google's cached version of the Electronic Frontier Foundation home page.

- **link**: This operator searches websites or pages that contain links to the specified website or page.

  For example, [link:www.googleguide.com] finds pages that point to Google Guide's home page.

  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.

- **related**: This operator displays websites that are similar or related to the URL specified.

  For example, [related:www.microsoft.com] provides the Google search engine results page with websites similar to microsoft.com.

- **info**: This operator finds information for the specified web page.

  For example, [info:gothotel.com] provides information about the national hotel directory GotHotel.com home page.

What can a Hacker do with Google Hacking?

The attacker creates complex search engine queries in order to filter large amounts of search results to obtain information related to computer security. The hacker uses Google operators that help to locate the specific strings of text within the search results. Doing so, an attacker is able to detect websites and web servers that are vulnerable to numerous exploits and vulnerabilities, as well as locate private, sensitive information about others, such as credit card numbers, social security numbers, passwords, etc. Once the vulnerable sites are identified, attackers try to launch various possible attacks such as buffer overflows, SQL Injection, etc., that compromise information security.

Sensitive information left on public servers that an attacker can extract with the help of Google Hacking Database (GHDB) queries include:

- Error messages that contain sensitive information
- Files containing passwords
- Sensitive directories
- Pages containing logon portals
- Pages containing network or vulnerability data, such as firewall logs
- Advisories and server vulnerabilities
- Software version information
- Web application source code.

Example: Use Google Advance Operator syntax `[intitle:intranet inurl:intranet +intext:"human resources"]` to find sensitive information about a target organization and its employees. Attackers use the gathered information to perform social engineering attacks.

The screenshot below shows a Google search engine results page displaying the results for the query mentioned before.

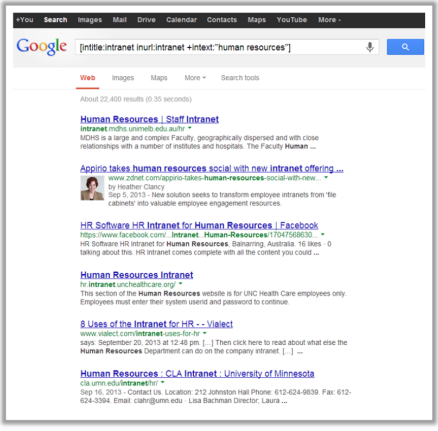


FIGURE 2.7: Search Engine showing results for given Google Advance Operator Syntax

Source: *http://www.googleguide.com*

Google Hacking Database (GHDB)

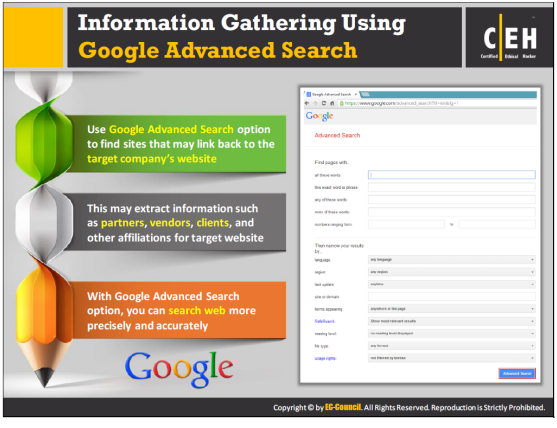
Source: *http://www.hackersforcharity.org*

The Google Hacking Database (GHDB) is a database of queries that an attacker uses to 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 the software that runs websites.

Google Dorks

Source: *http://www.exploit-db.com*

Google Dorks are the center of the Google Hacking. Many hackers use Google to find vulnerable webpages and later use these vulnerabilities for hacking. Google Dorks helps to refine the search results based on various parameters.



An attacker cannot always gather information easily from an information-rich site using only a normal search box. A complicated search involves a number of interrelated conditions.

Google's Advanced search feature helps an attacker to perform complex web searching. Using Google's Advanced search option one can find sites that may link back to the target organization's website. This helps to extract information such as partners, vendors, clients, and other affiliations of the target website.

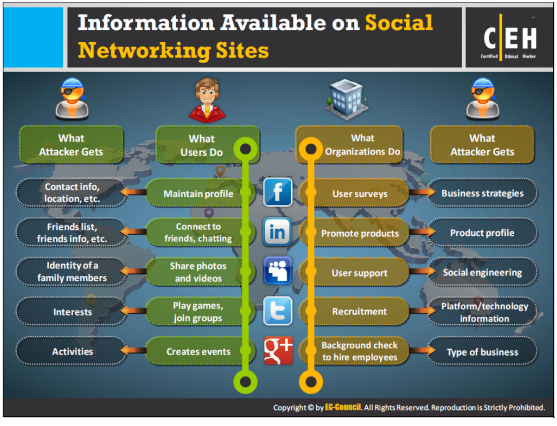
To perform an advanced search in Google, click Settings at the bottom-right of the Google home page and choose Advanced search in the menu. Advanced search allows the user to specify any number of criteria that the search must match, as this pattern builds on the search box pattern by adding more search options. To do this, you choose a field. enter the string you want to search for in the field's text box, and then click on the Advanced Search button. By default, various values are joined together with "and" (meaning all of them need to match) except for sets, blocks and formats, which are joined together with "or" (meaning any of them can match).

Though footprinting through social networking sites may seem 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 those sites. Attackers can even use social networking sites as a medium to perform social engineering attacks.

This section explains the type of information one can collect from social networking sites by means of social engineering, and how it can be done.

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

Therefore, for an attacker social networking sites can be great sources of information about the target person or organization. The attacker can only gather information that is posted by the person or the organization. Attackers can easily access the public pages of accounts created on the social networking sites. To obtain more information about the target, attackers may create a fake account and use social engineering techniques 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.



So far, we have discussed *how* an attacker can collect 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 help them connect with others. The profile generally contains information such as name, contact information (cell phone number, email address), friends' information, information about family members, their interests, activities, etc. People usually connect with friends and chat with them. Attackers can gather sensitive information through these chats. Social networking sites also allow people to share photos and videos. If the people do not set privacy settings for their albums, then attackers can see the pictures and videos shared by them. Users may join groups to play games or to share their views and interests. Attackers can collect information about victim's interests by tracking their groups and then can trick the victim to reveal more information. Users may create events to notify other users about upcoming occasions, from which attackers will come to know user activities. The activities of users on the social networking sites and the respective information that an attacker can collect is shown in the slide.

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 collect is shown in the slide.

Collecting Facebook Information

Facebook is one of the world's largest social networking sites. It allows people to create their personal profile, add friends, exchange instant messages, create or join various groups or communities, etc. To retrieve information from Facebook, the attacker should have an active account. The attacker should log in 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 addresss, friends' information, educational details, professional details, interests, photos, etc. The attacker can then use this information to plan an attack, which on implementation reveals even more information about the target.

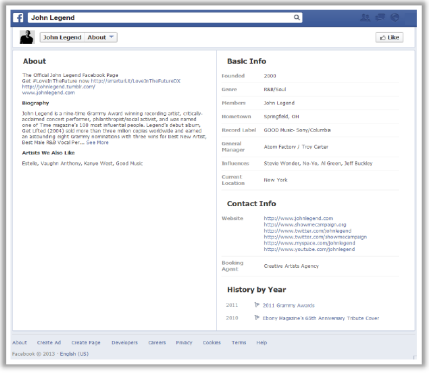


FIGURE 2.8: Screenshot of Facebook revealing information about a person

Collecting Twitter Information

Twitter is a popular social networking site used to send and read text-based messages. It allows users to follow friends, experts, favorite celebrities, etc. From the Twitter, an attacker may extract information of a target person such as personal information, friend information, activities of the target posted as tweets, whom the target is following, the followers of the target, photos uploaded, etc. The attacker may get meaningful information from the target user's tweets.

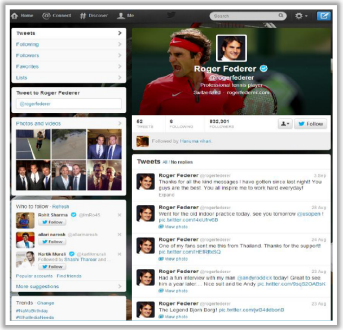


FIGURE 2.9: Screenshot of Twitter showing information about a user's tweets

Collecting LinkedIn Information

Similar to Facebook and Twitter, LinkedIn is another social networking site for professionals. It allows users to create and manage their professional profile. It also allows users to build and engage with their professional network. Hence, this can be a great information resource for the attacker from which details such as current employment, past employment, education, contact information, etc. about the target person can be obtained.

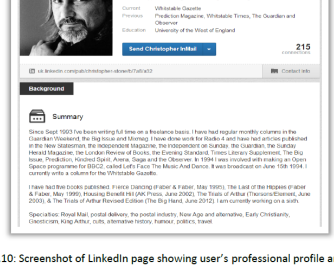


FIGURE 2.10: Screenshot of LinkedIn page showing user's professional profile and identity

So far, we have discussed footprinting through social networking sites. Now we will discuss website footprinting. An organization's website is the first place to get sensitive information such as names and contact details of the leaders of the organization, upcoming project details, etc. This section covers the website footprinting concept, mirroring websites, the tools used for mirroring, and monitoring web updates.

Website footprinting refers to monitoring and analyzing the target organization's website for information. It is possible for an attacker to build a detailed map of a website's structure and architecture without triggering the IDS or without raising any system administrator's suspicions. Attackers use sophisticated footprinting tools or the basic tools that come with the operating system, such as Telnet, or by using a browser.

The Netcraft tool 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. However, this tool may not give all these details for every site. In such cases, the attacker can browse the target website.

Browsing the target website will provide the following information:

- **Software used and its version:** An attacker can easily find the software and version in use on an off-the-shelf software-based website.
- **Operating system used:** Usually the operating system in use can also be determined.
- **Sub-directories and parameters:** Searches 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:** The attacker will carefully analyze anything after a query that looks like a filename, path, database field name, or query to check whether it offers opportunities for SQL injection.

- **Scripting platform:** With the help of script filename extensions such as .php, .asp, .jsp, etc., one 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. An attacker can use these details to perform a social engineering attack. CMS software allows URL rewriting in order to disguise the script filename extensions, if the attacker is willing to put in a little more effort to determine the scripting platform.

Use Burp Suite, Zaproxy, Paros Proxy, Website Informer, Firebug, etc. to view headers that provide information shown in the slide.

Burp Suite

Source: *http://portswigger.net*

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through finding and exploiting security vulnerabilities.

We can perform website footprinting by examining HTML source code and cookies.

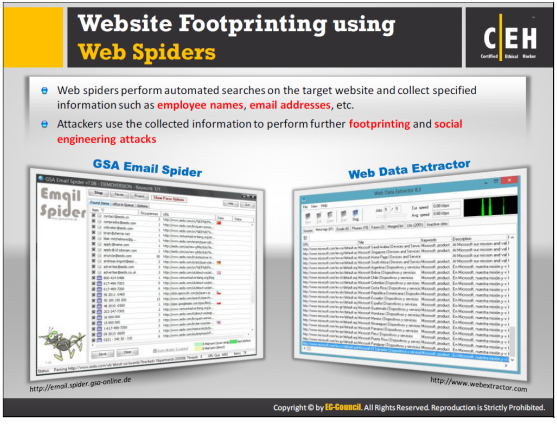
- **Examining the HTML source code**

  Attackers can gather sensitive information by examining the HTML source code, and following the comments that the CMS system creates or that are inserted manually. These comments may provide clues to what is running in the background. This may even provide contact details of the web developer or administrator.

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

- **Examining Cookies**

  Examine cookies set by the server to determine the software running and its behavior. Identify the scripting platforms by observing sessions and other supporting cookies.



Web spider (also known as web crawler or web robot) is a program or automated script that browses websites in a methodical manner to collect specified information such as employee names, email addresses, etc. Attackers thereafter use the collected information to perform footprinting and social engineering attacks. Web spidering fails if the target website has the robots.txt file in its root directory, with a listing of directories to protect from crawling.

Web spidering tools can collect sensitive information from the target website. These tools include:

GSA Email Spider

Source: *http://email.spider.gsa-online.de*

GSA Email Spider collects and extracts emails, phone and fax numbers from websites using the keywords entered as search string.

Web Data Extractor

Source: *http://www.webextractor.com*

Web Data Extractor automatically extracts specific information from web pages. It extracts targeted contact data (email, phone, and fax) from the website, extracts the URL and meta tag (title, description, keyword) for website promotion, searches directory creation, web research, etc. With Web Data Extractor, one can automatically get lists of meta-tags, e-mail addresses, phone and fax numbers, etc. and store them in different formats for future use.

Website mirroring is the process of creating an exact replica of the original website. Users can duplicate the websites by using mirroring tools such as HTTrack Web Site Copier, BlackWidow, SurfOffline, NCollector Studio, Teleport Pro, etc. These tools download a website to a local directory, building recursively all directories, HTML, images, flash, videos, and other files from the web server to another computer.

Website mirroring has the following benefits:

- It is helpful for offline site browsing
- It helps an attacker to spend more time viewing and analyzing the website for vulnerabilities and loop holes
- It assists in finding directory structure and other valuable information from the mirrored copy without multiple requests to the web server..

Website Mirroring Tools:

HTTrack Web Site Copier

Source: *http://www.httrack.com*

HTTrack is an offline browser utility. It downloads a website from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the web server to another computer. HTTrack arranges the original site's relative link-structure. HTTrack can also update an existing mirrored site, and resume interrupted downloads.

SurfOffline

Source: *http://www.surfoffline.com*

SurfOffline is website download software that downloads entire websites to the local hard drive. After downloading the target website, one can use SurfOffline as an offline browser and view downloaded web pages. IOne can use the Export Wizard to view downloaded pages in another browser.

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

In addition to the website mirroring tools, a few more well-known tools include:

BlackWidow

Source: *http://softbytelabs.com*

BlackWidow scans websites (it is a site ripper) for images, pictures, videos, music, etc. It can download an entire website, or download portions of a site. It can build a site structure first, and then download later.

NCollector Studio

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

NCollector Studio downloads content from the web to another computer. It crawls for specific file types, makes the website available for offline browsing, or allows downloading a website to the local computer that has the same structure and content as the original website.

