
C|EH
Certified Ethical Hacker
Module 02
Footprinting and Reconnaissance

# Module Objectives

Module Objectives

- Understanding Footprinting Concepts
- Footprinting through Search Engines and Advanced Google Hacking Techniques
- Footprinting through Web Services and Social Networking Sites
- Understanding Website Footprinting, Email Footprinting, and Competitive Intelligence
- Understanding WHOIS, DNS, and Network Footprinting
- Footprinting through Social Engineering
- Understanding different Footprinting Tools and Countermeasures
- Understanding Footprinting Penetration Testing

# Module Flow

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures
5. Footprinting Penetration Testing

# What is Footprinting?

- Footprinting is the first step of any attack on information systems in which an attacker **collects information about a target network** for identifying various ways to intrude into the system

## Types of Footprinting

| Passive Footprinting | Active Footprinting |
|---|---|
| Gathering information about a target **without direct interaction** | Gathering information about the target **with direct interaction** |

## Information Obtained in Footprinting

| Organization Information | Network Information | System Information |
|---|---|---|
| Employee details, telephone numbers, location, background of the organization, web technologies, etc. | Domain and sub-domains, network blocks, IP addresses of the reachable systems, Whois record, DNS, etc. | OSes and location of web servers, users and passwords, etc. |

# Objectives of Footprinting



**Know Security Posture**

Footprinting allows attackers to know the **security posture of the target organization**

**Reduce Focus Area**

It **reduces the attacker's focus area** to a specific range of IP addresses, networks, domain names, remote access, etc.

**Identify Vulnerabilities**

It allows attacker to **identify vulnerabilities** in the target systems in order to select appropriate exploits

**Draw Network Map**

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

# Module Flow

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures
5. Footprinting Penetration Testing

# Footprinting through Search Engines



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

- Major search engines:

Google Bing YAHOO! Ask.com Aol. Baidu 百度 DuckDuckGo

- Attackers can use **advanced search operators** available with these search engines and create complex queries to find, filter, and sort specific information regarding the target

- Search engines are also used to find all other sources of **publically accessible information resources**, e.g., you can type "Top Job Portals" to find major job portals that provide critical information about the target organization

# Footprint Using Advanced Google Hacking Techniques

- Google hacking refers to the use of advanced Google search operators for **creating complex search queries** in order to extract sensitive or hidden information that helps attackers to **find vulnerable targets**

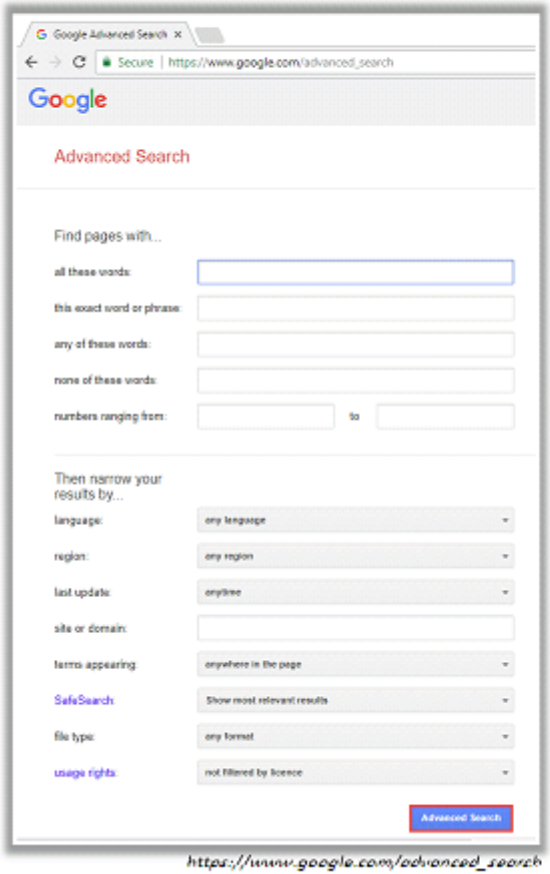
**Google supports several advanced operators *that help in modifying the search***

- **[cache:]** Displays the web pages stored in the Google cache
- **[link:]** Lists web pages that have links to the specified web page
- **[related:]** Lists web pages that are similar to a specified web page
- **[info:]** Presents some information that Google has about a particular web page
- **[site:]** Restricts the results to those websites in the given domain
- **[allintitle:]** Restricts the results to those websites with all of the search keywords in the title
- **[intitle:]** Restricts the results to documents containing the search keyword in the title
- **[allinurl:]** Restricts the results to those with all of the search keywords in the URL
- **[inurl:]** Restricts the results to documents containing the search keyword in the URL
- **[location:]** Finds information for a specific location

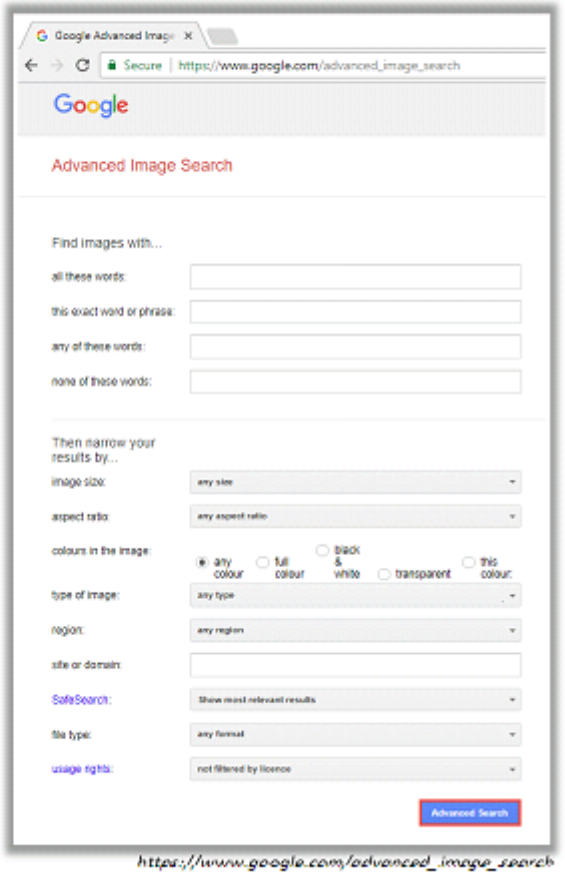
# Information Gathering Using Google Advanced Search and Image Search



- With **Google Advanced Search** and **Advanced Image Search**, you can search web more precisely and accurately
- You can use these search features to achieve the same precision as of using the advanced operators but **without typing or remembering these operators**
- You can use Google Advanced Image Search to **check out pictures** of the target, its location, employees, etc.




https://www.google.com/advanced_search




https://www.google.com/advanced_image_search

# Google Hacking Database

- The Google Hacking Database (GHDB) is an authoritative source for **querying the ever-widening reach of the Google search engine**
- The Exploit Database is a **Common Vulnerabilities and Exposures (CVE) compliant archive of public exploits** and corresponding vulnerable software


*https://www.exploit-db.com*

# VoIP and VPN Footprinting through Google Hacking Database

## Google search queries for VoIP footprinting

| Google Dork | Description |
|---|---|
| intitle:"Login Page" intext:"Phone Adapter Configuration Utility" | Pages containing login portals |
| inurl:/voice/advanced/ intitle:Linksys SPA configuration | Finds the Linksys VoIP router configuration page |
| intitle:"D-Link VoIP Router" "Welcome" | Pages containing D-Link login portals |
| intitle:asterisk.management.portal web-access | Look for the Asterisk management portal |
| inurl:"NetworkConfiguration" cisco | Find the Cisco phone details |
| inurl:"ccmuser/logon.asp" | Find Cisco call manager |
| intitle:asterisk.management.portal web-access | Finds the Asterisk web management portal |
| inurl:8080 intitle:"login" intext:"UserLogin" "English" | VoIP login portals |
| intitle:" SPA Configuration" | Search Linksys phones |

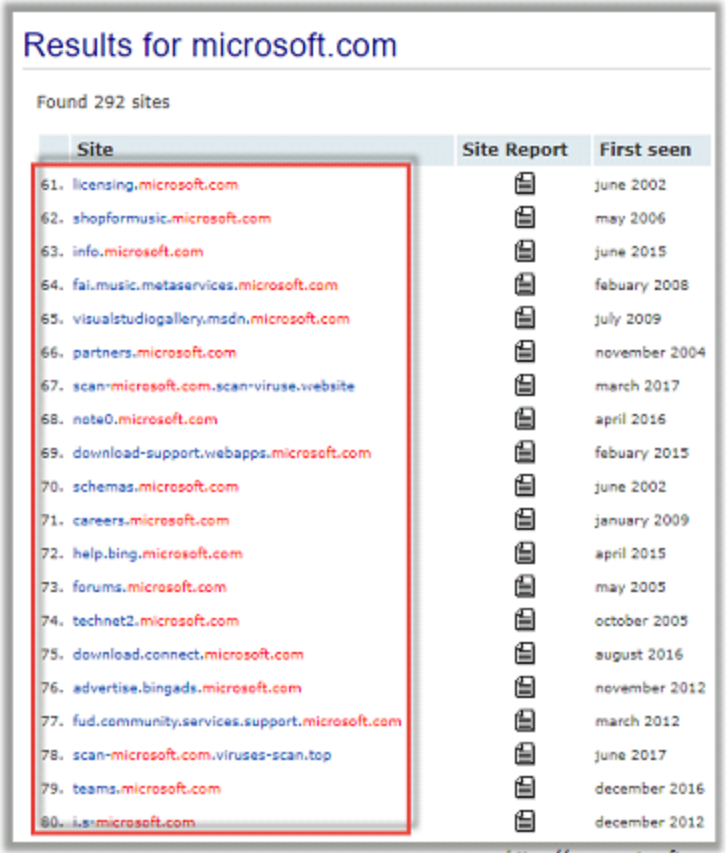
## Google search queries for VPN footprinting

| Google Dork | Description |
|---|---|
| filetype:pcf "cisco" "GroupPwd" | Cisco VPN files with Group Passwords for remote access |
| "[main]" "enc_GroupPwd=" ext:txt | Finds Cisco VPN client passwords (encrypted, but easily cracked!) |
| "Config" intitle:"Index of" intext:vpn | Directory with keys of VPN servers |
| inurl:/remote/login?lang=en | Finds FortiGate Firewall's SSL-VPN login portal |
| !Host=*.* intext:enc_UserPassword=* ext:pcf | Look for .pcf files which contains user VPN profiles |
| filetype:rcf inurl:vpn | Finds Sonicwall Global VPN Client files containing sensitive information and login |
| filetype:pcf vpn OR Group | Finds publicly accessible profile configuration files (.pcf) used by VPN clients |