Website Ripper Copier

Source: *http://www.tensons.com*

Website Ripper Copier (WRC) can download website files to the hard drive for offline browsing, extract website files of a certain size and type, like image, video, picture, movie, and music, retrieve a large number of files as a download manager with resumption support, and mirror sites. WRC is also a site link validator, explorer, and tabbed antipop-up Web / offline browser. It also resumes broken downloads from HTTP, HTTPS, and FTP connections, access password-protected sites, support Web cookies, analyze scripts, update retrieved sites or files, etc.

Teleport Pro

Source: *http://www.tenmax.com*

Teleport Pro can download all or part of a website to the computer, enabling the attacker to browse the site directly from the hard disk. It creates an exact duplicate, or mirror of a website, complete with subdirectory structure and required files, searches a website for files of a certain type and size, downloads a list of files at known addresses, explores websites linked from a central website, searches a website for keywords, and makes a list of pages and files on a website.

Portable Offline Browser

Source: *http://www.metaproducts.com*

Portable Offline Browser is an offline browser / web sites downloader. It copies entire web sites (or portions thereof) onto the hard drive, CD, DVD or other media. The downloaded Web site is a duplicate copy of the original Web site without modifications. It can be used to archive Web pages or entire Web sites, investigate the contents of those Web pages (data mine), or make the offline presentation of those Web sites, etc.

PageNest

Source: *http://www.pagenest.com*

PageNest copies favorite webpages or the entire site to the hard disk. It creates a cache of pages the user visits regularly. It browses the sites either within PageNest or from the favorite browser.

Backstreet Browser

Source: *http://www.spadixbd.com*

BackStreet is an Offline Browser that makes multiple simultaneous server requests to quickly download entire website or section of a site, and saves the files in the hard drive, either in their native format or as a compressed ZIP file, allowing user to view the website when view offline.

Features:

- Multi-threading website download
- Resume feature to pick up a session where left off
- Update feature to download new or modified files
- Built-in file viewer in onboard browser window to view files offline
- Built-in Zip/Unzip facility for downloaded websites
- Option of duplicating the original directory structure of a site
- Filters files by URL, size, type, date modified, text
- User-selectable recursion levels, retrieval threads, timeout and proxy support
- Accesses password-protected sites.

Offline Explorer Enterprise

Source: http://www.metaproducts.com

Offline Explorer Enterprise is an offline browser that downloads favorite Web, HTTPS, and FTP sites for later offline viewing, editing, or browsing. It also supports RTSP, PNM, and MMS streaming media downloads. It can create a static offline copy of SharePoint and ASP/ASPX sites.

Features:

- An OLE (Object Linking and Embedding) Automation interface to enable control from other applications
- Internal Proxy server to access downloaded sites transparently in your browser
- Generation of Google SiteMap files
- Multi-threaded processing of downloaded files by using all CPU cores
- Password-protected access to the Internal server from other computers.

GNU Wget

Source: http://www.gnu.org

GNU Wget is a non-interactive command line tool that retrieves files using HTTP, HTTPS, and FTP, the most widely used Internet protocols.

Features to make retrieve large files or mirror entire web or FTP sites:

- Can resume aborted downloads, using REST and RANGE
- Can use filename wild cards and recursively mirror directories
- NLS-based message files for many different languages
- Supports HTTP proxies
- Supports HTTP cookies
- Supports persistent HTTP connections
- Uses local file timestamps to determine whether documents need to be re-downloaded when mirroring.

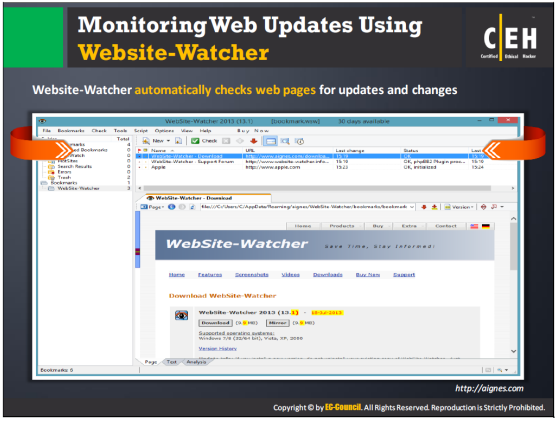
Hooeey Webprint

Source: http://www.hooeeywebprint.com

Hooeey webprint enables a user to save, retrieve, and analyze web pages. It builds a personal library of browsed web pages on the user's computer automatically. It captures both the text and screenshots in the user's web library. It also stores the user's web library on a number of different storage services such as Google Docs, Zoho, Amazon S3 and on Hooeey Webprint's own cloud.

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

Source: *http://www.archive.org*



Website Watcher helps to track 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 about updates
- Monitors web pages, password protected pages, forums for new postings and replies, RSS feeds, newsgroups and local files
- 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.

Source: *http://aignes.com*

Similar to the earlier discussed Website Watcher tool, following tools also monitor website changes.

Change Detection

Source: *http://www.changedetection.com*

ChangeDetection.com provides page change monitoring and notification services to internet users. When a change is detected in the page text, it sends an alert by email. It maintains a log of recent changes to the page and displays the difference between any two versions of the page.

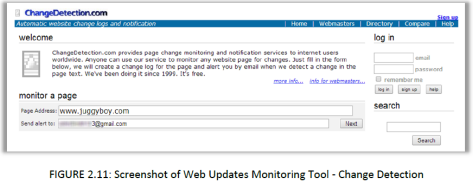


FIGURE 2.11: Screenshot of Web Updates Monitoring Tool - Change Detection

FollowThatPage

Source: *http://www.followthatpage.com*

Follow That Page monitors web pages and notifies via email when a page has changed or damaged.

FIGURE 2.12: Screenshot of Web Updates Monitoring Tool - Follow That Page

Page2RSS

Source: *http://www.page2rss.com*

Page2RSS is a service that helps to monitor web sites that do not publish feeds. It checks web pages for updates and delivers them to one's favorite RSS reader. It posts page updates to the Twitter account.

FIGURE 2.13: Screenshot of Web Updates Monitoring Tool - Page2RSS

Watch That Page

Source: *http://www.watchthatpage.com*

WatchThatPage is a service that collects new information from web pages on the Internet. It sends new information in an email and/or a personal web page. It also allows the user to specify when to check for the changes.

Check4Change

Source: *https://addons.mozilla.org*

Check4Change (aka C4C) is a simple extension that periodically checks a web page for updates.

Note: C4C currently only works with open tabs. It does not continue to monitor tabs that have closed, nor does it remember running jobs between FireFox restarts.

OnWebChange

Source: *http://onwebchange.com*

OnWebChange tracks and monitors changes to any public web page. If any change is detected in a web page, the user is notified by email, directly to the cell phone (using Pushover mobile notifications) and with a URL 'callback'. It monitors selected specific parts, or even multiple parts of a web page.

Infominder

Source: *http://www.infominder.com*

InfoMinder tracks changes made to web pages, blogs, RSS feeds and wikis. It tracks products, competitors (news, products, changes to the management team, new partnerships, etc.), grant proposals and request proposals on government sites, profiles on MySpace, certain types of news items, activity of certain standards bodies and communities, blogs, social book marking sites like del.icio.us, Flickr, etc.

TrackedContent

Source: *http://www.trackedcontent.com*

TrackedContent monitors and compares web pages. It tracks HTML changes, design and markup changes, content change in the website, etc. It sends custom email alerts when changes are detected.

Websnitcher

Source: *http://www.websnitcher.com*

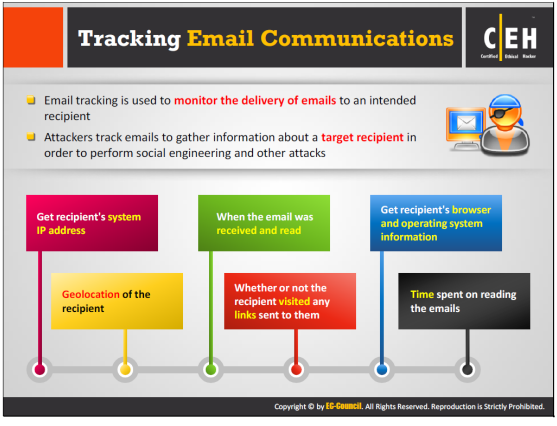
Websnitcher monitors sites periodically and shows a detailed list of changed text areas. It also generates RSS Newsfeeds from the collected data, to use in the favorite Newsfeedbrowser. Websnitcher collects per default, only relevant changes on the sites.

Update Scanner

Source: *https://addons.mozilla.org*

Update Scanner monitors web pages for updates. It monitors the websites that do not provide Atom or RSS feeds. It allows the user to schedule scanning time for each site and highlights the changes automatically.

So far we have discussed footprinting through search engines, footprinting using Google, footprinting through social networking sites, and website footprinting. Now we will discuss email footprinting. This section describes how to track email communications, how to collect information from email headers, and email tracking tools.

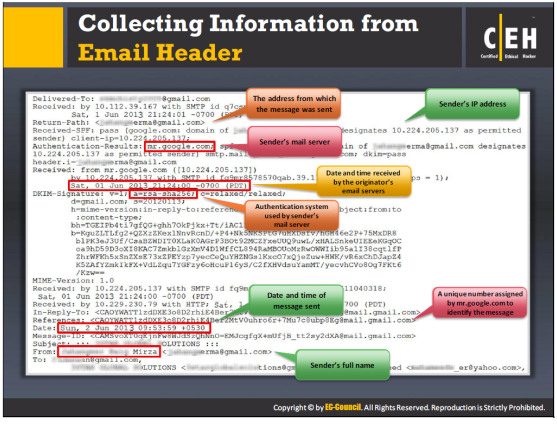


Email tracking monitors and tracks the emails of a particular user. This kind of tracking is possible through digitally time stamped records that reveal the time and date when the target receives and opens a specific email. Using email tracking tools allows an attacker to collect information such as IP addresses, mail servers, and service provider involved in sending the mail. Attackers can use this information to build a hacking strategy. Examples of email tracking tools include eMailTrackerPro, Paraben E-mail Examiner, etc.

Information gathered about the victim using email tracking tools:

- **Recipient's system IP address:** Allows to track the recipients IP address
- **Geolocation:** Estimates and displays the location of the recipient on the map and may even calculate the distance from the attacker's location
- **Email received and Read:** Notifies when the email is received and read by the recipient
- **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:** Checks whether or not the links sent to the recipient through email have been checked

- **Operating system and Browser information:** Reveals information about the operating system and the browser used by the recipient. The attacker can use this information to find loopholes in that version of operating system and browser, in order to launch further attacks
- **Forward Email:** Determines whether or not the email sent to the user is forwarded to another person



An email header contains the details of the sender, routing information, date, subject, recipient, etc. that are a great source of information for an attacker to launch attacks against the target. The process of viewing the email header varies with different email programs.

Commonly used email programs:

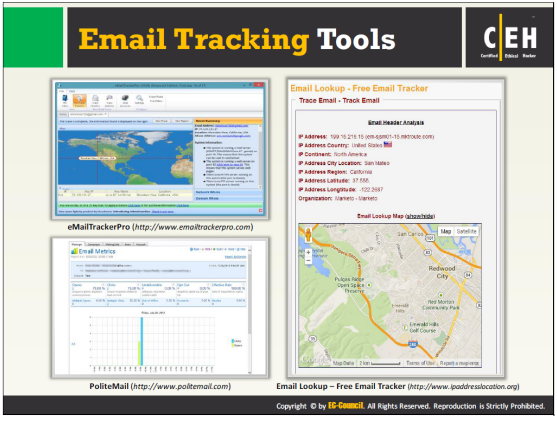
- SmarterMail Webmail
- Outlook Express
- Outlook
- Eudora
- Entourage
- Netscape Messenger
- MacMail

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 the 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 allow an attacker to track an email and extract information such as sender identity, mail server, sender's IP address, etc. Attackers use the extracted information to attack the target organization's systems by sending malicious emails.

The following are a few of the most widely used email tracking tools:

eMailTrackerPro

Source: *http://www.emailtrackerpro.com*

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

PoliteMail

Source: *http://www.politemail.com*

PoliteMail is an email tracking tool for Outlook. It tracks and provides complete details such as who opened an email message, which document was opened, as well as the links that were clicked. It offers mail merging, split testing, and full list management including segmenting. An attacker can compose an email containing malicious links, send it to the employees of the target organization, and keep track of that email message. If the employee clicks the link, she/he is infected and the tools notifies the attacker. Thus, an attacker can gain control over the target system with the help of this tool.

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. An attacker can copy and paste the email header into this email tracking tool and start tracing an email.

Some email tracking tools include:

Yesware

Source: *http://www.yesware.com*

Yesware is an add-on for Gmail that reveals who opened emails, when and where in the world, and on what device. It tracks email opens as well as links clicked in emails, and sends an alert each time someone opens an email or clicks a link.

ContactMonkey

Source: *https://contactmonkey.com*

ContactMonkey tracks emails. It automatically tracks an email and sends instant notifications when the recipients open the email, method of opening, if they have clicked any links and forwarded it.

Read Notify

Source: *http://www.readnotify.com*

Read Notify is an email tracking service. It notifies the user when the recipient opens, re-opens, or forwards the tracked emails and documents. Read Notify tracking reports contain information such as delivery details, date and time of opening, geographic location of the 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. This utility invisibly tracks every (sends) email that you send, without alerting the recipient. If the user opens the mail, then the tools display exact time of opening, duration it remained open and the location of opening.

Trace Email

Source: *http://whatismyipaddress.com*

The Trace Email tool attempts to locate the source IP address of an email based on the email headers. One needs to copy and paste the full headers of the target email into the Trace Email Analyzer box and then click the Get Source button. It shows the email header analysis and results.