*https://www.exploit-db.com*

# Finding Company's Top-level Domains (TLDs) and Sub-domains

- Search for the target company's external URL in a search engine such as **Google**, **Bing**, etc.
- Sub-domains **provide an insight** into different departments and business units in an organization
- You may find a company's sub-domains by **trial and error method** or using a service such as ***https://www.netcraft.com***
- You can use **Sublist3r** python script that enumerates subdomains across multiple sources at once

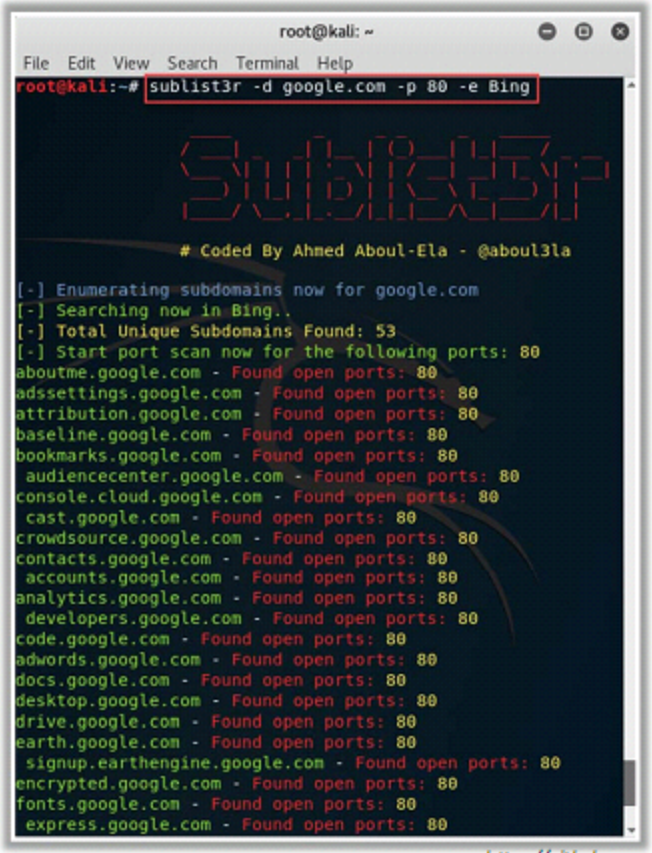


Results for microsoft.com

Found 292 sites

| | Site | Site Report | First seen |
|---|---|---|---|
| 61. | licensing.microsoft.com | | june 2002 |
| 62. | shopformusic.microsoft.com | | may 2006 |
| 63. | info.microsoft.com | | june 2015 |
| 64. | fai.music.metaservices.microsoft.com | | febuary 2008 |
| 65. | visualstudiogallery.msdn.microsoft.com | | july 2009 |
| 66. | partners.microsoft.com | | november 2004 |
| 67. | scan-microsoft.com.scan-viruse.website | | march 2017 |
| 68. | note0.microsoft.com | | april 2016 |
| 69. | download-support.webapps.microsoft.com | | febuary 2015 |
| 70. | schemas.microsoft.com | | june 2002 |
| 71. | careers.microsoft.com | | january 2009 |
| 72. | help.bing.microsoft.com | | april 2015 |
| 73. | forums.microsoft.com | | may 2005 |
| 74. | technet2.microsoft.com | | october 2005 |
| 75. | download.connect.microsoft.com | | august 2016 |
| 76. | advertise.bingads.microsoft.com | | november 2012 |
| 77. | fud.community.services.support.microsoft.com | | march 2012 |
| 78. | scan-microsoft.com.viruses-scan.top | | june 2017 |
| 79. | teams.microsoft.com | | december 2016 |
| 80. | i.s-microsoft.com | | december 2012 |

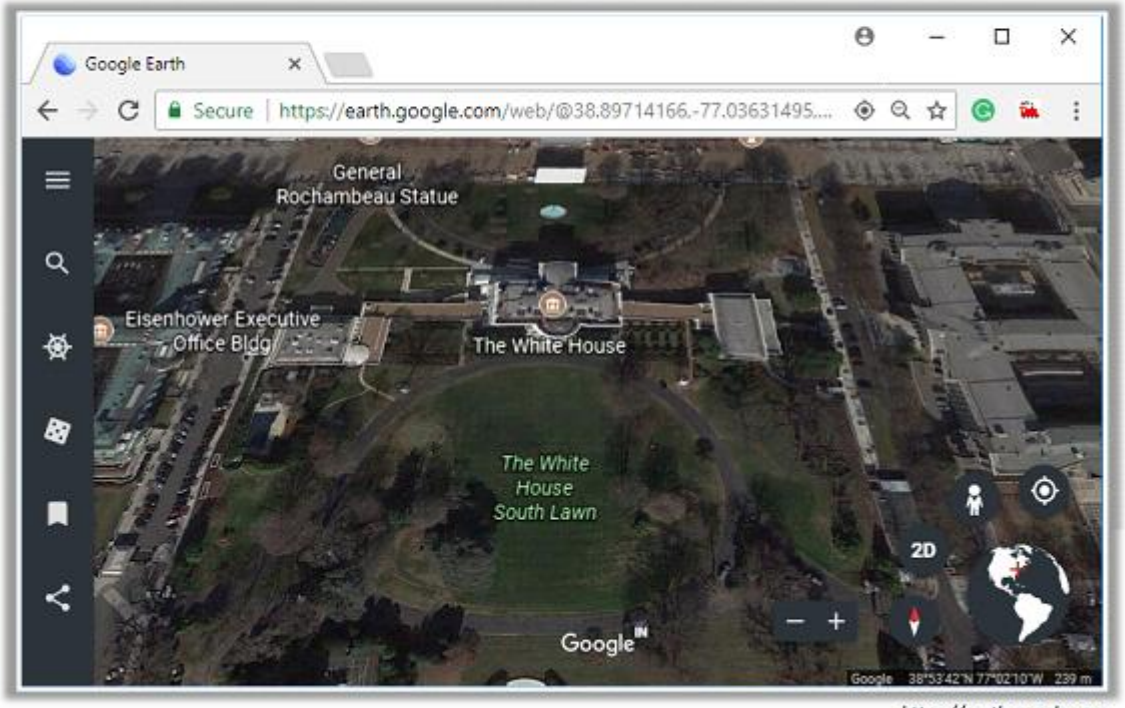
*https://www.netcroft.com*




*https://github.com*

# Finding the Geographical Location of the Target

Attackers use **Google Earth** tool to get the physical location of the target, which helps them to perform social engineering and other non-technical attacks



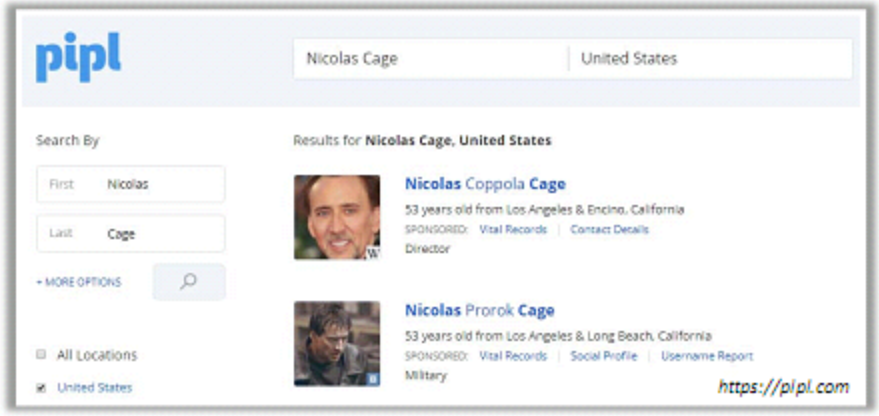

- **Google Maps** — *https://maps.google.com*
- **Wikimapia** — *http://www.wikimapia.org*
- **National Geographic Maps** — *http://maps.nationalgeographic.com*
- **Yahoo Maps** — *https://maps.yahoo.com*
- **Bing Maps** — *https://www.bing.com/maps*

# People Search on Social Networking Sites and People Search Services

- Social networking services provide **useful information about the individual** that helps the attacker in performing social engineering and other attacks
- The people search can provide critical **information about a person or organization** including location, emails, websites, blogs, contacts, important dates, etc.

- Facebook (*https://www.facebook.com*)
- Twitter (*https://twitter.com*)
- LinkedIn (*https://www.linkedin.com*)
- Google+ (*https://plus.google.com*)
- YouTube (*https://www.youtube.com*)

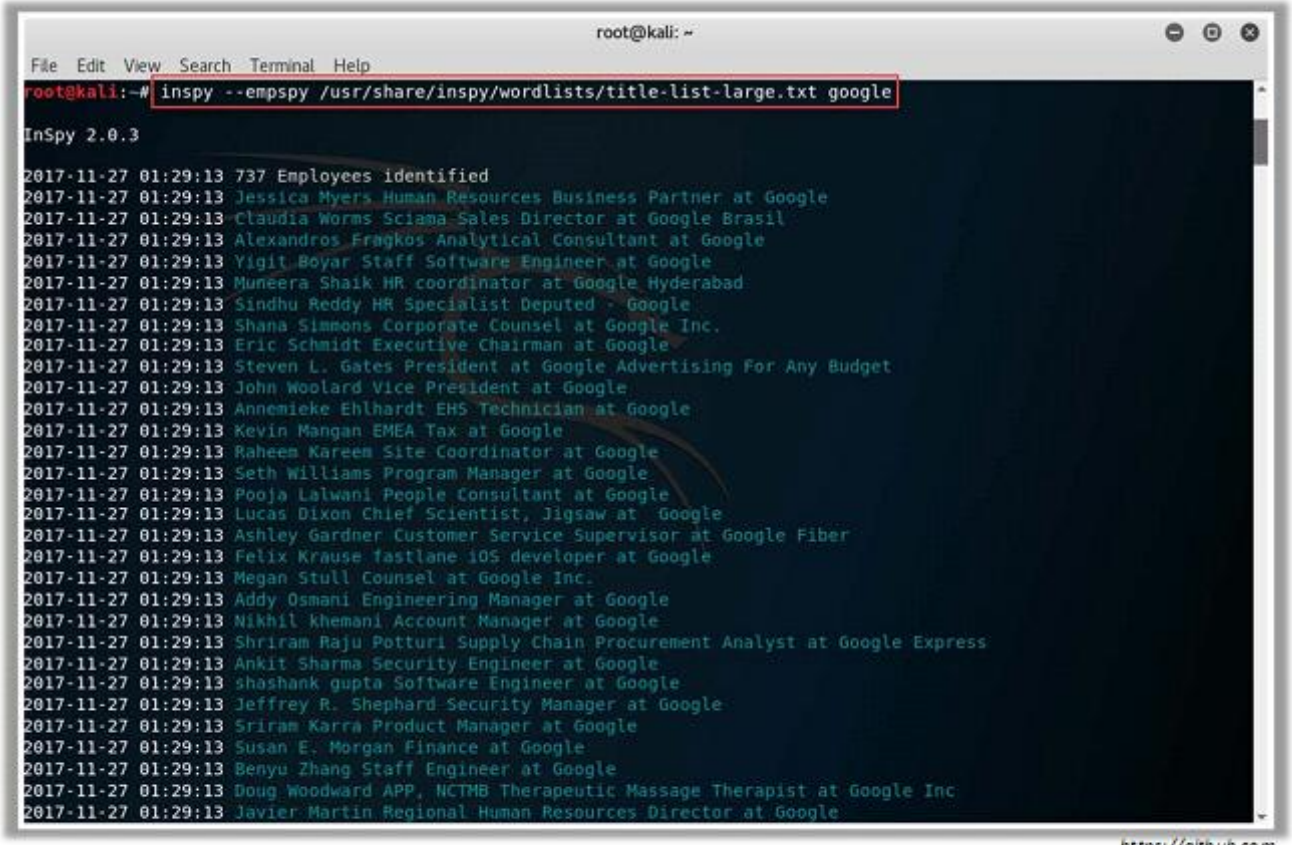
- Information about an individual can be found at various **people search websites**