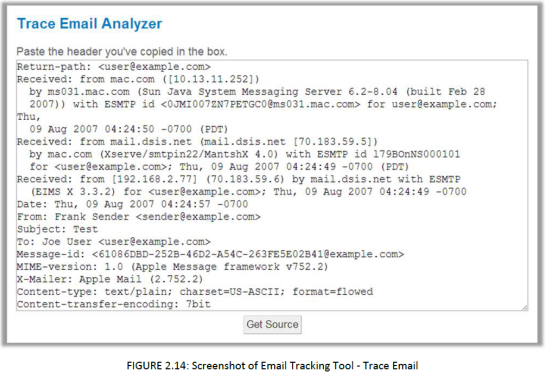


FIGURE 2.14: Screenshot of Email Tracking Tool - Trace Email

Zendio

Source: *http://www.zendio.com*

Zendio is email tracking software add-in for Outlook that notifies the user when the recipient reads an email, and if they clicked on any links in the message.

Pointofmail

Source: *http://www.pointofmail.com*

Pointofmail.com is a proof of receipt and reading service for email. It delivers read receipts, tracks attachments, and lets the sender modify or delete sent messages. It provides detailed

information about the recipient, history of the email reads and forwards, links and attachment tracking, email, and web and SMS text notifications.

WhoReadMe

Source: *http://whoreadme.com*

WhoReadMe is an online platform providing an email tracking service. It tracks the emails invisibly without alerting the recipients. The tool notifies the sender every time the recipient opens the message sent. It tracks information such as OS and browser used, Active X Controls, CSS version, duration between the message's 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 message. The tool tracks links in the email, duration it was open, date and time the user opened it, along with recipient's IP address, geographical location, browser, applications, OS name, etc.

G-Lock Analytics

Source: *http://glockanalytics.com*

G-Lock Analytics is an email tracking service. It provides the status of a message after the user sends it. It reports the number of times the email was printed and forwarded, geographical location of the recipient, email clients used by recipients to open the message, etc.

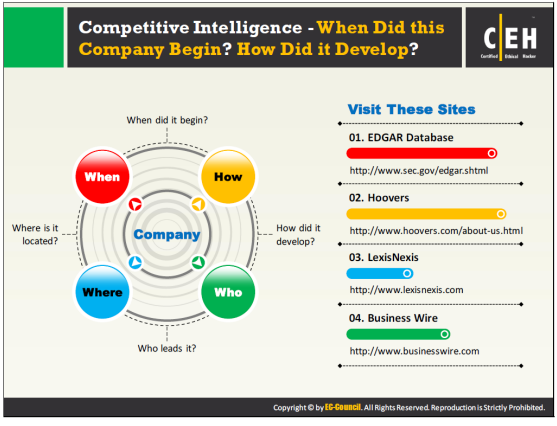
The next phase in footprinting methodology is competitive intelligence.

Competitive intelligence is a process that gathers, analyzes, and distributes information 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 of valuable information.

Competitive intelligence gathering is the process of identifying, gathering, analyzing, verifying, and using information about your competitors from resources such as the Internet. Competitive intelligence means understanding and learning what about other businesses, in order to become as competitive as possible. It is non-interfering and subtle in nature compared to the direct intellectual property theft carried out through hacking or industrial espionage. It concentrates on the external business environment. In this method, professionals gather information ethically and legally instead of gathering it secretly. Competitive intelligence helps in determining:

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

Companies carry out competitive intelligence either by employing people to search for the information, or by utilizing a commercial database service, which can be lower in cost.



Gathering competitor documents and records helps to improve productivity and profitability that in turn stimulates the growth of the company. It helps in determining answers to the following:

When did it begin?

Through competitive intelligence, companies can collect the history of a particular company, such as its establishment date. Sometimes, they gather crucial information that is not usually available to others.

How did it develop?

What are the various strategies the company uses? Development intelligence might include advertisement strategies, customer relationship management, etc.

Who leads it?

This information helps a company learn about the competitor's decision makers.

Where is it located?

Competitive intelligence also includes the location of the company and information related to various branches and their operations.

Attackers can use the information gathered through competitive intelligence to build a hacking strategy.

Information Resource Sites

Information resource sites that help to gain competitive intelligence include:

EDGAR Database

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

EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, performs automated collection, validation, indexing, acceptance, and forwarding of submissions by companies and others who are required by law to file with the U.S. Securities and Exchange Commission (SEC). Its primary purpose is to increase the efficiency and fairness of the securities market for the benefit of investors, corporations, and the economy by accelerating the receipt, acceptance, dissemination, and analysis of time-sensitive corporate information filed with the agency.

Hoover's

Source: http://www.hoovers.com/about-us.html

Hoover's is a business research company that provides complete details about companies and industries all over the world. Hoover's provides patented business-related information through the 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.

LexisNexis

Source: http://www.lexisnexis.com

LexisNexis provides 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 of legal and public-records related information. It enables customers to access documents and records of legal, news, and business sources.

Business Wire

Source: http://www.businesswire.com

Business Wire focuses on press release distribution and regulatory disclosure. This company distributes full text news releases, photos, and other multimedia content from various organizations 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 news.

MarketWatch

Source: http://www.marketwatch.com

MarketWatch tracks the pulse of markets for engaged investors. The site is an innovator in business news, personal finance information, real-time commentary, and investment tools and data, with journalists generating headlines, stories, videos, and market briefs.

The Wall Street Transcript

Source: http://www.twst.com

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

Lipper Marketplace

Source: http://www.lippermarketplace.com

Lipper Marketplace offers web-based solutions that are helpful for identifying the market of a company. Lipper 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 the organization's needs.

Experian

Source: *http://www.experian.com*

Experian helps to gain insights into competitors' search, affiliate, display, and social marketing strategies and metrics to improve marketing campaign results. It allows the user to:

- Benchmark the effectiveness of existing customer acquisition strategies
- Determine what is driving competitors' success
- Provides historical consumer data to forecast future trends and quickly respond to changing behaviors
- Measure website's performance against industry or specific sites.

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 many links added to SEC documents. It allows searches 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 competitive intelligence to monitor brand and trademark use, affiliate compliance, and competitive advertisers on paid search, organic search, local search, social media, mobile, and shopping engines worldwide. It helps interactive agencies, search marketers, and affiliate marketers to track ad rank, ad copy, keyword reach, click rates and CPCs, monthly ad spend, market share, trademark use, and affiliate activity.

Copernic Tracker

Source: *http://www.copernic.com*

Copernic Tracker is website tracking software. It looks for new content on Web pages and when it detects a change, it notifies the user by email, including a copy of the Web page with the changes highlighted, or by displaying a desktop alert. Copernic Tracker helps to track online forums and social media, auctions, news sites, product updates, new job notices, competitors' Web sites, etc.

SEMRush

Source: *http://www.semrush.com*

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

Jobitorial

Source: *http://www.jobitorial.com*

Jobitorial provides anonymous employee job reviews for many companies. It allows the user to browse various companies and look for reviews of jobs at that respective company.

AttentionMeter

Source: *http://www.attentionmeter.com*

AttentionMeter is a tool used for comparing any website (traffic) by using Alexa, Compete, CrunchBase, and Quantcast. It gives a snapshot of traffic data as well as graphs from Alexa, Compete, CrunchBase, and QuantCast for the specified websites.

ABI/INFORM Global

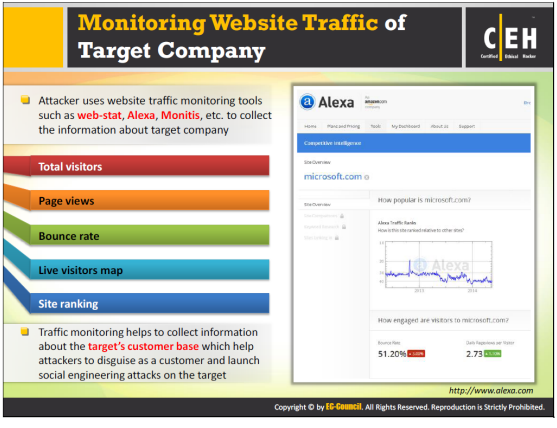
Source: *http://www.proquest.com*

ABI/INFORM Global is a business database. ABI/INFORM Global offers the latest business and financial information for researchers. 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 sites, search, and referral analytics in a single product.



Attackers can monitor a target company's website traffic using tools such as Web-Stat, Alexa, Monitis, etc., to collect valuable information. It helps to collect information about the target's customer base which help attackers to disguise as a customer and launch social engineering attacks on the target.

The information collected includes:

- **Total visitors**

  Tools such as Clicky find the total number of visitors browsing the target website.

- **Page views**

  Tools such as Opentracker monitor the total number of pages viewed by the users along with the time stamps and the status of the user on a particular web page (whether the webpage is still active or closed).

- **Bounce rate**

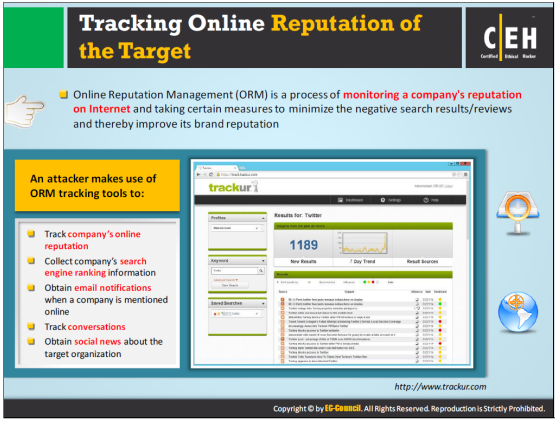
  Tools such as Google Analytics measure the bounce rate of the target company's website.

- **Live visitors map**

  Tools such as Web-Stat track the geographical location of the users visiting the company's website.

- **Site ranking**

  Tools such as Alexa track a company's rank on the web.



Online Reputation Management (ORM) is a process of monitoring what displays when someone searches your company's reputation on the Internet, and then taking measures to minimize negative search results or reviews. This process helps to improve brand reputation.

Companies often track the feedback given to them using ORM tracking tools, and then take measures to improve their credibility and keep their customer's trust. For positive online reputation management, organizations try to be more transparent over the Internet. This may help the attacker to collect genuine information about the target organization.

A list of online reputation tracking tools includes:

Rankur

Source: http://rankur.com

Rankur is a tool for monitoring, measuring, and management of one's reputation online. It helps to identify leads and opinion leaders, lets the user engage with online communities, and tracks success. It helps to protect name, business, and reputation online.

Social Mention

Source: http://www.socialmention.com

Social Mention is a social media search and analysis platform that aggregates user-generated content from across the web into a single stream of information. It allows the user to track and measure what people are saying about an individual, a company, a new product, or any topic across the web's social media landscape. It monitors social media properties including: Twitter, Facebook, FriendFeed, YouTube, Digg, Google etc., and provides a point-in-time social media search and analysis service, daily social media alerts, and a third-party API.

ReputationDefender

Source: https://www.reputation.com

ReputationDefender® offers solutions to suppress negative search results and replace them with accurate, positive content. It helps to define the user's online reputation and provides tools to monitor, manage, and secure information on the Internet.

Naymz

Source: http://www.naymz.com

Naymz helps to measure and manage social reputation. It calculates influence across LinkedIn, Facebook, & Twitter and compares the user's reputation against peers and other Naymz members.

BrandYourself

Source: https://brandyourself.com

BrandYourself offers Online reputation management tools and services that allow control over what people find when they Google a person's name.

Google Alerts

Source: http://www.google.com

Google alerts sends an alert each time a website mentions the user's brand, and can be used for real-time online reputation management.

WhosTalkin

Source: http://www.whostalkin.com

WhosTalkin.com is a social media search tool that allows users to search for conversations surrounding the topics that they care about most, such as a favorite sport, favorite food, celebrity, or company's brand name. Its goal is to deliver the most relevant and current conversations happening in the world of social media.

PR Software

Source: http://www.cision.com

PR software helps to find what people are saying about an individual, across millions of social media platforms and other websites, as well as traditional broadcast and print media.

BrandsEye

Source: http://www.brandseye.com

BrandsEye is an online monitoring and insights tool to track online conversations. It sends email notifications if any site mentions the user's brand online, and tracks conversations and compares metrics with internal data.

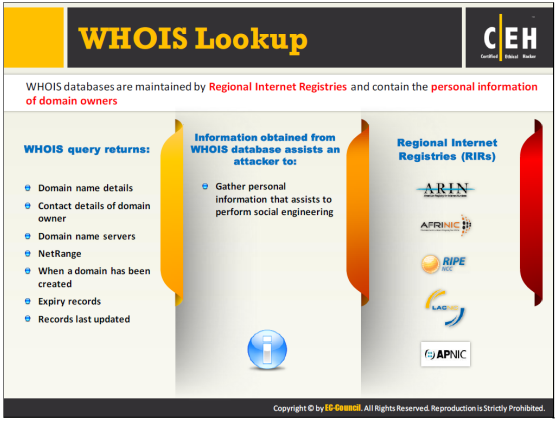
Talkwalker

Source: http://www.talkwalker.com

Talkwalker monitors the Web for interesting new content about a user's name, brand, competitors, events, or any favorite topic. It provides email updates of the latest relevant mentions on the Web to an email address or RSS feed reader.

Gathering network-related information such as whois information about the target organization is important when planning a hack. In this section we will discuss Whois footprinting.

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



WHOIS is a query and response protocol used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system. This protocol listens to requests on port 43 (TCP). Regional Internet Registries (RIRs) maintain WHOIS databases and it contains the personal information of domain owners. For each resource, WHOIS database provides text records with information about the resource itself, and relevant information of assignees, registrants, and administrative information (creation and expiration dates).

Two types of data models exist to store and look up WHOIS information:

- **Thick WHOIS** - stores the complete WHOIS information from all the registrars for the particular set of data
- **Thin WHOIS** - stores only the name of the WHOIS server of the registrar of a domain, which in turn holds complete details on the data being looked up

An attacker queries a WHOIS database server to obtain information about the target domain name, contact details of its owner, expiry date, creation date, etc., and the WHOIS sever responds to the query with the requested information. Using this information an attacker can create a map of the organization's network, trick domain owners with social engineering, and then obtain internal details of the network.

Regional Internet Registries (RIRs)

The RIRs include:

AFRINIC (African Network Information Center)

Source: https://www.afrinic.net

AFRINIC is the RIR for Africa, responsible for the distribution and management of Internet number resources such as IP addresses and ASN (Autonomous System Numbers) for the African region.

ARIN (American Registry for Internet Numbers)

Source: https://www.arin.net

ARIN provides services related to the technical coordination and management of Internet number resources. ARIN offers its services in form of three areas:

- Registration - pertains to the technical coordination and management of Internet number resources
- Organization - pertains to the interaction between ARIN members and stakeholders and ARIN
- Policy Development - facilitates the development of policy for the technical coordination and management of Internet number resources in the ARIN region

ARIN also develops technical services to support the evolving needs of the Internet community.

APNIC (Asia Pacific Network Information Center)

Source: https://www.apnic.net

APNIC is one of five RIRs charged with ensuring the fair distribution and responsible management of IP addresses and related resources that are required for the stable and reliable operation of the global Internet.

RIPE (Réseaux IP Européens Network Coordination Centre)

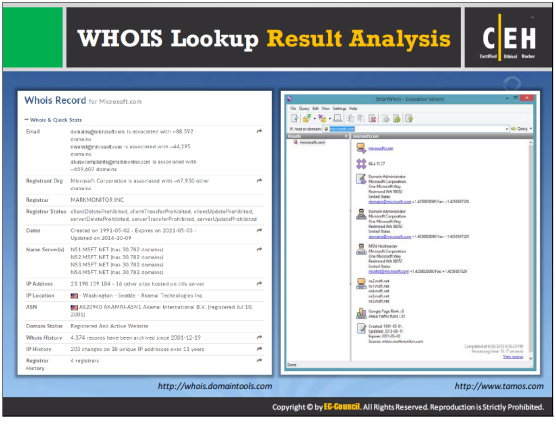
Source: http://www.ripe.net

RIPE NCC provides Internet resource allocations, registration services, and coordination activities that support the operation of the Internet globally.

LACNIC (Latin American and Caribbean Network Information Center)

Source: http://www.lacnic.net

LACNIC is an international non-government organization responsible for assigning and administrating Internet numbering resources (IPv4, IPv6), autonomous system numbers, reverse resolution, and other resources for the region of Latin America and the Caribbean.



Whois services such as whois.domaintools.com or tamos.com can help to perform a whois lookup. The figure shows the result analysis of a Whois lookup obtained with the two mentioned Whois services. Both these services perform 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 SmartWhois available at http://www.tamos.com gives 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 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. It supports Internationalized Domain Names (IDNs), which means one can query domain names that use non-English characters. It also supports IPv6 addresses.

There are numerous tools available to retrieve Whois information, including:

LanWhoIs

Source: *http://lantricks.com*

LanWhoIs provides information about domains and addresses on the Internet. This program helps to determine who, where, and when a domain or site was registered, and the information about those who support it now. This tool allows the user to save the search result in the form of an archive to view it later.

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.

Features:

- Lookup IP address for a single or list of domain names and vice versa
- Find out the country associated with a single or list of domains or IP addresses
- Perform batch and continuous pings on multiple servers
- Trace IP addresses to their destination and investigate connection problems

- Obtain all available information on a given IP address or domain name such as an organization or the ISP that owns the IP address, including the country, state, city, address, contact phone numbers and e-mails
- Determine name, date, last-modified, version and operation system of the remote web server
- Scan a given web site and produce a list of links (including htm, cgi, php, asp, jsp, jpg, gif, mp3, mpeg, exe, zip, rar, swf, etc.) found on the site
- Monitor all the TCP/IP connections from the computer to the internet automatically

CallerIP

Source: *http://www.callerippro.com*

CallerIP is IP and port monitoring software that displays the incoming and outgoing connections to the computer. It also finds the origin of all connecting IP addresses on the world map. The Whois reporting feature provides key information such as the name of the person registered with an IP along with contact email addresses and phone numbers.

WhoIs Lookup Multiple Addresses

Source: *http://www.sobolsoft.com*

WhoIs Lookup Multiple Addresses 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.

WhoIs Analyzer Pro

Source: *http://www.whoisanalyzer.com*

WhoIs Analyzer Pro grants access to contact records and other information from all registrars and routing registries worldwide without having to know which one to visit. It selects the most specific whois server automatically and performs multiple queries simultaneously. It gives whois information for any IP address, email address, URL, or ASN (Autonomous System Number) by giving access to contact records from every country worldwide.

HotWhois

Source: *http://www.tialsoft.com*

With HotWhois, one can retrieve all IP Whois and Domain whois information about IP addresses and domain names. This IP tracking tool 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 an IP address. HotWhois can make whois queries even if the registrar, supporting a particular domain, does not have the whois server itself.

Features:

- Ability to determine name and version of the remote web server
- Ability to ping remote hosts
- Multilingual Interface

ActiveWhois

Source: *http://www.johnru.com*

ActiveWhois is a network tool that provides information about the owners of an IP address or Internet domain. One can determine the country, personal and postal addresses of the owner, and/or user of domain and IP addresses. This technology allows ActiveWhois users to explore DNS aliases as well as simultaneously display both the domain and IP address information. After completing the search, the tool displays reports that include DNS records, domain owner, IP address, and HTTP headers.

WhoisThisDomain

Source: *http://www.nirsoft.net*

WhoisThisDomain is a domain registration lookup utility that provides information about a registered domain. It automatically connects to the right WHOIS server, according to the top-level domain name, and retrieves the WHOIS record of the domain. It supports both generic domains and country code domains.

SoftFuse Whois

Source: *http://www.softfuse.com*

SoftFuse Whois is a desktop domain lookup utility. It does a lookup search for a domain and presents the available information, such as administrative, technical, or billing contacts, domain location, hosting provider, creation, and expiration date. It also shows Google™ Page Rank and Alexa™ Traffic Rank for the specified domain. SoftFuse Whois supports all generic and country code top-level domains and constantly updates the list of supported gTLD/ccTLD domains.

Whois

Source: *http://technet.microsoft.com*

Whois performs the registration record for a domain name or IP address.

Usage: `whois domainname [whois.server]`

The domainname can be either a DNS name (e.g. www.sysinternals.com) or IP address (e.g. 66.193.254.46).

More Whois lookup tools include:

Domain Dossier

Source: *http://centralops.net*

This tool investigates domains and IP addresses. Provides registrant information, DNS records, and more.

BetterWhois

Source: *http://www.betterwhois.com*

BetterWhois offers WHOIS searches that allow users to check domain availability, display domain ownership, and verify nameserver information across several domain registrars.

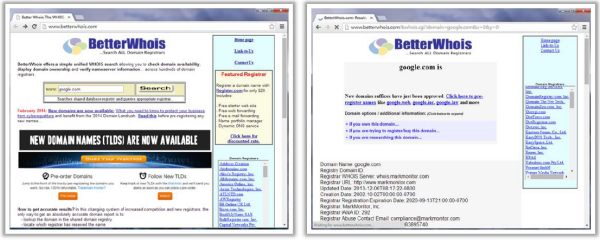


FIGURE 2.15: Screenshots of WHOIS Online Lookup Tool - BetterWhois

Whois Online

Source: *http://whois.online-domain-tools.com*

Whois Online provides information about Internet resources such as domain names, networks, IP addresses, domain registrants, or autonomous systems. Whois Online queries WHOIS databases to retrieve information.

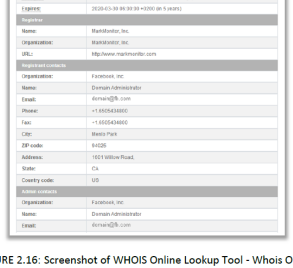


FIGURE 2.16: Screenshot of WHOIS Online Lookup Tool - Whois Online

Web Wiz

Source: *http://www.webwiz.co.uk/domain-tools/whois-lookup.htm*

The Web Wiz WHOIS Lookup tool can look up WHOIS information for Domains and IP Addresses.

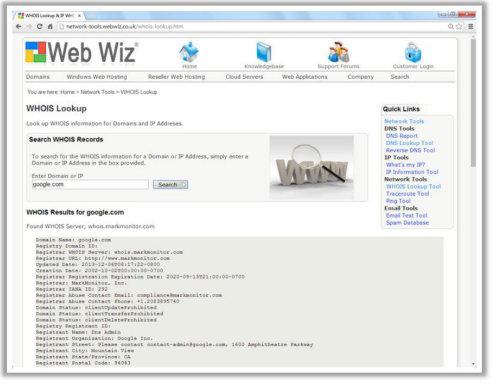


FIGURE 2.17: Screenshot of WHOIS Online Lookup Tool - Web Wiz

Network-Tools.com

Source: *http://network-tools.com*

Network-Tools.com offers Whois services including:

Whois - Input: domain name.

This program checks the domain name and searches for the registration records for that domain based on the top-level domain (.com, .uk. .au, etc.). To find information on a top level domain, enter the domain ending such as "com" "uk" "ro" "biz" etc. This tool cannot look up who owns an e-mail address, just who registered a domain name.

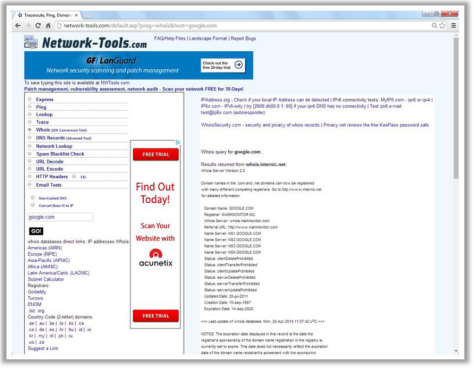


FIGURE 2.18: Screenshot of WHOIS Online Lookup Tool - Network-Tools.com

Whois

Source: *http://tools.whois.net*

The Whois.net site has been set up for domain name analysis, website analysis, and search engine optimization (SEO). Whois.net offers Domain-based research services. Whois Domain Search tool allows one to perform Whois Lookup – domain names search, registration and availability.

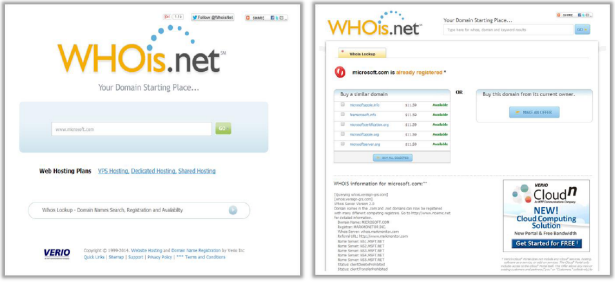


FIGURE 2.19: Screenshots of WHOIS Online Lookup Tool - Whois

DNSstuff

Source: *http://www.dnsstuff.com*

The DNSstuff toolbox tools can:

- Perform forensic analysis of name and email servers, path analysis, authenticate and locate domains
- Monitor blacklists and monitors web, email and name server compliance and connectivity
- Increase the efficiency, accuracy and quality of your searches, lookups and analysis
- Perform forensic analysis on a variety of domain and email concerns

DNSstuff toolbox tool - WHOIS/IPWHOIS Lookup

The WHOIS and IPWHOIS tools find contact information for the owner of specified domain/hostname. IPWHOIS is similar to WHOIS - finds contact information for the owner of the domain associated with the specific IP address. The results obtained using WHOIS/IPWHOIS Lookup tool help to track down spammers, to get contact Info for the owner of a domain, or report a problem with a domain

Network Solutions Whois

Source: *http://www.networksolutions.com*

Network Solutions Whois performs searches by domain name or IP address. It searches all the WHOIS records and returns results that reveal WHOIS behind the specified domain.

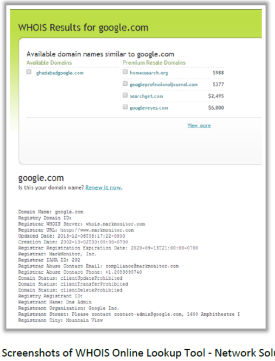


FIGURE 2.20: Screenshots of WHOIS Online Lookup Tool - Network Solutions Whois

WebToolHub

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

WebToolHub provides a WHOIS query protocol for querying databases to determine the registrant or the assignee of Internet resources, such as a domain name or an IP address. The WHOIS search can discover when and by whom a domain was registered, contact information, etc. A WHOIS search can also reveal the name or network mapped to a numerical IP address.

UltraTools

Source: *https://www.ultratools.com/whois/home*

Ultra Tools WHOIS+ shows information about the specified domain name, including the Whois registration data, a site profile, and IP information.

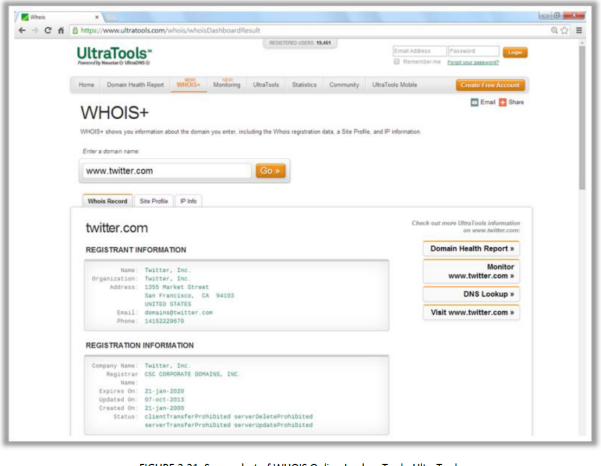
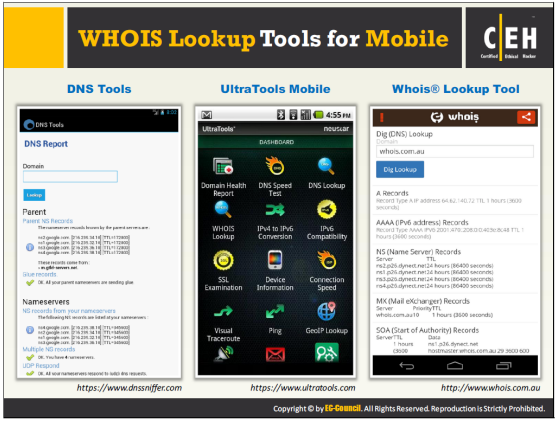


FIGURE 2.21: Screenshot of WHOIS Online Lookup Tool - UltraTools



Some of the WHOIS Lookup Tools for cell phones include:

DNS Tools

Source: *https://www.dnssniffer.com*

DNSSniffer's Mobile App has various network tools for mobile devices— Android, Windows , and Blackberry cell phones.