- Intelius (*https://www.intelius.com*)
- BeenVerified (*https://www.beenverified.com*)
- Spokeo (*https://www.spokeo.com*)

# Gathering Information from LinkedIn

- Attacker use **InSpy** utility, which performs enumeration on LinkedIn and finds people based on job title, company, or email address
- InSpy has two functionalities:
  - **TechSpy**: Crawls LinkedIn job listings for technologies used by the target company
  - **EmpSpy**: Crawls LinkedIn for employees working at the provided company



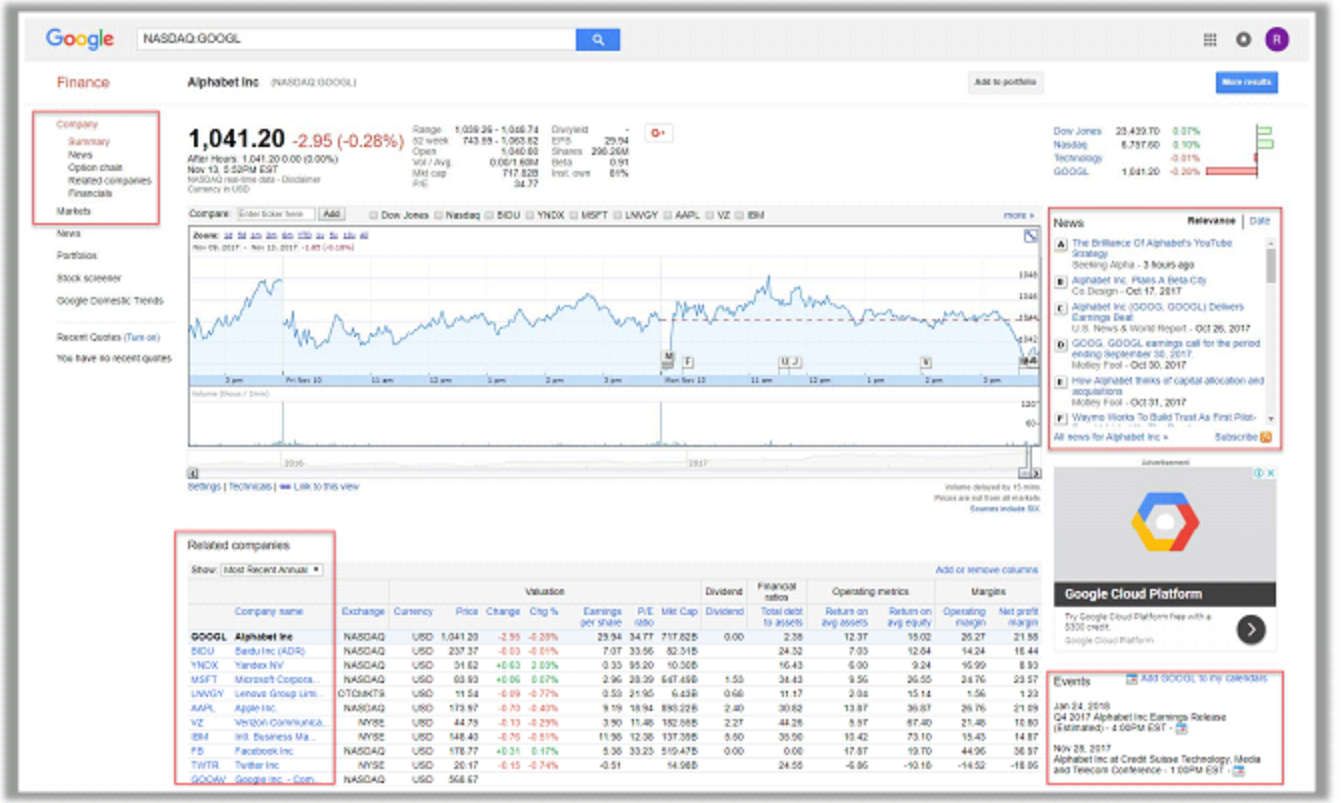

https://github.com

# Gathering Information from Financial Services

- Financial services provide a useful information about the target company such as the **market value of a company's shares**, **company profile**, **competitor details**, etc.

## Online Financial Services

- Yahoo! Finance (*https://finance.yahoo.com*)
- TheStreet (*https://www.thestreet.com*)
- MarketWatch (*https://www.marketwatch.com*)

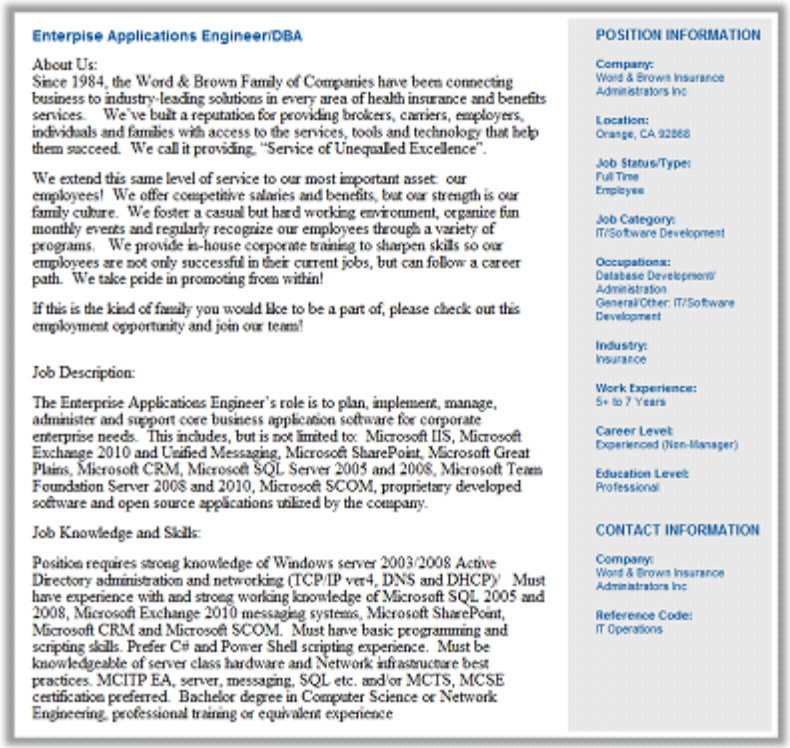



*https://www.google.com/finance*

# Footprinting through Job Sites



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



**Enterpise Applications Engineer/DBA**

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

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

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

Job Description:

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

Job Knowledge and Skills:

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

POSITION INFORMATION

Company:
Word & Brown Insurance Administrators Inc

Location:
Orange, CA 92868

Job Status/Type:
Full Time
Employee

Job Category:
IT/Software Development

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

Industry:
Insurance

Work Experience:
5+ to 7 Years

Career Level:
Experienced (Non-Manager)

Education Level:
Professional

CONTACT INFORMATION

Company:
Word & Brown Insurance Administrators Inc

Reference Code:
IT Operations

**Look for these:**

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

**Examples of Job Websites**

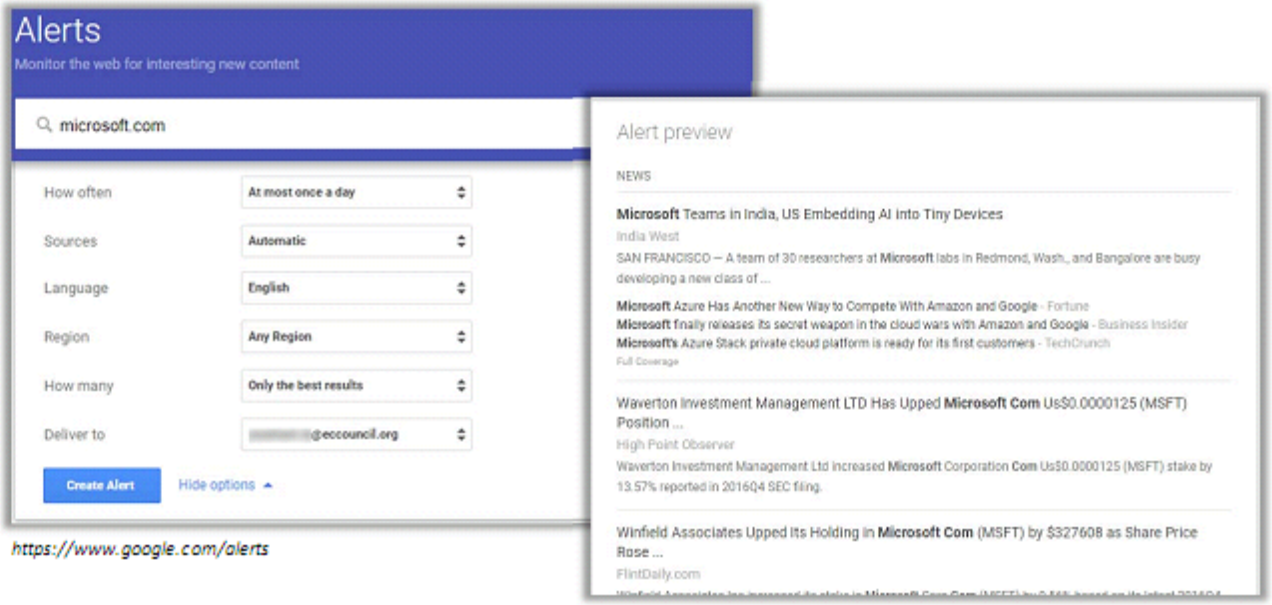
- https://www.indeed.com
- http://www.careerbuilder.com
- http://www.dice.com
- https://www.glassdoor.com
- https://www.linkedin.com
- https://www.monster.com