Features:

- **DNS Check** – Runs a full DNS Check for a domain
- **Blacklist Check** – Checks if a mail server is blacklisted
- **Email Check** – Checks if a mail server accepts a specified email address
- **WHOIS** – Displays the WHOIS of a domain
- **Ping** – Pings a hostname or IP
- **Reverse DNS Lookup** – Looks up the reverse DNS record of an IP

UltraTools Mobile

Source: *https://www.ultratools.com*

UltraTools Mobile for Android includes fourteen useful tools for DNS, website, and network administration, including:

- **Domain Health Report**

  Checks the health of a DNS configuration from a smartphone

- **Visual Traceroute**

  Checks the route from a mobile device to a server — both over the network and around the world

- **DNS Lookup**

  Queries any domain nameserver for information

- **WHOIS Lookup**

  Checks DNS domain registration and owner information

- **SSL Examination**

  Checks if the SSL certificate of a website present — or more importantly, if is it valid

- **DNS Speed Test**

  Checks the response time for DNS queries

- **Ping**

  Checks from anywhere if a mobile device has connectivity

- **GeoIP Lookup**

  Shows the location information about IP address and plots the results on Google Maps

- **RBL Lookup**

  Checks if email servers are present on real-time black lists (RBL) and allows them to be removed from the mobile device

- **Port Scanner**

  Checks for common services – and custom ports

- **Device Connection Speed**

  Checks and compares network download and upload speeds from a device over whatever network is in use

- **IPv4 to IPv6 converter**

  Converts addresses conveniently from IPv4 to IPv6

- **IPv6 Compatibility**

  Confirms a domain is ready for IPv6

- **Device Information**

  Stores critical information about mobile device hardware, OS, and connected networks in a single location

Whois® Lookup Tool

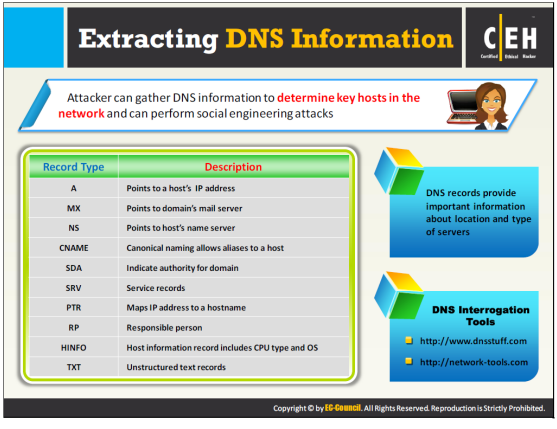
Source: http://www.whois.com.au

Whois.com.au provides an Android app that allows one to make WHOIS queries from the Android device. The Whois® lookup tool allows the user to perform fast WHOIS+Dig lookups and TraceRoutes without having to open a mobile browser.

Features:

- **Domain availability checks** – Checks the availability of domain names
- **WHOIS lookups** – Performs a WHOIS lookup on a domain name's publicly available registration details
- **DIG lookups** – Displays the DNS information critical for identifying who is hosting a particular domain name or website
- **TraceRoutes** – This network diagnostic tool discovers a network path and displays the transit relays

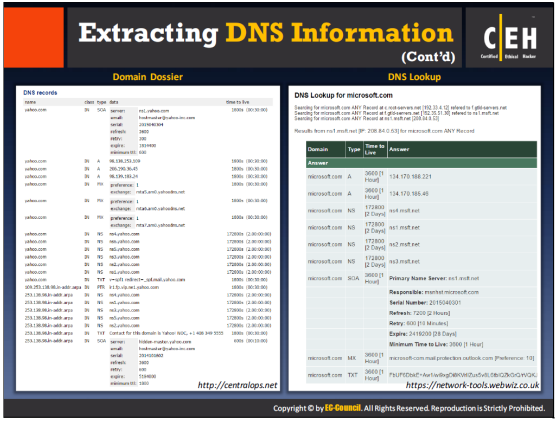
The next phase in footprinting methodology is DNS footprinting. This section describes how to extract DNS information and the DNS interrogation tools.



DNS footprinting reveals information about DNS zone data. DNS zone data include DNS domain names, computer names, IP addresses, and much more about a particular network. An attacker uses DNS information to determine key hosts in the network, and then performs social engineering attacks to gather even more information.

DNS interrogation tools such as DNSstuff.com enable user to perform DNS footprinting. DNSstuff extracts DNS information about IP addresses, mail server extensions, DNS lookups, Whois lookups, etc. It can extract a range of IP addresses utilizing an IP routing lookup. If the target network allows unknown, unauthorized users to transfer DNS zone data, then it is easy for an attacker to obtain the information about DNS with the help of the DNS interrogation tool.

When the attacker queries the DNS server using the DNS interrogation tool, the server responds with a record structure that contains information about the target DNS. DNS records provide important information about the location and type of servers.



Tools to extract DNS information include:

Domain Dossier

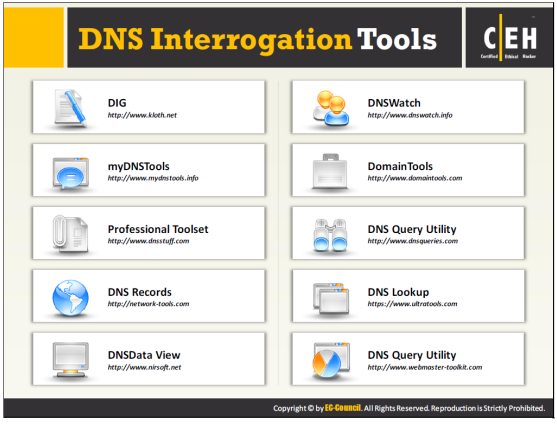
Source: *http://centralops.net*

Domain Dossier retrieves domains and IP addresses, domain whois record, DNS records, network whois record, etc.

DNS Lookup Tool

Source: *http://network-tools.webwiz.co.uk*

DNS Lookup Tool looks up DNS record and name server information on a hostname.



Some of the DNS interrogation tools used to extract DNS information include:

DIG

Source: *http://www.kloth.net*

DIG is an online web tool to query a DNS nameserver for IP address information of computers on the internet, and to convert host and domain names to IP addresses (and vice versa).

myDNSTools

Source: *http://www.mydnstools.info*

myDNStools is a collection of free IP address & DNS tools for DNS Lookup, Whois, troubleshooting, testing, checking, or for exploring.

The DNS Lookup tool shows the DNS records for a specified domain or hostname. The DNS records available are:

- A - IPv4
- AAAA - IPv6
- ANY - All cached records
- CNAME - Domain Alias
- MX - Mail Exchange

- NS - Name Servers
- PTR - Pointer Record
- SOA - Start of Authority
- SPF - Sender Policy Framework
- SRV - Service Record
- TXT - Text Records

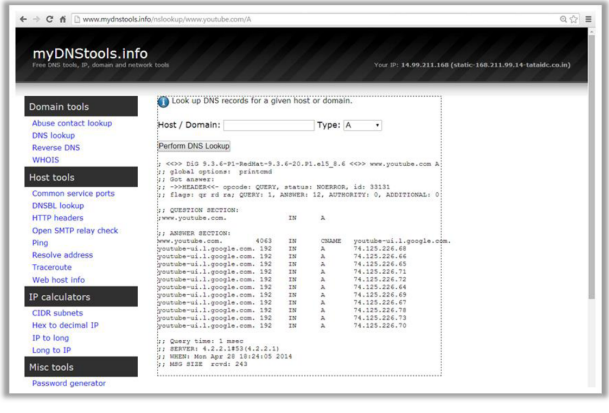


FIGURE 2.22: Screenshot of DNS Interrogation Tool - myDNStools

Professional Toolset

Source: *http://www.dnsstuff.com*

Professional Toolset assists IT professionals with troubleshooting, managing, and configuring the domain and email.

Professional Toolset includes Domain/WWW tools, IP tools, Networking tools, and Email tools that assist with:

- DNS troubleshooting, management and monitoring
- Network administration and troubleshooting
- Email troubleshooting and diagnostics
- Internet/Cybercrime forensics

- Spam combat
- Insight into an IP address
- Internet configuration, connectivity and performance

DNS Records

Source: *http://network-tools.com*

Active domains have a configuration file stored in their nameservers. This file gives information about IP addresses mapped to particular computer names. Example: www.consumer.net converts to 209.207.246.160. It also provides information about which mail server a domain uses (Mail eXchanger or MX record). Example: Network-Tools.com used the mail.consumer.net mail server.

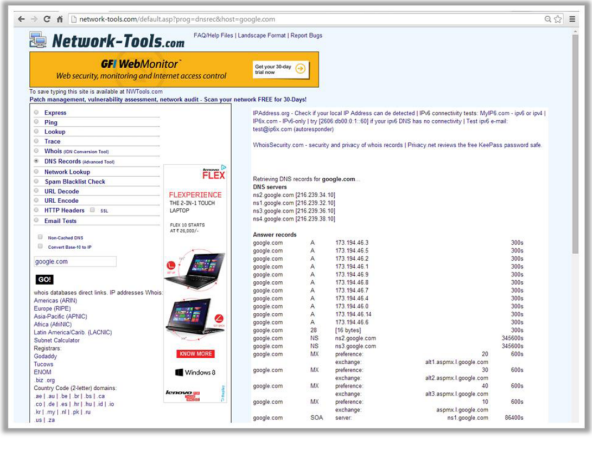


FIGURE 2.23: Screenshot of DNS Interrogation Tool - DNS Records

DNSData View

Source: *http://www.nirsoft.net*

DNSData View is a GUI alternative to the NSLookup tool that comes with the Windows OS. It allows the user to easily retrieve the DNS records (MX, NS, A, SOA) of the specified domains. One can use the default DNS server of their Internet connection, or use any other specified DNS

server. After retrieving the DNS records for the desired domains, the user can save them into text/xml/html/csv file.

DNSWatch

Source: *http://www.dnswatch.info*

DNSWatch is a DNS lookup and performance monitoring tool.

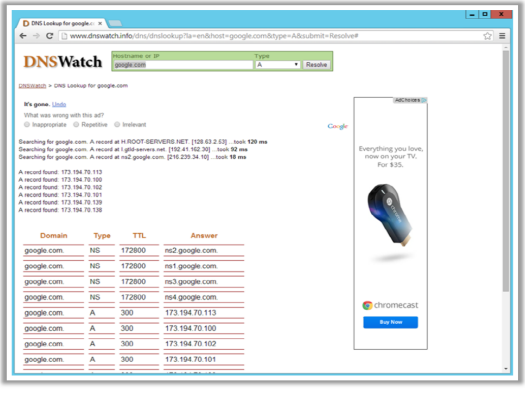


FIGURE 2.24: Screenshot of DNS Interrogation Tool - DNSWatch

DomainTools

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

DomainTools offers the searchable database of domain name registration and hosting data. Combined with their other data sites such as DailyChanges.com, Screenshots.com, and ReverseMX.com, users of DomainTools.com can review historical domain name records from basic Whois and DNS information, to homepage images and email settings.

DNS Query Utility

Source: *http://www.dnsqueries.com*

DNS query utility performs a DNS query on any host. There are several types of queries, corresponding to all the implementable types of DNS records such as a record, MX, AAAA, CNAME, and SOA.

DNS Lookup

Source: *https://www.ultratools.com*

The UltraTools DNS Lookup provides a report on DNS records for a specified domain or hostname and details about common resource record types for root server, TLD server and Nameserver information.

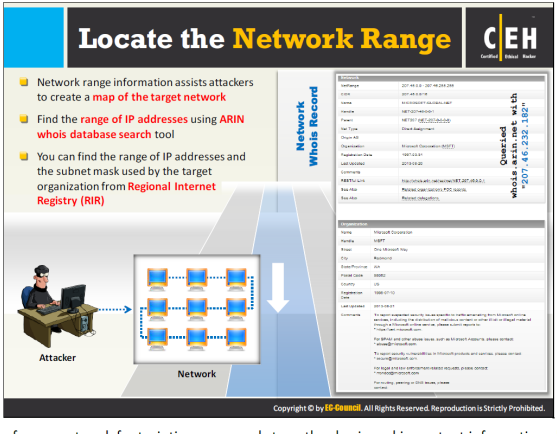
DNS Query Utility

Source: *http://www.webmaster-toolkit.com*

DNS Query Utility allows a user to look up DNS information on a domain.

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

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



To perform a network footprinting, one needs to gather basic and important information about the target organization such as what the organization does, who works there, and what type of work they perform. The answers to these questions provide information about the internal structure of the target network.

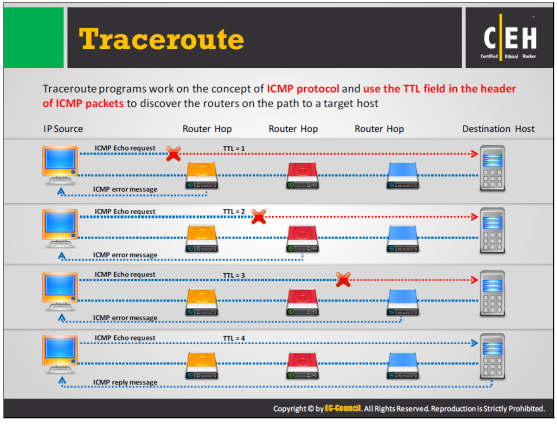
After gathering this information, an attacker can proceed to find the network range of a target system. Detailed information is available from the appropriate regional registry database regarding IP allocation and the nature of the allocation. An attacker can also determine the subnet mask of the domain, and trace the route between the system and the target system. Traceroute tools that are widely used include NeoTrace and Visual Route.

Obtaining private IP addresses can be useful to 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 the attacker information about how the network is structured, 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, one needs to enter the server IP address (that was gathered in WHOIS footprinting) in the ARIN whois database search tool. A user can also visit the ARIN website (https://www.arin.net/knowledge/rirs.html) and enter the server IP in the SEARCH Whois text box. This gives the network range of the target network. Improperly set up DNS servers offer

the attacker a good chance of obtaining a list of internal machines on the server. In addition, sometimes if an attacker traces a route to a machine, it is sometimes possible to obtain the internal IP address of the gateway, which might be useful.