# Monitoring Target Using Alerts

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

## Examples of Alert Services

1. Google Alerts (*https://www.google.com/alerts*)
2. Twitter Alerts (*https://twitter.com/alerts*)
3. Giga Alert (*http://www.gigaalert.com*)
4. TalkWalker Alerts (*https://www.talkwalker.com*)




*https://www.google.com/alerts*

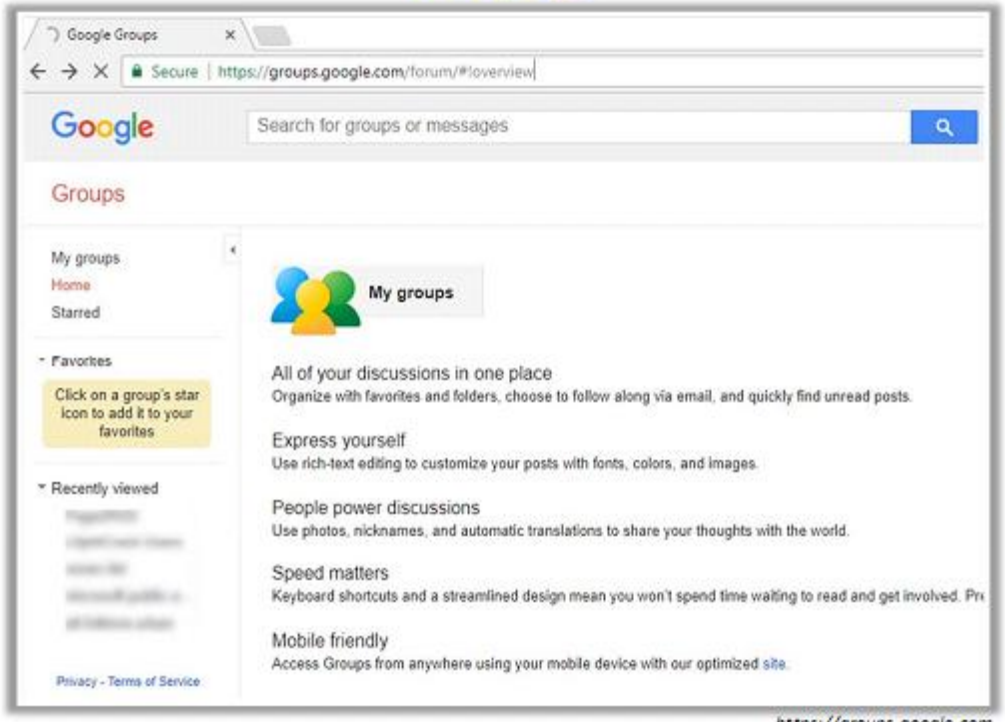
# Information Gathering Using Groups, Forums, and Blogs



Groups, forums, and blogs provide sensitive information about a target such as **public network information**, **system information**, **personal information**, etc.

Register with fake profiles in **Google groups**, **Yahoo groups**, etc. and try to join the target organization's employee groups where they share personal and company information

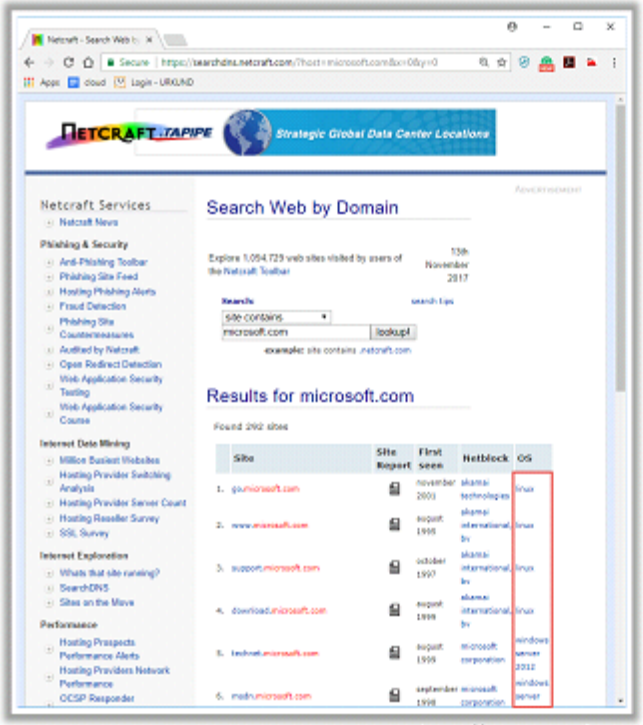
Search for information by Fully Qualified Domain Names (**FQDNs**), **IP addresses**, and **usernames** in groups, forums, and blogs




*https://groups.google.com*

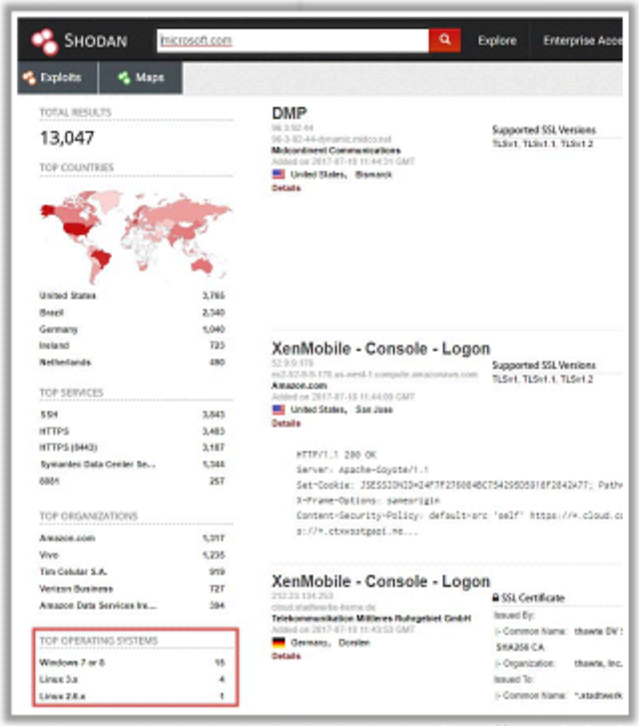
# Determining the Operating System

- Use the **Netcraft** tool to determine the **Operating Systems** in use by the target organization



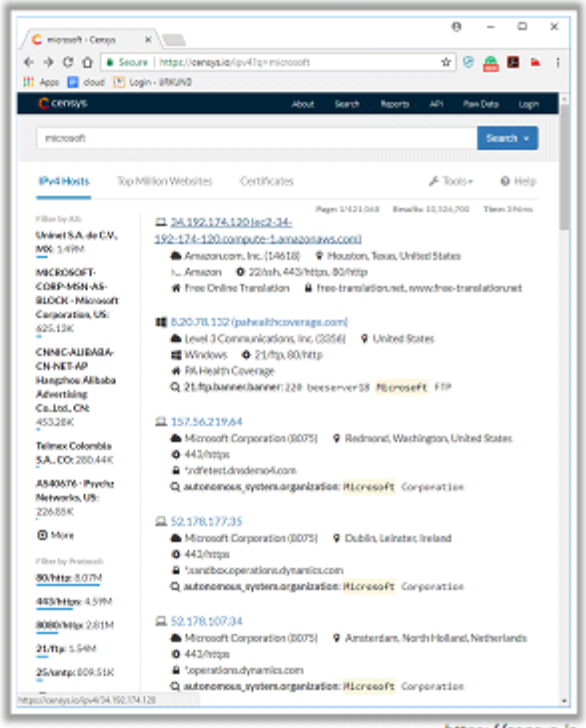

https://www.netcraft.com

- **SHODAN** search engine lets you **find connected devices** (routers, servers, IoT, etc.) using a variety of filters




https://www.shodan.io

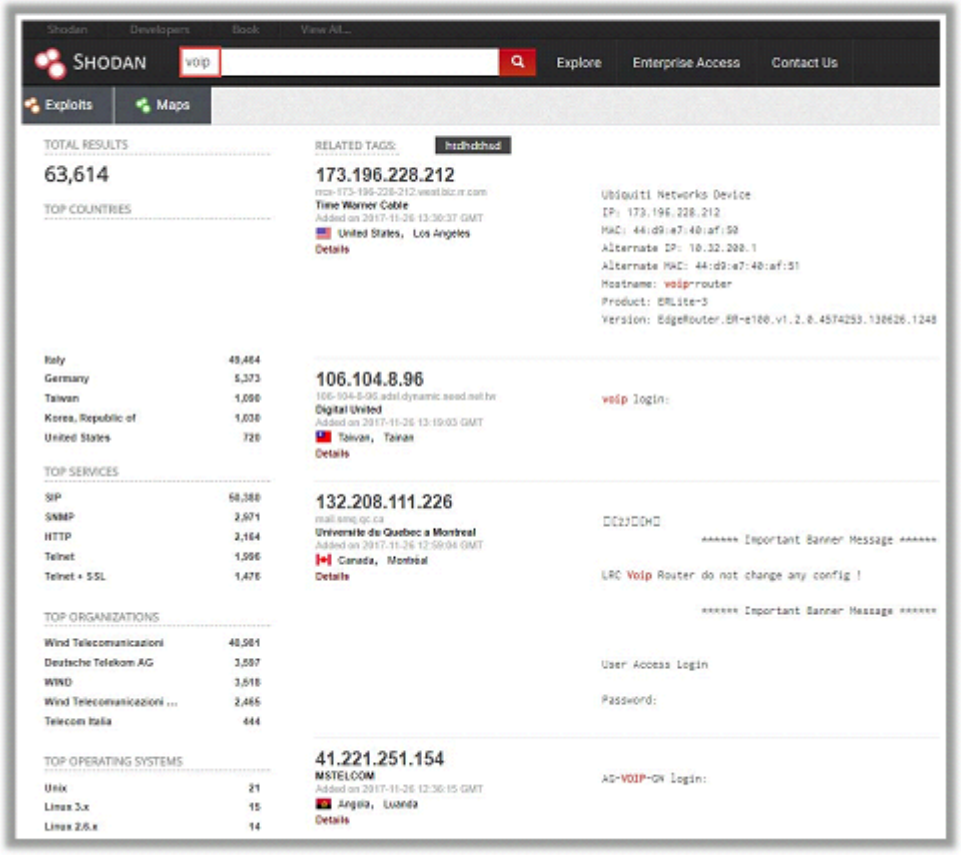
- **Censys** search engine enables researchers to ask questions about the **hosts and networks that compose the Internet**

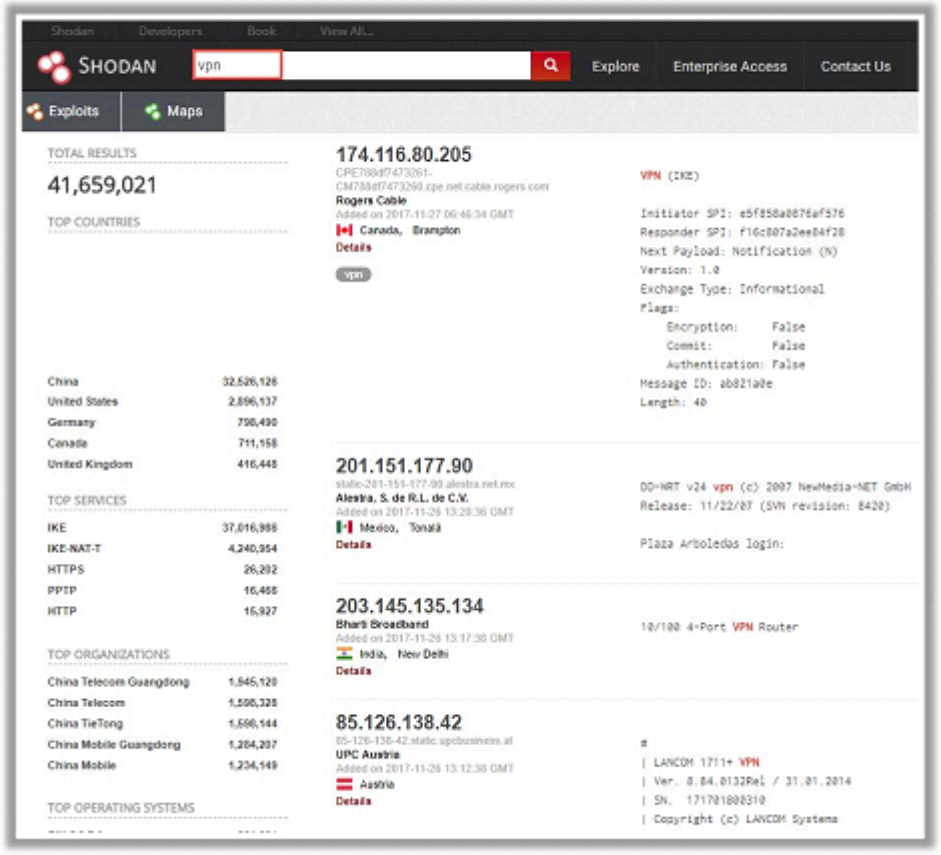



https://censys.io

# VoIP and VPN Footprinting through SHODAN





# Collecting Information through Social Engineering on Social Networking Sites



Attackers use **social engineering trick** to gather sensitive information from social networking websites

Attackers create a **fake profile** and then use the false identity to lure the employees to give up their sensitive information

Attackers collect information about employees' **interests** and then trick them to reveal more information

| What Users Do | What Attacker Gets |
|---|---|
| Maintain profile | Contact info, location, etc. |
| Connect to friends, chatting | Friends list, friend's info, etc. |
| Share photos and videos | Identity of family members, interests, etc. |
| Play games, join groups | Interests |
| Creates events | Activities |

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

# Website Footprinting

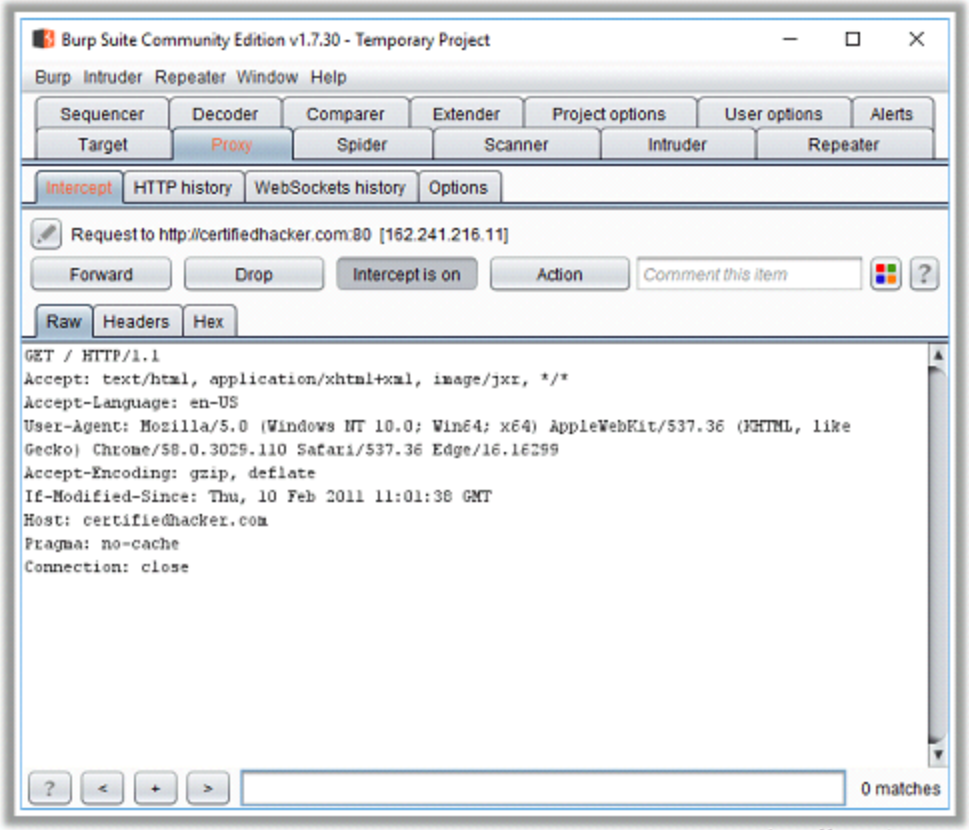
- Website footprinting refers to **monitoring and analyzing the target organization's website** for information

Browsing the target website may provide:

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

Use **Burp Suite**, **Zaproxy**, **Paros Proxy**, **Website Informer**, **Firebug**, etc. to view headers that provide:

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

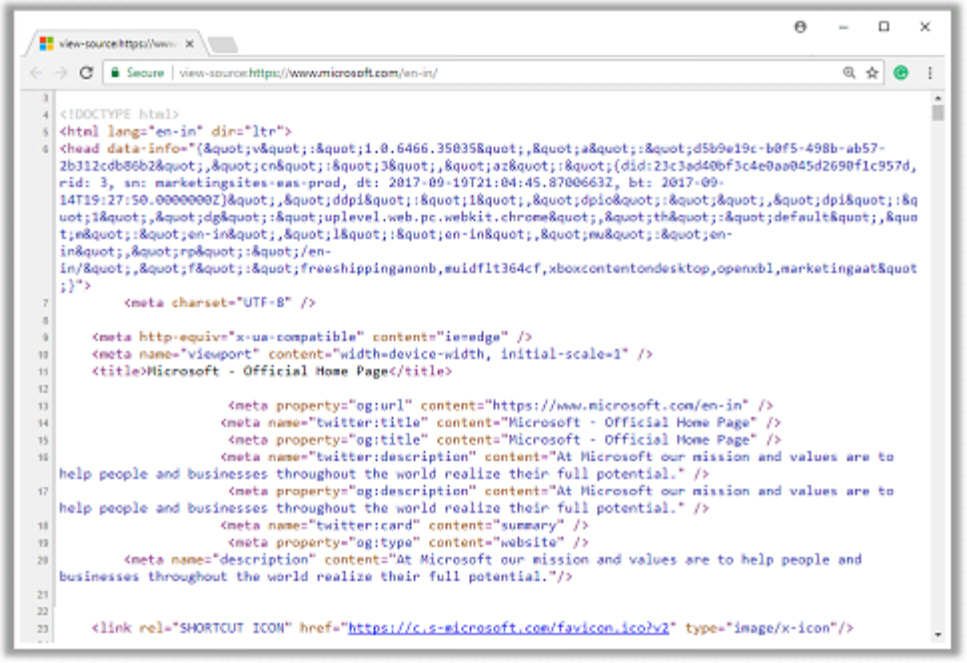



https://portswigger.net

# Website Footprinting (Cont'd)

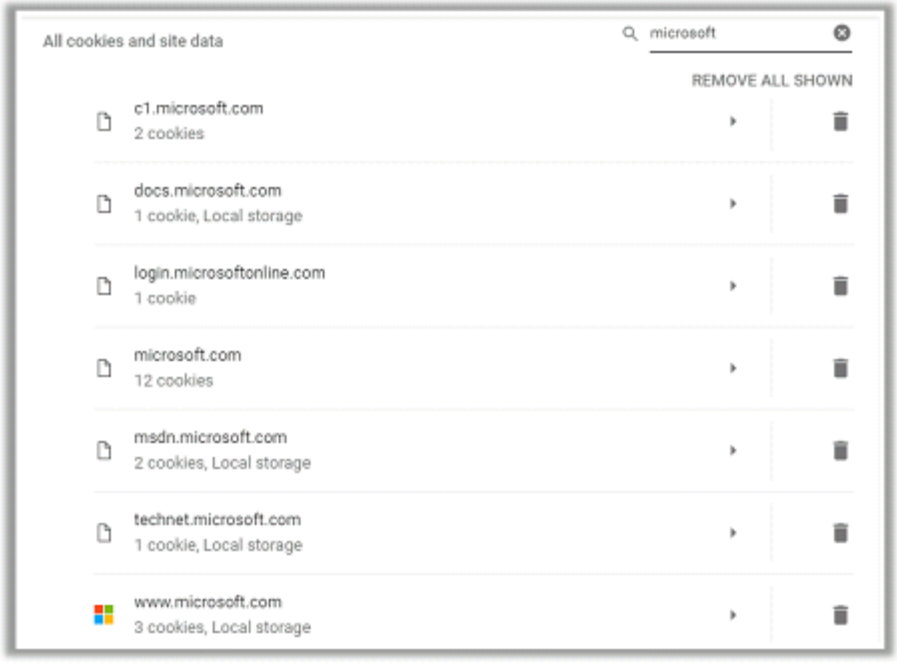
## Examining HTML source provide:

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




## Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used



# Website Footprinting using Web Spiders

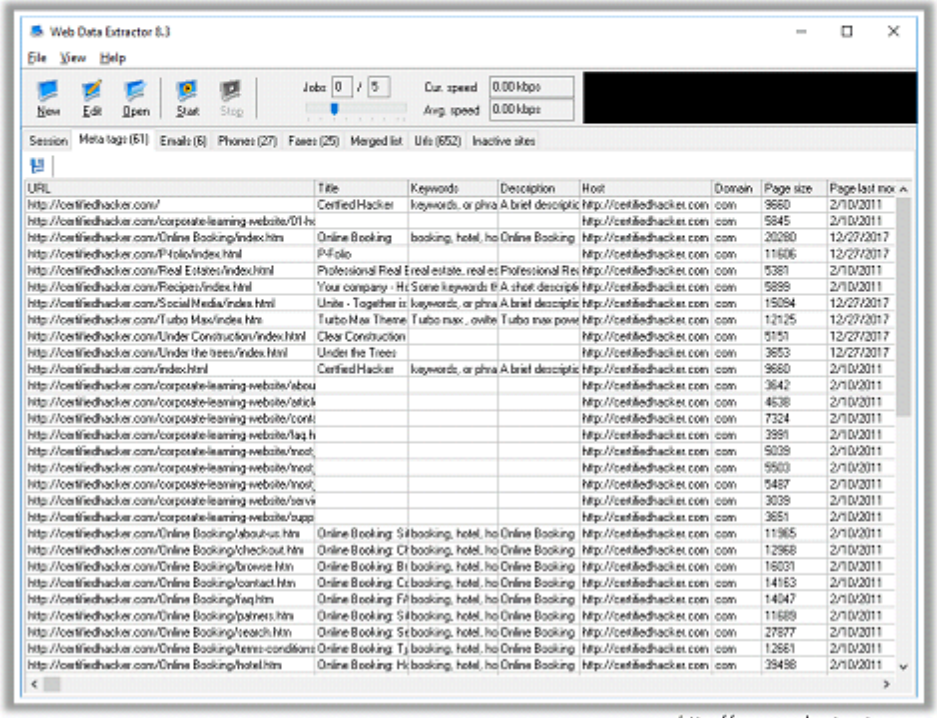
- Web spiders perform automated searches on the target website and collect specified information such as **employee names**, **email addresses**, etc.
- Attackers use the collected information to perform further **footprinting** and **social engineering attacks**

## Web Spidering Tools

- SpiderFoot (*http://www.spiderfoot.net*)
- Visual SEO Studio (*https://visual-seo.com*)
- WildShark SEO Spider Tool (*https://wildshark.co.uk*)
- Beam Us Up SEO Spider SEO (*http://beamusup.com*)

## Web Data Extractor

Web Data Extractor is a tool that **automatically extracts** specific information from **web pages**




*http://www.webextractor.com*

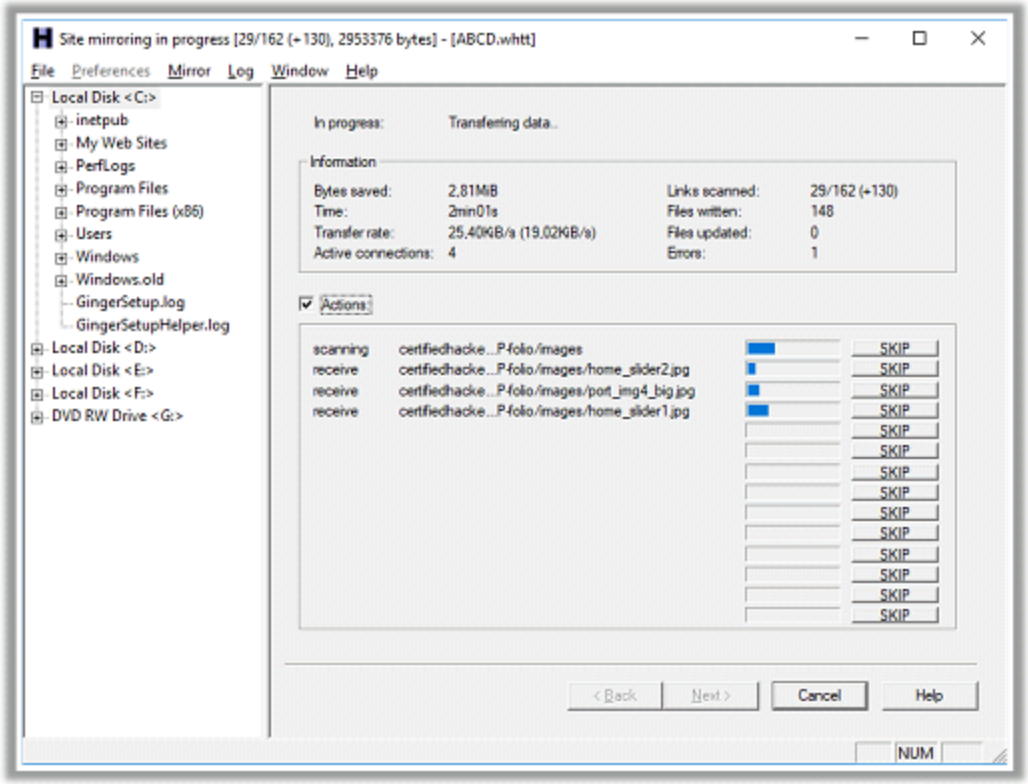
# Mirroring Entire Website

- Mirroring an entire website onto the local system enables an attacker to browse website offline; it also assists in finding **directory structure** and other valuable information from the mirrored copy without multiple requests to web server
- Web mirroring tools allow you to **download a website to a local directory**, building recursively all directories, HTML, images, flash, videos, and other files from the server to your computer

## Web Mirroring Tools

- NCollector Studio (*http://www.calluna-software.com*)
- Teleport Pro (*http://www.tenmax.com*)
- Portable Offline Browser (*http://www.metaproducts.com*)
- Website Ripper Copier (*http://www.tensons.com*)
- Gnu Wget (*https://www.gnu.org*)

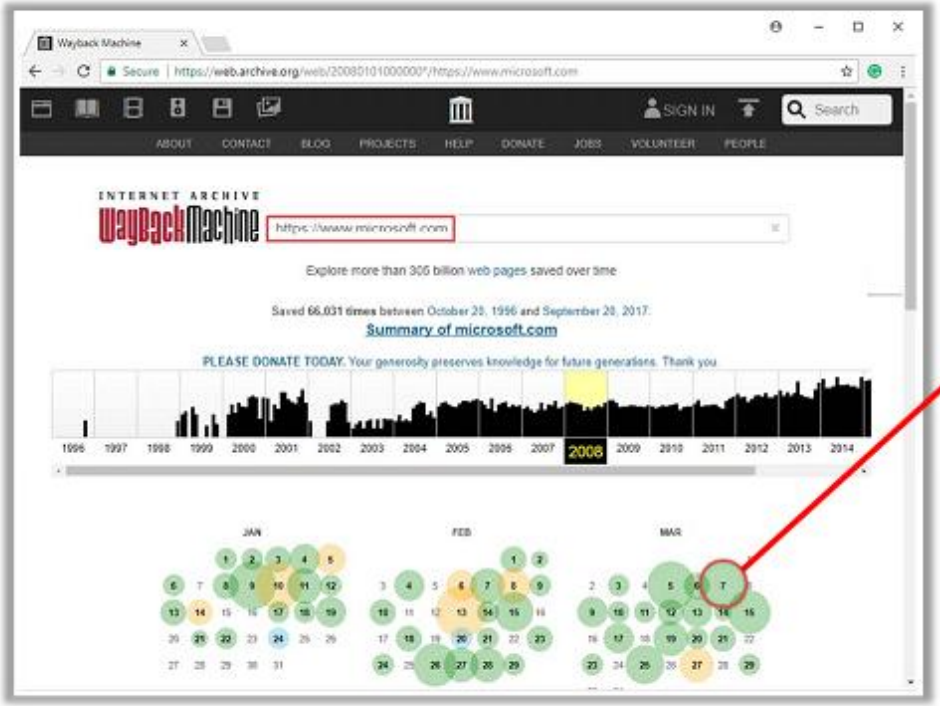
## HTTrack Web Site Copier

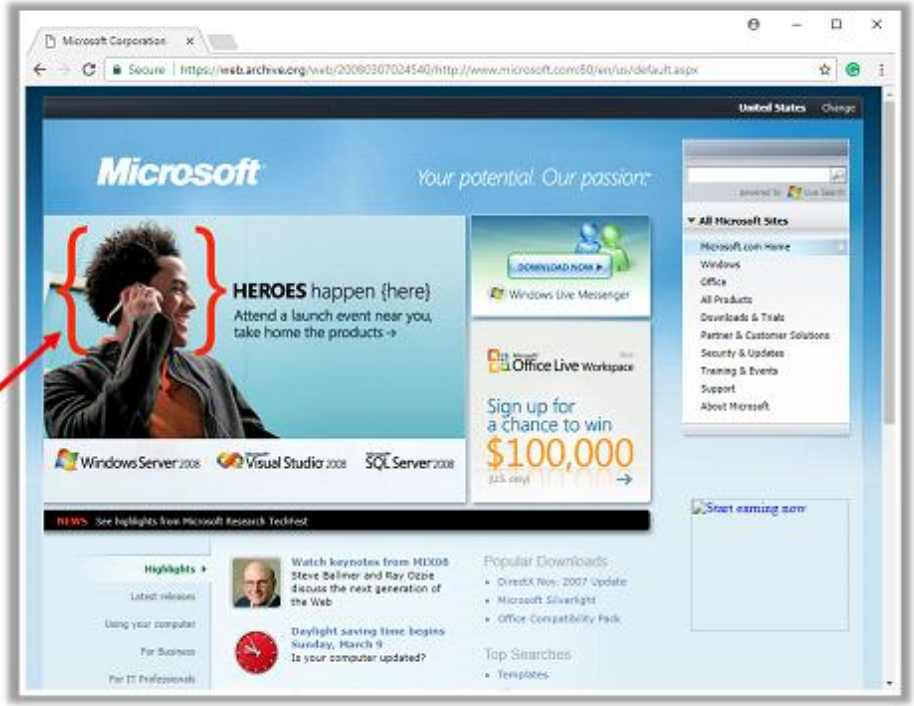



http://www.httrack.com

# Extracting Website Information from https://archive.org

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



# Extracting Metadata of Public Documents

- Useful information may reside on the target organization' website in the form of **pdf documents**, **Microsoft Word files**, etc.
- Attackers use this metadata and hidden information in order to perform **social engineering** and other attacks

## Metagoofil

- Metagoofil extracts metadata of public documents (pdf, doc, xls, ppt, docx, pptx, xlsx, etc.) belonging to a target company

```
*************************************
* Metagoofil Ver 2.1 -              *
* Christian Martorella              *
* Edge-Security.com                 *
* cmartorella_at_edge-security.com  *
* Blackhat Arsenal Edition          *
*************************************

[-] Starting online search...

[-] Searching for doc files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 4 files found
Starting to download 50 of them:
----------------------------------------

[1/50] /webhp?hl=en
Error downloading /webhp?hl=en
[2/50] /intl/en/ads
Error downloading /intl/en/ads
[3/50] /services
Error downloading /services
[4/50] /intl/en/policies/

[-] Searching for pdf files, with a limit of 200
        Searching 100 results...
        Searching 200 results...
Results: 34 files found
Starting to download 50 of them:
```