Attackers typically use more than one tool in order to obtain network information, as a single tool cannot deliver all of the required information.



Finding the route of the target host on the network is necessary to test against man-in-the-middle attacks and other relative attacks. Most operating systems come with a Traceroute utility to perform this task. It traces 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 indicates the maximum number of routers a packet may transit. Each router that handles a packet decrements the TTL count field in the ICMP header by one. When the count reaches zero, the tool discards the packet and transmits an error message to the originator of the packet.

The utility 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.

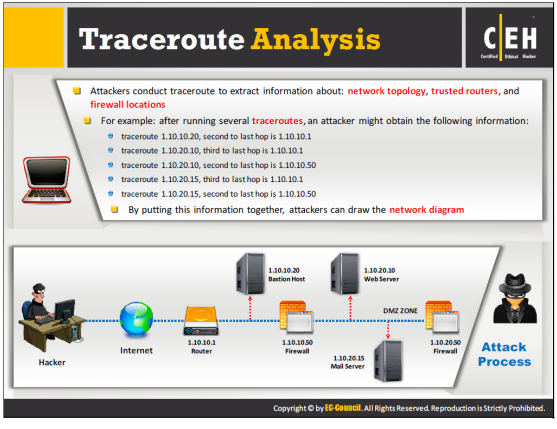
How to use the tracert command

Go to the command prompt and type the `tracert` command along with the 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:

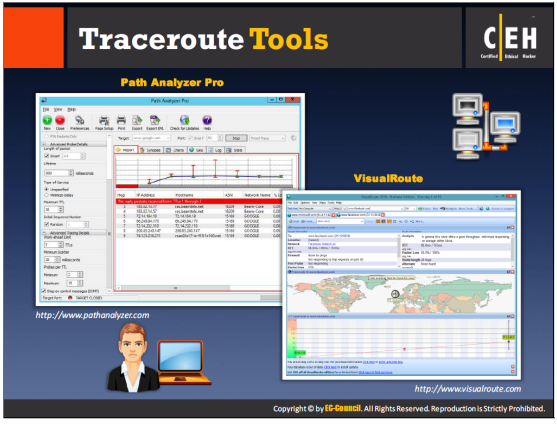
```
  1  1262 ms   186 ms   124 ms  195.229.252.10
  2  2796 ms  3061 ms  3436 ms  195.229.252.130
  3   155 ms   217 ms   155 ms  195.229.252.114
  4  2171 ms  1405 ms  1530 ms  194.170.2.57
  5  2685 ms  1280 ms   655 ms  dxb-emix-ra.ge6303.emix.ae [195.229.31.99]
  6   202 ms   530 ms   999 ms  dxb-emix-rb.so100.emix.ae [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.
```



We have seen how the Traceroute utility helps to find the IP addresses of intermediate devices such as routers, firewalls, etc. present between a source and its destination. After running several traceroutes, an attacker will be able to find the location of a hop in the target network. 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 topology diagram of the target network as shown in the slide.



Path Analyzer Pro and VisualRoute 2010 are two tools similar to Traceroute that trace the target host in a network.

Path Analyzer Pro

Source: *http://www.pathanalyzer.com*

Path Analyzer Pro delivers network route tracing with performance tests, DNS, whois, and network resolution to investigate network issues. It shows the route from source to destination graphically. It also provides information such as the hop number, its IP address, hostname, ASN, network name, percentage loss, latency, average latency, and standard deviation for each hop in the path.

Path Analyzer Pro can:

- Research IP addresses, e-mail addresses, and network paths
- Troubleshoot network availability and performance issues
- Determine what ISP, router, or server is responsible for a network problem
- Locate firewalls and other filters that may be impacting connections
- Visually analyze a network's path characteristics
- Graph protocol latency, jitter and other factors
- Trace actual applications and ports, not just IP hops

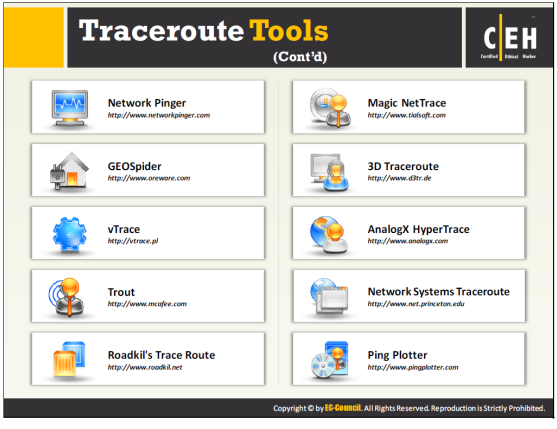
VisualRoute

Source: *http://www.visualroute.com*

VisualRoute is a traceroute and network diagnostic tool. It identifies the geographical location of routers, servers, and other IP devices. It provides 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



Other traceroute tools similar to Path Analyzer Pro and VisualRoute include:

Network Pinger

Source: *http://www.networkpinger.com*

Network Pinger is a freeware network monitoring utility for systems that use the .Net framework such as Windows.

Features include:

- Traceroutes
- Mass pings with automatic extraction of hosts
- Pings to single hosts
- Port scans
- WMI queries
- Whois to domain names and IPs
- Name resolution
- IP calculator
- Host extraction from memory
- Host list creation with network masks

GEOSpider

Source: http://www.oreware.com

GEO Spider helps to trace, identify, and monitor the network activity on a world map. It traces any website or IP address on Earth.

GEOSpider can:

- Check the domain name
- Detect fraudulent sites
- Detect network problems
- Lookup WhoIs information about the site and IP address
- If the website became unreachable or inaccessible one can be alerted shortly by:
  - Launched application
  - Played media file
  - Email

vTrace

Source: http://vtrace.pl

vTrace provides information about a target host that includes visual traceroute from your host, IANA information (WhoIs, ASN for BGP systems), DNS records (like nslookup or DIG), geographical placement, and open TCP ports (simple port scanner). It also provides some information about your machine such as Geographical map of all TCP connections that you make or somebody makes with you (NetStat) and IP statistics. The vTrace combines the tools traceroute, ping, whois, nslookup (dig), netstat into a graphical interface that analyzes Internet connections to locate where an outage or slowdown occurs. In addition, vTrace identifies the geographical location of IP addresses on a map.

Trout

Source: http://www.mcafee.com

Trout is a traceroute and Whois program. Pinging can be set at a controllable rate as can the frequency of repeatedly scanning the selected host. The built-in Whois lookup allows the system to identify hosts discovered along the route to the destination computer.

Roadkil's Trace Route

Source: http://www.roadkil.net

Roadkil's Trace Route tool displays network routing information between a computer and a given address. It shows information such as ping times between computers and name information. It tracks down network faults and finds the areas where data bottlenecks occur.

Magic NetTrace

Source: http://www.tialsoft.com

Magic NetTrace is an IP Tracer software with multithreading that defines the exact route of the signal from a PC to any host or IP on the Web. This IP tracing tool helps in resolving connectivity problems, and finding out where spam originates. The tool runs whois queries for all intermediate routing nodes, looking up their IP addresses and domain names. The program features an IP tracing multithreading architecture, integration with Internet Explorer, and multilingual support.

3D Traceroute

Source: http://www.d3tr.de

3D Traceroute is tracer software with multiple graphics modification options. The tool has a statistics window with minimum, maximum, average, standard deviation, and history, with the destination ping time.

Features:

- Long period Ping and HTTP monitor
- Whois query
- ASN inspector
- NSLookup with UDP and TCP; and zone transfer capability
- Command-line execution mode
- Passive OS fingerprinting
- Analyze email headers
- Connection viewer: TCP, IP, UDP etc. statistics
- Query HTTP-headers and webpages
- Build in the TELNET client

AnalogX HyperTrace

Source: http://www.analogx.com

AnalogX HyperTrace shows you the route that information travels from one machine to another on the internet. This tool gives information about the connection, as well as spots problem areas in the connection.

Network Systems Traceroute

Source: http://www.net.princeton.edu

Network Systems Traceroute can trace the current path from www.net.princeton.edu to another device on the Internet.

Ping Plotter

Source: *http://www.pingplotter.com*

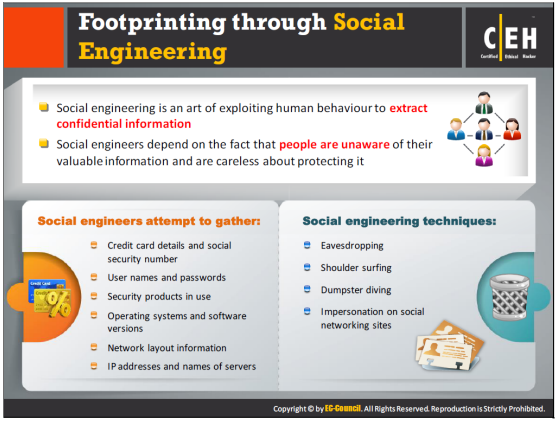
PingPlotter identifies where the problems are in an intuitive graphical display, and continues monitoring connections long-term to further identify issues.

PingPlotter offers some unique value for network monitoring and troubleshooting:

- Graphically display performance metrics about the route that data takes to a server
- Monitor network performance over time, capturing the moments when problems surface
- Zoom in on a problem period
- Notify the user when there is a network problem.

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 obtaining information from people by manipulating them.

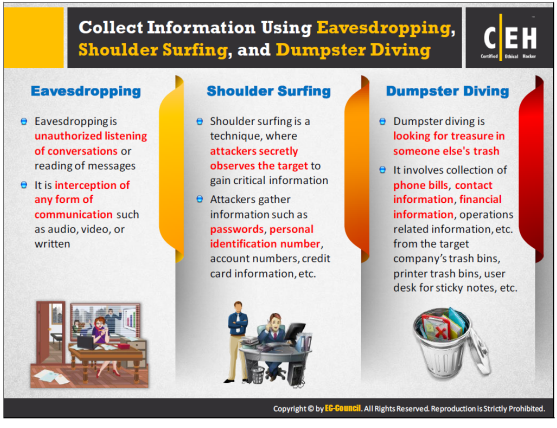
This section covers the social engineering concept and techniques used to gather information.



Social engineering is a totally non-technical process in which an attacker tricks a person and obtains confidential information in such a way that the target is unaware of the fact that someone is stealing confidential information. The attacker takes advantage of the helpful nature of people and their willingness to provide confidential information.

To perform social engineering, an attacker first needs to gain the confidence of an authorized user and then trick that user into revealing confidential information. The 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, commits frauds, etc. The information obtained through social engineering may include credit card details, social security numbers, usernames and passwords, other personal information, OS and software versions, IP addresses, names of servers, network layout information, etc.

Social engineering can be performed in many ways such as eavesdropping, shoulder surfing, dumpster diving, impersonation on social networking sites, tailgating, third-party authorization, piggybacking, reverse social engineering, etc.



Social engineering techniques—eavesdropping, shoulder surfing, and dumpster diving—are widely used to collect information from people.

- **Eavesdropping**

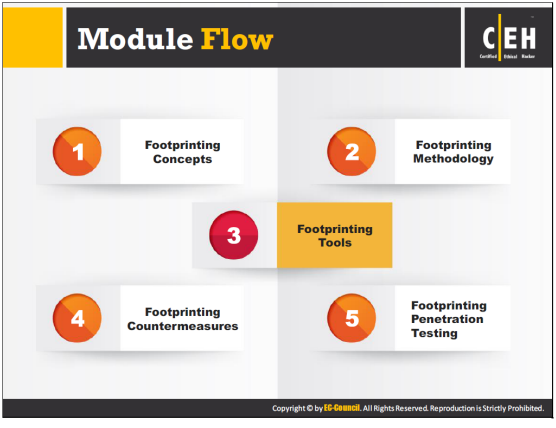
  Eavesdropping is the act of secretly listening to the conversations of people over a phone or video conference without their consent. It also includes reading confidential messages from communication media such as instant messaging or fax transmissions. Thus, it is the act of intercepting communication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

- **Shoulder Surfing**

  In the shoulder surfing technique, an attacker stands behind the victim and secretly observes the victim's activities on the computer, such as keystrokes while entering usernames, passwords, etc. This technique helps to gain passwords, PINs, security codes, account numbers, credit card information, and similar data. The attackers can easily perform shoulder surfing in a crowded place, as it is relatively easy to stand behind and watch the victim without his or her knowledge.

Dumpster Diving

This technique is also known as trashing, where the attacker looks for information in the trash bin. 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, sticky notes at users' desks, etc. The attacker may also gather account information from ATM trash bins. The information can help the attacker to commit attacks.

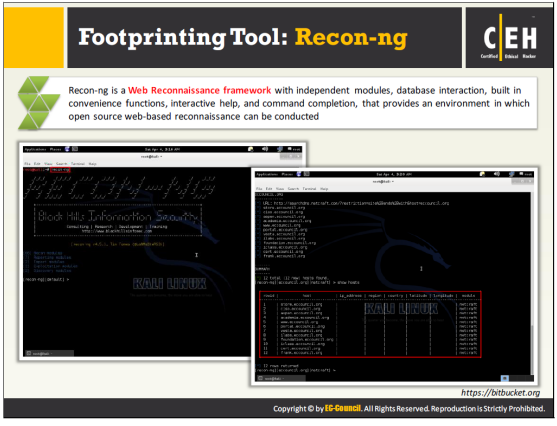


Attackers can perform footprinting with the help of various tools. Many organizations offer tools that make information gathering an easy task. This section describes tools intended for obtaining information from various sources.

Maltego is an open-source intelligence and forensics application. It is useful during 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. Maltego demonstrates the complexity and severity of single points of failure as well as trust relationships that exist within the scope of the infrastructure. The unique perspective that Maltego offers to both network and resource-based entities is the aggregation of information posted all over the internet.