*https://code.google.com*

## Metadata Extraction Tools

- ExtractMetadata (*http://www.extractmetadata.com*)
- FOCA (*https://www.elevenpaths.com*)
- Meta Tag Analyzer (*https://www.seocentro.com*)
- BuzzStream (*http://tools.buzzstream.com*)
- Analyse Metadata (*http://www.exadium.com*)
- Exiftool (*http://www.sno.phy.queensu.ca*)

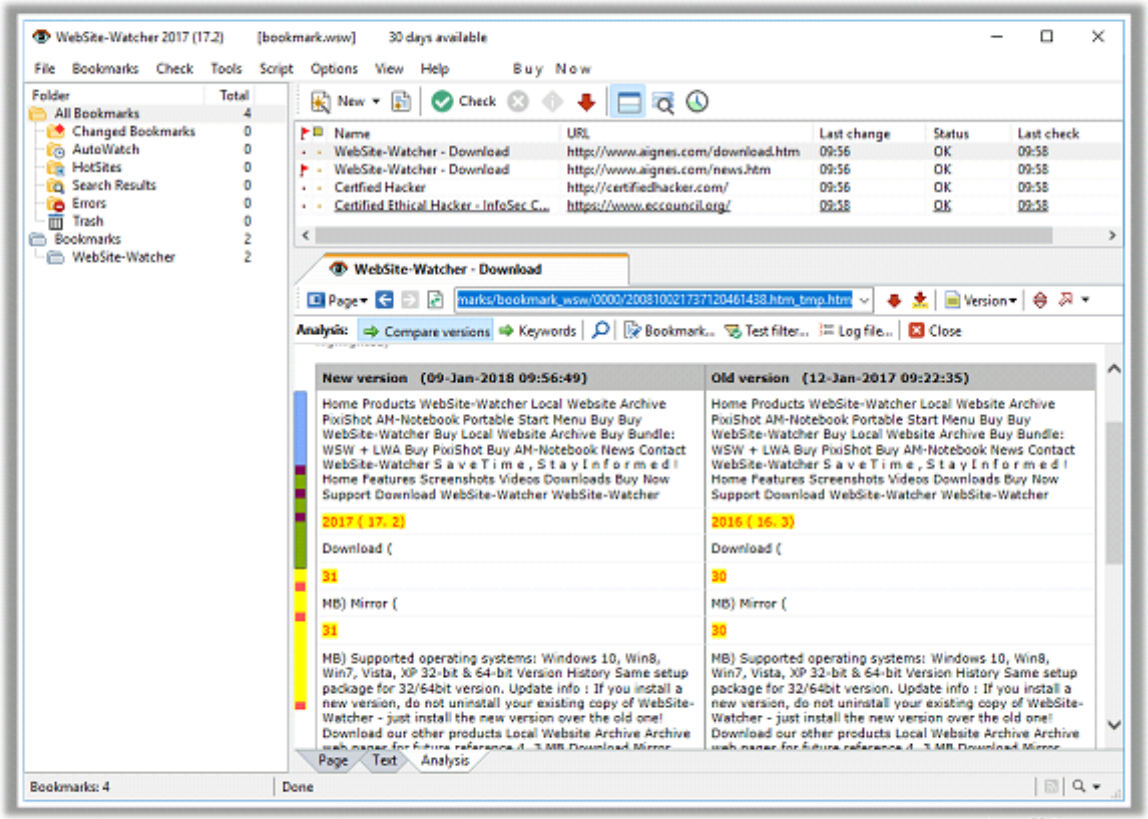
# Monitoring Web Pages for Updates and Changes

## WebSite-Watcher

WebSite-Watcher allows you to **automatically check web pages** for updates and changes

## Web Updates Monitoring Tools

- VisualPing (*https://visualping.io*)
- Follow That Page (*https://www.followthatpage.com*)
- Versionista (*https://versionista.com*)
- WatchThatPage (*http://www.watchthatpage.com*)
- OnWebChange (*https://onwebchange.com*)



# Tracking Email Communications

- Email tracking is used to **monitor the delivery of emails** to an intended recipient
- Attackers track emails to gather information about a **target recipient** in order to perform social engineering and other attacks

Get recipient's system IP address

Geolocation of the recipient

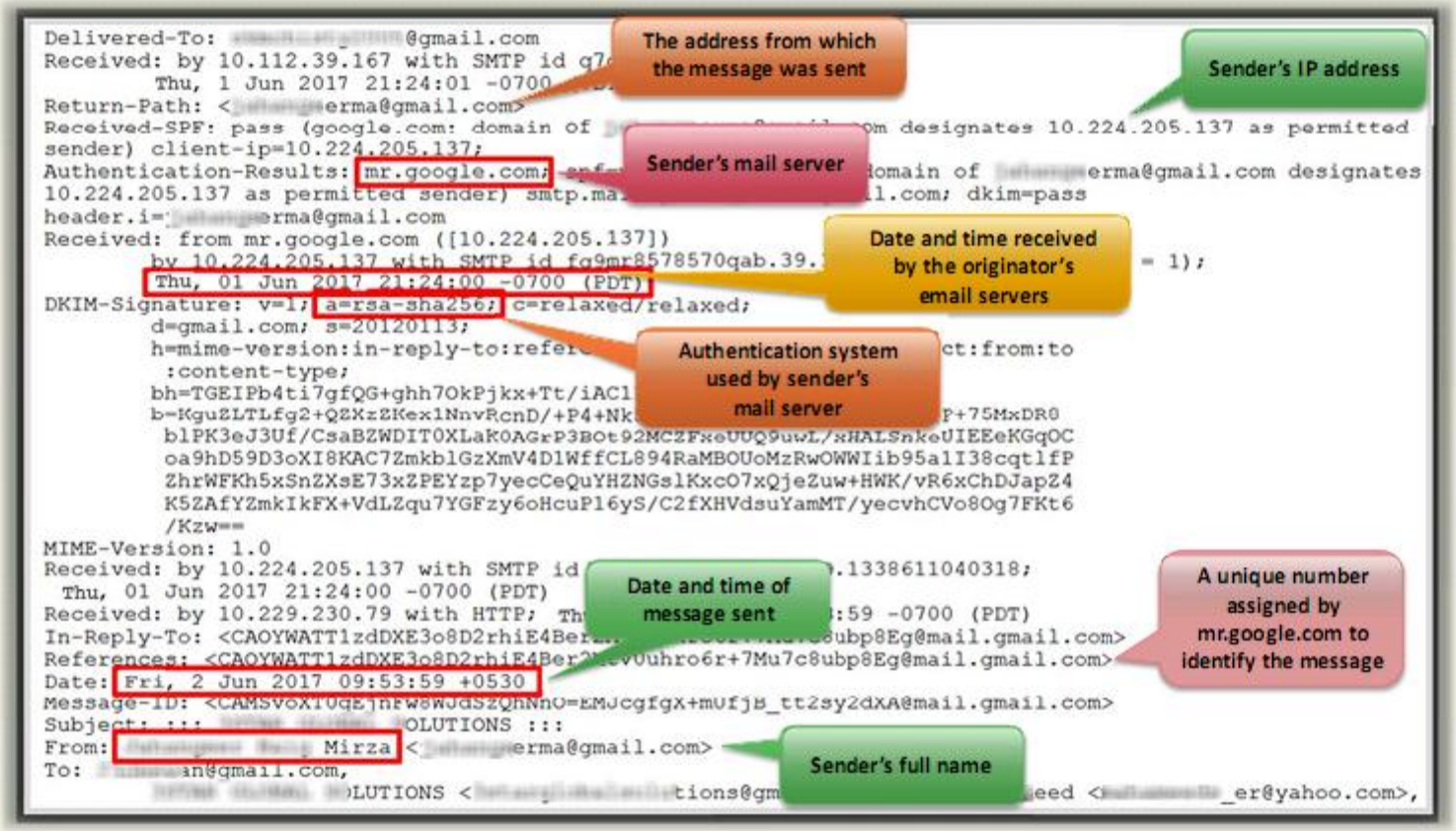
When the email was received and read

Whether or not the recipient visited any links sent to them

Get recipient's browser and operating system information

Time spent on reading the emails

# Collecting Information from Email Header

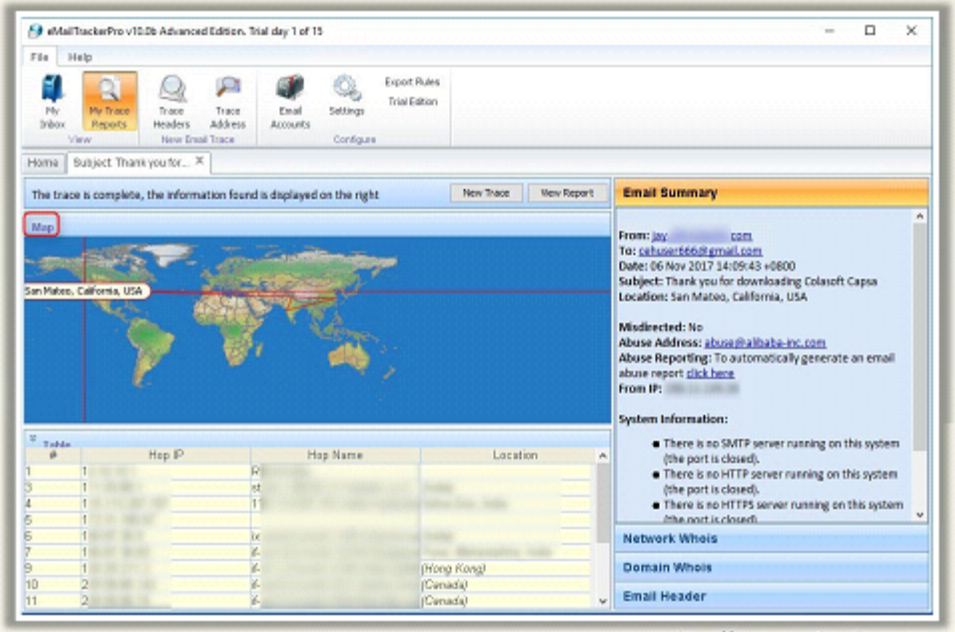


# Email Tracking Tools

- Email tracking tools allow an attacker to **track an email and extract information** such as sender identity, mail server, sender's IP address, location, etc.
- eMailTrackerPro analyzes email headers and reveals information such as **sender's geographical location**, IP address, etc.