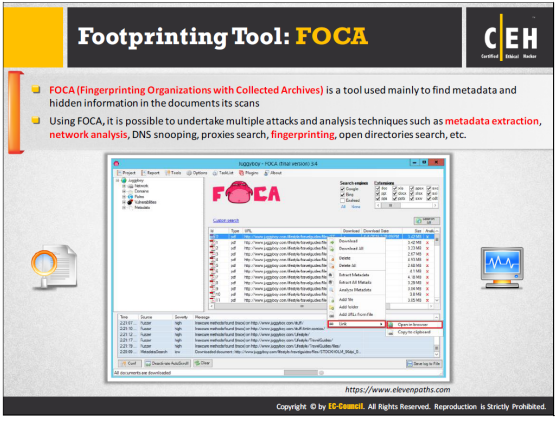
It can be used to determine the relationships and real-world links between people, social networks, companies, organizations, websites, Internet infrastructure (domains, DNS names, Netblocks, IP addresses), phrases, affiliations, documents, and files.

Source: *http://paterva.com*



Recon-ng has a look and feel similar to the Metasploit Framework, reducing the learning curve for leveraging the framework. However, it is quite different. Recon-ng is not intended to compete with existing frameworks, as it is designed exclusively for web-based open source reconnaissance.

Source: *https://bitbucket.org*



FOCA is capable of scanning and analyzing a wide variety of documents, with the most common being Microsoft Office, Open Office, or PDF files.

Features:

- **Web Search** - Searches for hosts and domain names through URLs associated to the main domain. Each link is analyzed to extract from it new host and domain names.
- **DNS Search** - Checks each domain to ascertain which are the host names configured in NS, MX, and SPF servers to discover a new host and domain names.
- **IP resolution** - Each host name is resolved by comparison to the DNS to obtain the IP address associated with this server name. To perform this task accurately, the tool performs analysis against the organization's internal DNS.
- **PTR Scanning** - To find more servers in the same segment of a determined address, IP FOCA executes a PTR logs scan.
- **Bing IP** - For each IP address discovered, FOCA launches a search process for new domain names associated with that IP address.
- **Common Names** - Common names module performs dictionary attacks against the DNS.

Source: *https://www.elevenpaths.com*

Additional footprinting tools that assist in gathering information about the target person or organization include:

Prefix WhoIs

Source: *http://pwhois.org*

The Prefix WhoIs Project provides a whois-compatible client and server framework for disclosing various up-to-date routing information. Instead of using registrar-originated network information (which is often unspecific or inaccurate), Prefix WhoIs uses the Internet's global routing table as gleaned from a number of routing peers around the world. It operates a global network of servers running a derivative of Prefix WhoIs Server software.

NetScanTools Pro

Source: *http://www.netscantools.com*

NetScanTools Pro is an integrated windows operating system tool for internet information gathering and network troubleshooting utilities for network professionals. Research IPv4 addresses, IPv6 addresses, hostnames, domain names, email addresses and URLs automatically or with manual tools.

Benefits:

- Saves time in gathering information about Internet or local LAN network devices, IP addresses, domains, device ports, and many other network specifics.

- Simplifies and speeds up the information gathering process by automating the use of many network tools.

TCtrace

Source: *http://www.phenoelit.org*

TCtrace uses TCP SYN packets to trace and makes it possible for users to trace through firewalls if they know a TCP service that can pass from the outside.

Autonomous System Scanner (ASS)

Source: *http://www.phenoelit.org*

ASS, the autonomous system scanner, finds the AS of the router. It supports the following protocols: IRDP, IGRP, EIGRP, RIPv1, RIPv2, CDP, HSRP, and OSPF.

In passive mode (./ass -i eth0), it just listens to routing protocol packets (like broadcast and multicast hellos).

In active mode (./ass -i eth0 -A), it tries to discover routers by asking for information. The tool discovers the router based on the appropriate address provided for each protocol (either broadcast or multicast addresses). If you specify a destination address, the tool will use this, but may be not as effective as the defaults.

DNS-Digger

Source: *http://www.dnsdigger.com*

DNS-Digger is a massive reverse lookup service that can locate "hidden" data in the vast flood of information behind the Internet. DNS-Digger tries digging deeper into the hostname/domain data.

FIGURE 2.25: Screenshot of Footprinting Tool - DNSdigger

Netmask

Source: *http://www.phenoelit.org*

Netmask searches for the netmask by Internet Control Message Protocol (ICMP).

Binging

Source: *http://www.blueinfy.com*

Binging is a tool to query Bing search engine. It uses the Bing API key to fetch multiple results. This tool can be used for cross-domain footprinting for Web 2.0 applications, site discovery, reverse lookup, host enumeration etc. One can use various directives like site, IP address, etc. and run queries against the engine. It also provides filtering capabilities that ask for unique URLs or hosts. It is also possible to filter results by applying the power of regular expression.

SearchBug

Source: *http://www.searchbug.com*

SearchBug is a professional online service for finding and investigating people, businesses, addresses, phone numbers, conducting social security number verification in lieu of e-verify, etc.

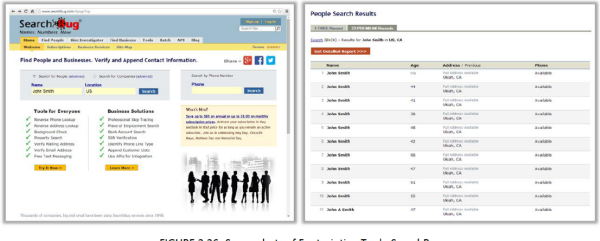


FIGURE 2.26: Screenshots of Footprinting Tool - SearchBug

TinEye

Source: *http://www.tineye.com*

TinEye is a reverse image search engine. It reveals the source of an image c, its usage, modified versions of the image if they exist, or if there is a higher resolution version. TinEye regularly crawls the web for new images. It uses image identification technology rather than keywords, metadata, or watermarks.

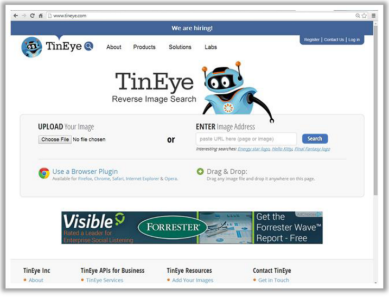


FIGURE 2.27: Screenshot of Footprinting Tool - TinEye

Robtex

Source: *http://www.robtex.com*

Robtex is a software tool that provides detailed information about an Internet host. It also provides detailed DNS information, including reverse DNS and forwards, whois information, who hosts the machine, etc.

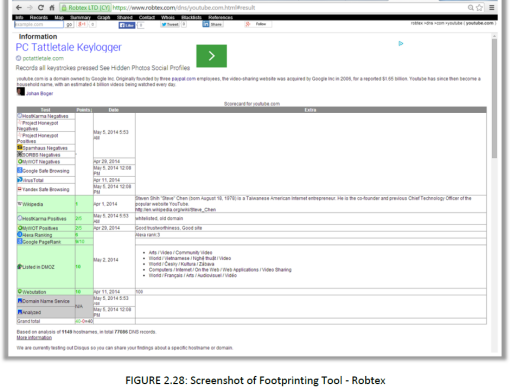


FIGURE 2.28: Screenshot of Footprinting Tool - Robtex

Dig Web Interface

Source: *http://www.digwebinterface.com*

This is an online web interface that performs a dns/nameserver query. This tool does not support automated lookups.

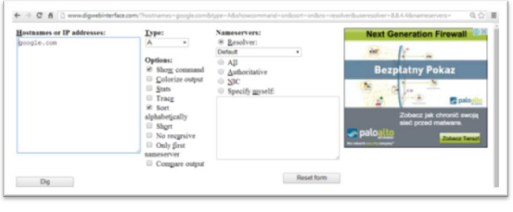


FIGURE 2.29: Screenshot of Footprinting Tool - Dig Web Interface

White Pages

Source: http://whitepages.com

The WhitePages objective is to help people find, be found, and connect. It performs people search, business search, reverse phone, reverse address, etc.

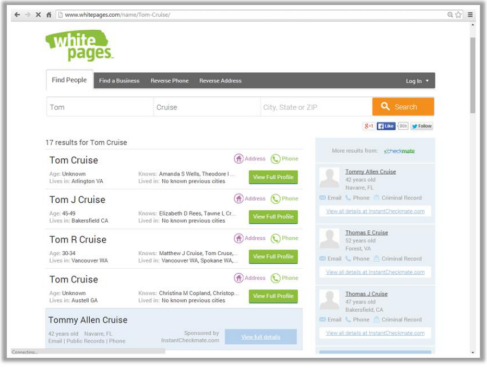


FIGURE 2.30: Screenshot of Footprinting Tool - White Pages

Email Tracking Tool

Source: http://www.filley.com

This tool searches for the source IP address of an email based on the email headers.

FIGURE 2.31: Screenshot of Footprinting Tool - Email Tracking Tool

yoName

Source: *http://yoname.com*

yoName is a tool that acts like a meta search engine to explore individuals who are members of networks of MySpace, LinkedIn, Twitter, YouTube, etc. It searches for people across social networks, blogs, etc.

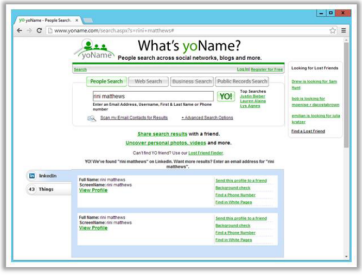


FIGURE 2.32: Screenshot of Footprinting Tool - yoName

Ping-Probe

Source: *http://www.ping-probe.com*

Ping-Probe offers a comprehensive suite of networking tools. It offers traceroute method that reveals routes behind blocking firewalls without being harmful.

Ping-Probe networking tools include:

- **Ping** - When one device pings another, the respondent sends a small fragment of data back to the requesting device. The device in turn sends the data back. This is an indication that the device is functioning and the connectivity from the computer making the request to that of the device answering the request is functioning.
- **Traceroute** - The traceroute tool searches for the route a request takes through the internet to get to its destination
- **TCP port scanner** - The TCP Port Scan tool scans TCP ports to see if they are in use
- **Network scanner** - This tool sends out ping requests to all IPs in a block range
- **SNMP browser** - This tool browses for the output of an 'SNMP Walk'
- **Bandwidth monitor** - This tool monitors the network through-traffic of any of the computer network interfaces
- **DNS client** – This tool offers the functionality of command line programs like nslookup or dig. The main function of DNS is to offer a system where the IP Address (10.5.99.1) can be resolved to the Fully Qualified Domain Name.
- **Finger client** - The finger protocol offers information regarding who is currently logged onto the computer
- **Whois client** - The Whois protocol obtains information about the owner of a domain
- **LDAP client** - This is a client for the LDAP (Lightweight Directory Access Protocol) that stores and delivers lists of data.

SpiderFoot

Source: *http://www.spiderfoot.net*

SpiderFoot is an open-source footprinting tool. The main objective of SpiderFoot is to automate the footprinting process to the greatest extent possible, freeing up a penetration tester's time to focus efforts on the security testing itself. Its web-based interface scans the network immediately after installation by giving the scan a name, the domain name of the target, and selecting the modules that it has to enable. After completion of the scan the information obtained includes URLs handling passwords, network ranges (netblocks), web servers, open ports, information about SSL certificates, etc.

NSlookup

Source: *http://www.kloth.net*

NSlookup helps to query a DNS domain nameserver to look up and find IP address information of computers in the internet. It converts a host or domain name into an IP address.

FIGURE 2.33: Screenshot of Footprinting Tool - NSlookup

ZabaSearch

Source: *http://www.zabasearch.com*

ZabaSearch accesses public information and displays what is available in the public domain. It searches for people, reverse phone lookup, area code, zip code, IP address, message, social security number, etc.

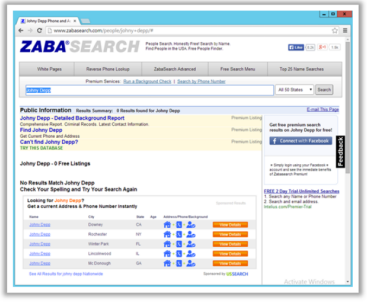


FIGURE 2.34: Screenshot of Footprinting Tool - ZabaSearch

GeoTrace

Source: *http://www.nabber.org*

GeoTrace tool tracks a domain name or IP address to a geographical location.

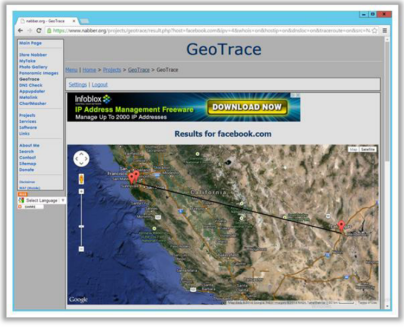


FIGURE 2.35: Screenshot of Footprinting Tool - GeoTrace

DomainHostingView

Source: *http://www.nirsoft.net*

DomainHostingView is a utility for windows that collects information about a domain by using a series of DNS and WHOIS queries, and generates a report. The information returned includes: the hosting company or data center that hosts the web server, mail server, and domain name server (DNS) of the specified domain, the created/changed/expire date of the domain, domain owner, domain registrar that registered the domain, list of all DNS records, etc.

Features:

- It is a Unicode application and thus it can display properly WHOIS records containing non-English characters
- Supports Internationalized Domain Names (IDN)

There are other tools that can perform Google hacking. These tools 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 extracts metadata of public documents (pdf, doc, xls, ppt, docx, pptx, xlsx, etc.) belonging to a target company.

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

Wikto

Source: *http://research.sensepost.com*

Wikto helps in finding directories and files on a website. It also searches for sample scripts that can be exploited in a network attack, or finds known vulnerabilities in the web server implementation itself. Wikto is Nikto for Windows with extra features including fuzzy logic error code checking, a back-end miner, Google-assisted directory mining, and real time HTTP request/response monitoring.

SiteDigger

Source: http://www.mcafee.com

SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and other security-related information on web sites.

Google Hacks

Source: http://code.google.com

Google Hacks is a compact utility that combines several carefully built Google searches. These searches expose novel functionality from Google's search and map services. For example, it can display a timeline of search results, display a map, search for music, search for books, and perform many other specific kinds of searches. One can also use this program to use Google as a proxy.

BiLE Suite

Source: http://www.sensepost.com

BiLE stands for Bi-directional Link Extractor. The BiLE suite includes Perl scripts used in enumeration processes. 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.

GMapCatcher

Source: http://code.google.com

GMapCatcher is an offline maps viewer. It can display maps from providers such as CloudMade, OpenStreetMap, Yahoo Maps, Bing Maps, Nokia Maps, SkyVector, etc. It displays them using a custom GUI.

SearchDiggity

Source: http://www.bishopfox.com

SearchDiggity is the primary attack tool of the Google Hacking Diggity Project. It serves as a front end to the recent versions of the Diggity tools: GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity. These attack tools use Google, Bing, and other resources to reveal network and system vulnerabilities.

Google HACK DB

Source: http://www.secpoint.com

Google HACK DB tool finds sensitive information about the target website indexed in Google. The site might contain sensitive information or disclose sensitive files that include password files, database files, clear text files, customer database profiles, database files, company secrets, etc.

Gooscan

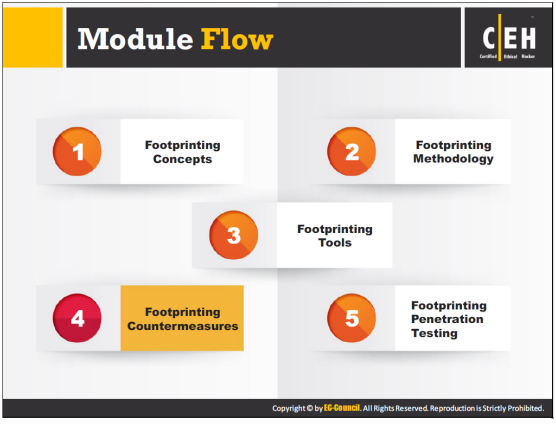
Source: *http://www.darknet.org.uk*

Gooscan is a Google hacking tool that automates queries against Google search appliances. The design of these particular queries helps to find potential vulnerabilities on web pages.

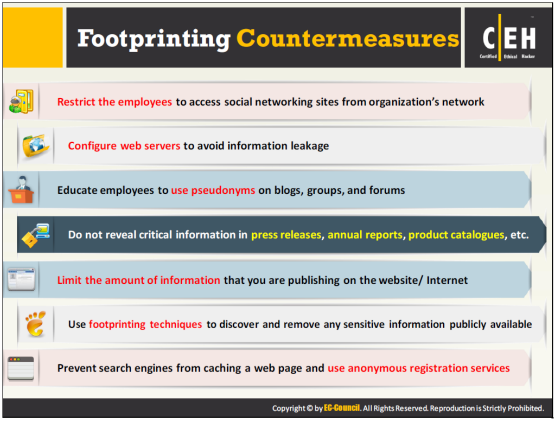
Trellian

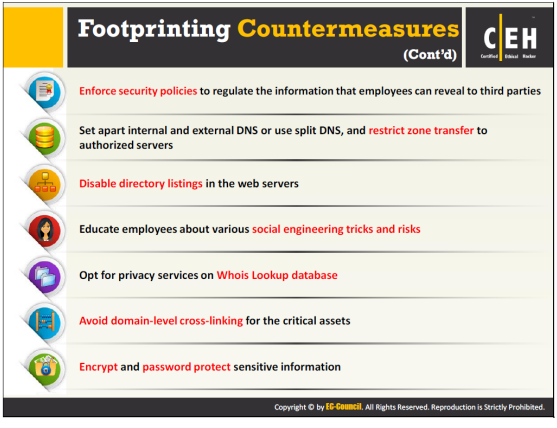
Source: *http://ci.trellian.com*

Trellian compiles and analyzes internet usage statistics to create a competitive Intelligence tool. Competitive Intelligence provides the means to monitor a competitor's web sites to identify their major traffic sources. Trellian searches for sites that are responsible for sending traffic to their pages, including search engines and the search keywords.



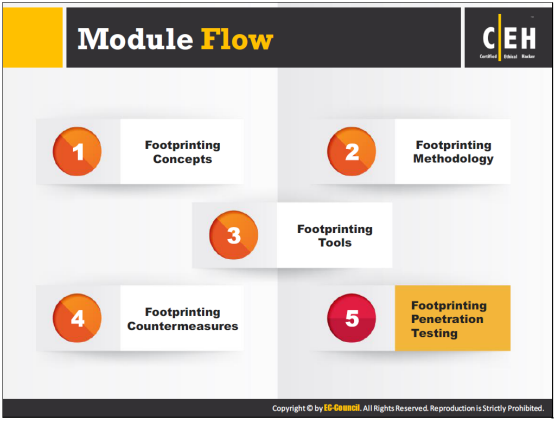
So far, we have discussed the importance of footprinting, various ways to perform footprinting, and the tools that help to conduct footprinting. Now we will discuss footprinting countermeasures, the measures or actions taken to prevent or offset information disclosure.



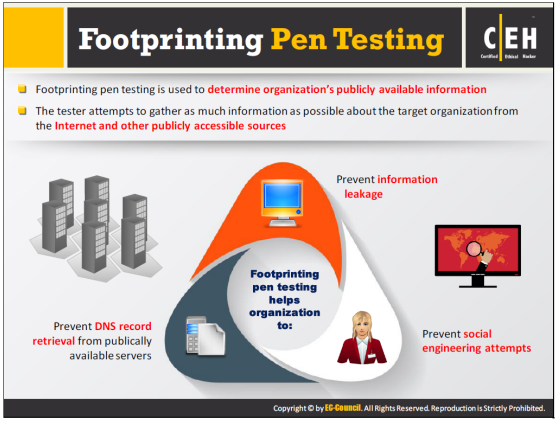


Other footprinting countermeasures include:

- Do not enable protocols that are not required.
- Always use TCP/IP and IPSec filters for defense in depth.
- Configure IIS to avoid information disclosure through banner grabbing.

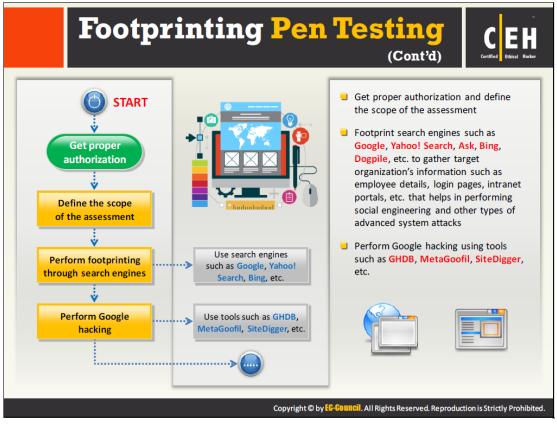


So far, we discussed all the necessary techniques and tools that can be used to footprint a target organization's network. Penetration testing (or pen testing) refers to the process of testing the organization's security posture using similar techniques and tools as that of an attacker, but with the knowledge and approval of the organization.. Footprinting is the first step to perform in the pen testing process. Performing footprinting in a systematic and methodical manner enables a pen tester to discover potential security liabilities that an attacker may exploit. In the pen testing process, the pen tester acts as a malicious outsider and simulates an attack to find security loopholes.



A footprinting pen test helps in determining an organization's publicly available information on the Internet such as network architecture, operating systems, applications, and users. 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 in which to gather as much information as possible in order to ensure the maximum scope of footprinting pen testing. If the pen tester finds sensitive information on any publicly available information resource, that information should be reported to the organization.



Pen testing is a procedural way of examining network security. Steps in the procedure should be followed in order, to ensure maximum scope of testing. The steps involved in footprinting pen testing are:

Step 1: Get proper authorization

Always perform pen testing with authorization. The first step in a footprinting pen test is to get proper authorization from the organization. This may or may not include the system administrators.

Step 2: Define the scope of the assessment

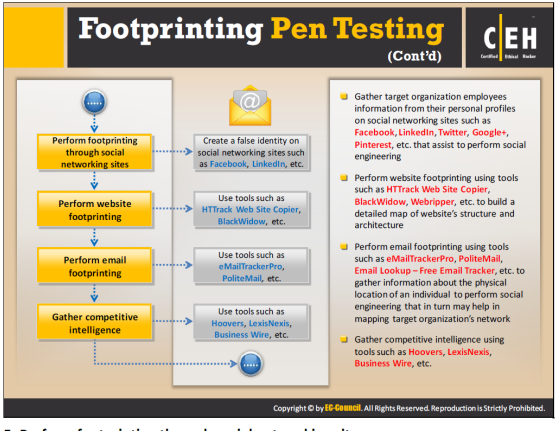
Defining the scope of the security assessment is a prerequisite for pen testing. Defining the scope of assessment determines the range of systems in the network to be tested and the resources that can be used to test, etc. It also determines the pen tester's limitations. Once you define the scope, you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

Step 3: Perform footprinting through search engines

Use 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 Google hacking

Perform Google hacking using tools such as GHDB, MetaGoofil, SiteDigger, etc. This helps to expose 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 5: Perform footprinting through social networking sites

Perform footprinting to gather target organization employee information from personal profiles on social networking sites such as Facebook, LinkedIn, Twitter, Google+, Pinterest, etc. This can assist in performing social engineering. You can also use people search engines to obtain information about a target person.

Step 6: Perform website footprinting

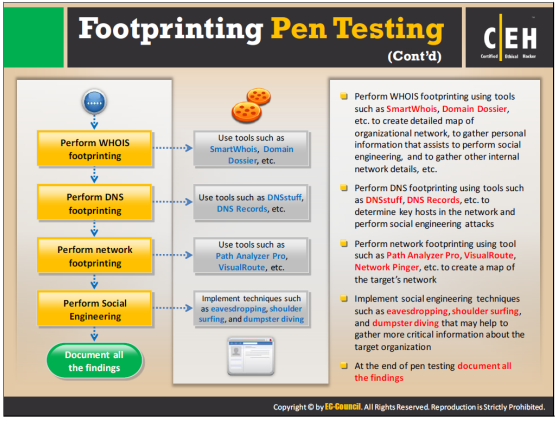
Perform website footprinting using tools such as HTTrack Web Site Copier, BlackWidow, etc. to build a detailed map of the website's structure and architecture.

Step 7: 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. Use this to perform social engineering that in turn may help in mapping the target organization's network. Analyzing email headers helps to collect information such as sender's IP address, sender's mail server, sender's address, data and time received by the originator's email servers, authentication system used by sender's mail server, sender's full name, etc.

Step 8: Gather competitive intelligence

Gather competitive intelligence using tools such as Hoover's, LexisNexis, Business Wire, etc. These tools extract competitor information such as its date of establishment, location, progress analysis, higher authorities, product analysis, marketing details, etc.



Step 9: Perform WHOIS footprinting

Perform WHOIS footprinting using tools such as SmartWhois, Domain Dossier, etc. to extract information about particular domains. You can get information such as IP address, domain owner name, registrant name, and contact details including phone numbers, email IDs, etc. You can use this information to create a detailed map of organizational network, to gather personal information that assists to perform social engineering, to gather other internal network details, etc.

Step 10: Perform DNS footprinting

Perform DNS footprinting using tools such as DNSstuff, DNS Records, etc. to determine key hosts in the network and to 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 a Path Analyzer Pro, VisualRoute, Network Pinger, etc. to learn the network range and other information about the target network that helps to draw the network diagram of the target.

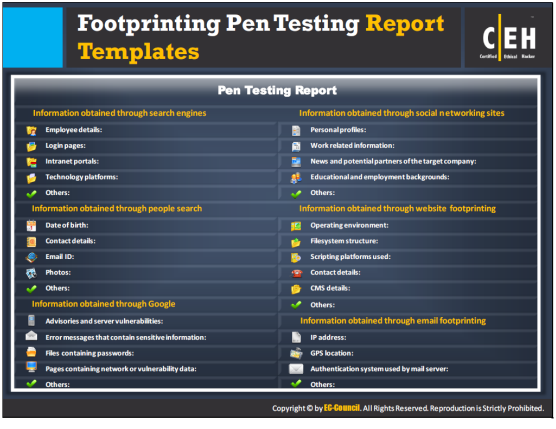
Step 12: Perform social engineering

Implement social engineering techniques such as eavesdropping, shoulder surfing, dumpster diving, and impersonation on social networking sites to gather critical information about the target organization. Through social engineering, you can gather target organization's security

products in use, OS and software versions, network layout information, IP addresses and names of servers, important personnel, etc.

Step 13: Document all the findings

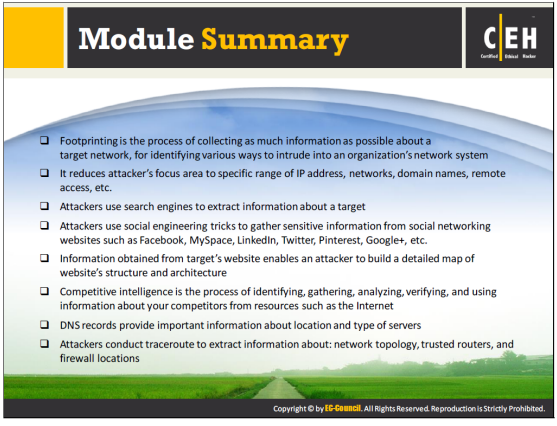
When finished with the implementation of all footprinting techniques, collect and document all the information obtained in every stage of testing. You can use this document to study, understand, and analyze the security posture of the target organization. This also enables you to find and fix security loopholes to prevent exploitation.



Conducting pen testing helps the organization to enhance its security perimeter. As a pen tester, you should gather sensitive information such as server details, OS, etc. of the target organization by conducting footprinting. Analyze the system and network defenses by breaking into its security with authorization (i.e., ethically) without causing any damage. Find the loopholes and weaknesses in the network or system security and list them along with respective countermeasures in a pen testing report. The pen testing report results from 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. Always keep the report confidential. If this information falls into the hands of attacker, the information in the report could be used to launch attacks.

Given below is the pen testing report template containing the information obtained through various footprinting techniques – footprinting through search engines, footprinting through social networking sites, footprinting through people search websites, website footprinting, footprinting through Google, and email footprinting.

The slide displays the pen testing report template showing information obtained through footprinting techniques - competitive intelligence, WHOis footprinting, DNS footprinting, network footprinting, and social engineering.



This module ends with an overview discussion on footprinting methodology. In the next module, we will see how attackers as well as ethical hackers and pen testers perform network scanning to collect information about a target of evaluation before an attack or audit.