## Email Tracking Tools

- PoliteMail (*http://www.politemail.com*)
- Yesware (*http://www.yesware.com*)
- ContactMonkey (*https://www.contactmonkey.com*)
- Zendio (*http://www.zendio.com*)
- ReadNotify (*http://www.readnotify.com*)
- DidTheyReadIt (*http://www.didtheyreadit.com*)
- Trace Email (*http://whatismyipaddress.com*)




http://www.emailtrackerpro.com

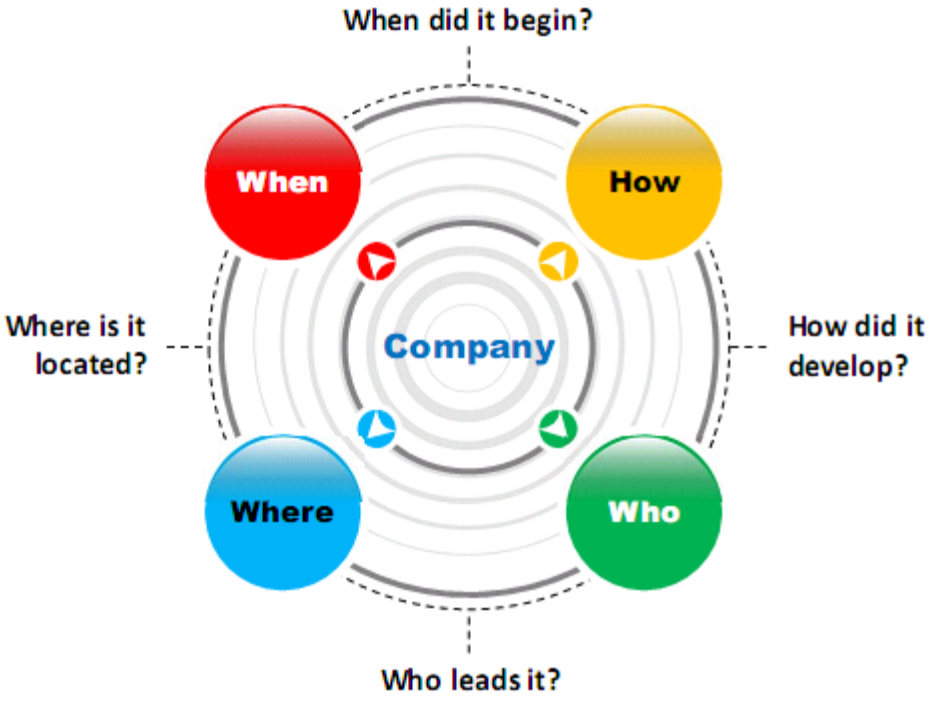
# Competitive Intelligence Gathering

- 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 is non-interfering and subtle in nature

## Sources of Competitive Intelligence

| | | | |
|---|---|---|---|
| 01 | Company websites and employment ads | Social engineering employees | 06 |
| 02 | Search engines, Internet, and online DB | Product catalogues and retail outlets | 07 |
| 03 | Press releases and annual reports | Analyst and regulatory reports | 08 |
| 04 | Trade journals, conferences, and newspapers | Customer and vendor interviews | 09 |
| 05 | Patent and trademarks | Agents, distributors, and suppliers | 10 |

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




## Visit These Sites

01. EDGAR Database
https://www.sec.gov/edgar.shtml

02. Hoovers
http://www.hoovers.com/about-us.html

03. LexisNexis
https://www.lexisnexis.com

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

# Competitive Intelligence - What Are the Company's Plans?

1. MarketWatch (*https://www.marketwatch.com*)
2. The Wall Street Transcript (*https://www.twst.com*)
3. Alexa (*https://www.alexa.com*)
4. Euromonitor (*http://www.euromonitor.com*)
5. Experian (*http://www.experian.com*)
6. SEC Info (*http://www.secinfo.com*)
7. The Search Monitor (*https://www.thesearchmonitor.com*)

# Competitive Intelligence - What Expert Opinions Say About the Company



**ABI/INFORM Global**

http://www.proquest.com

ProQuest

**SimilarWeb**

https://www.similarweb.com

SimilarWeb

**AttentionMeter**

http://www.attentionmeter.com

AttentionMeter

**Copernic Tracker**

http://www.copernic.com

copernic

**SEMRush**

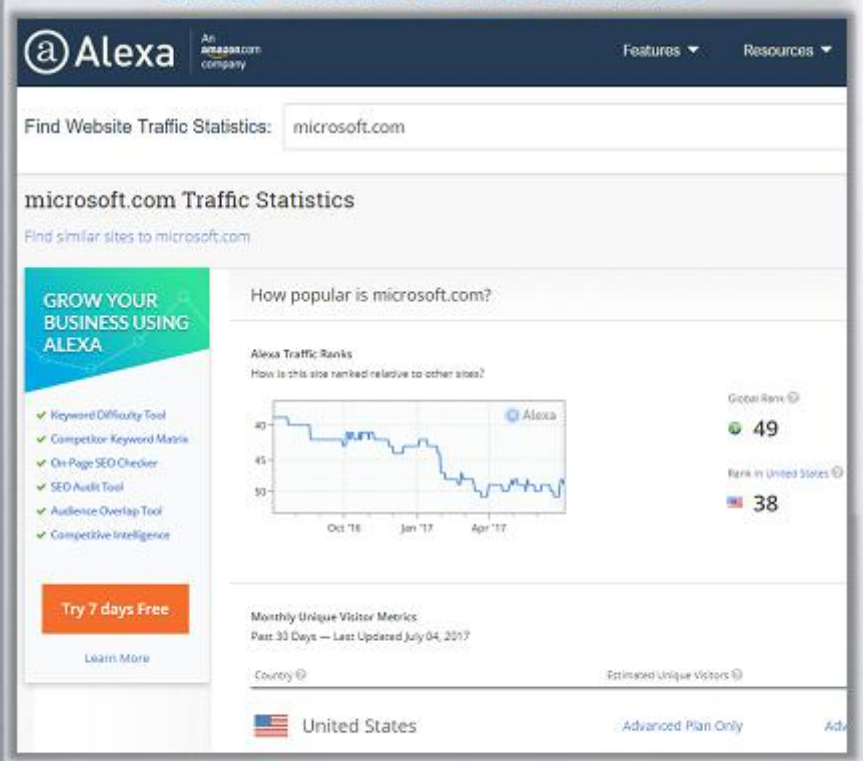
https://www.semrush.com

semrush
competitors research

# Monitoring Website Traffic of Target Company

- Attacker uses website traffic monitoring tools such as **Web-Stat**, **Alexa**, **Monitis**, etc. to collect the information about target company
  - Total visitors
  - Page views
  - Bounce rate
  - Live visitors map
  - Site ranking
  - Audience geography
- Traffic monitoring helps to collect information about the **target's customer base**, which help the attackers to disguise as a customer and launch social engineering attacks on the target

## Alexa Website Traffic Statistics

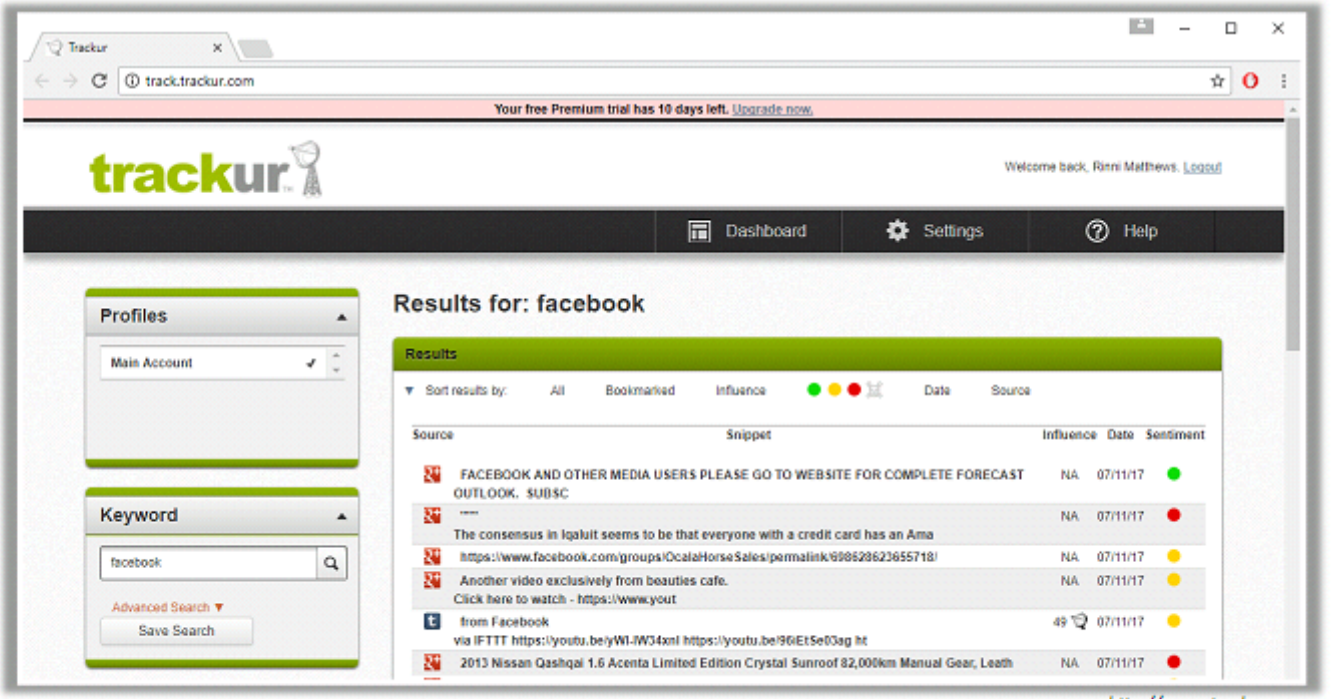



https://www.alexa.com

# Tracking Online Reputation of the Target

- Online Reputation Management (ORM) is a process of **monitoring a company's reputation on Internet** and taking certain measures to minimize the negative search results/reviews and thereby improve its brand reputation

- An attacker makes use of ORM tracking tools to:
  - Track **company's online reputation**
  - Collect company's **search engine ranking** information
  - Obtain **email notifications** when a company is mentioned online
  - Track **conversations**
  - Obtain **social news** about the target organization




http://www.trackur.com

# Whois Lookup

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

### Whois query returns:

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

### Information obtained from Whois database assists an attacker to:

- Gather personal information that assists in performing social engineering
- Create a map of the target organization's network
- Obtain internal details of the target network

### Regional Internet Registries (RIRs)

ARIN
AFRINIC
RIPE NCC
lacnic
APNIC

# Whois Lookup Result Analysis

## Whois Record for CertifiedHacker.com

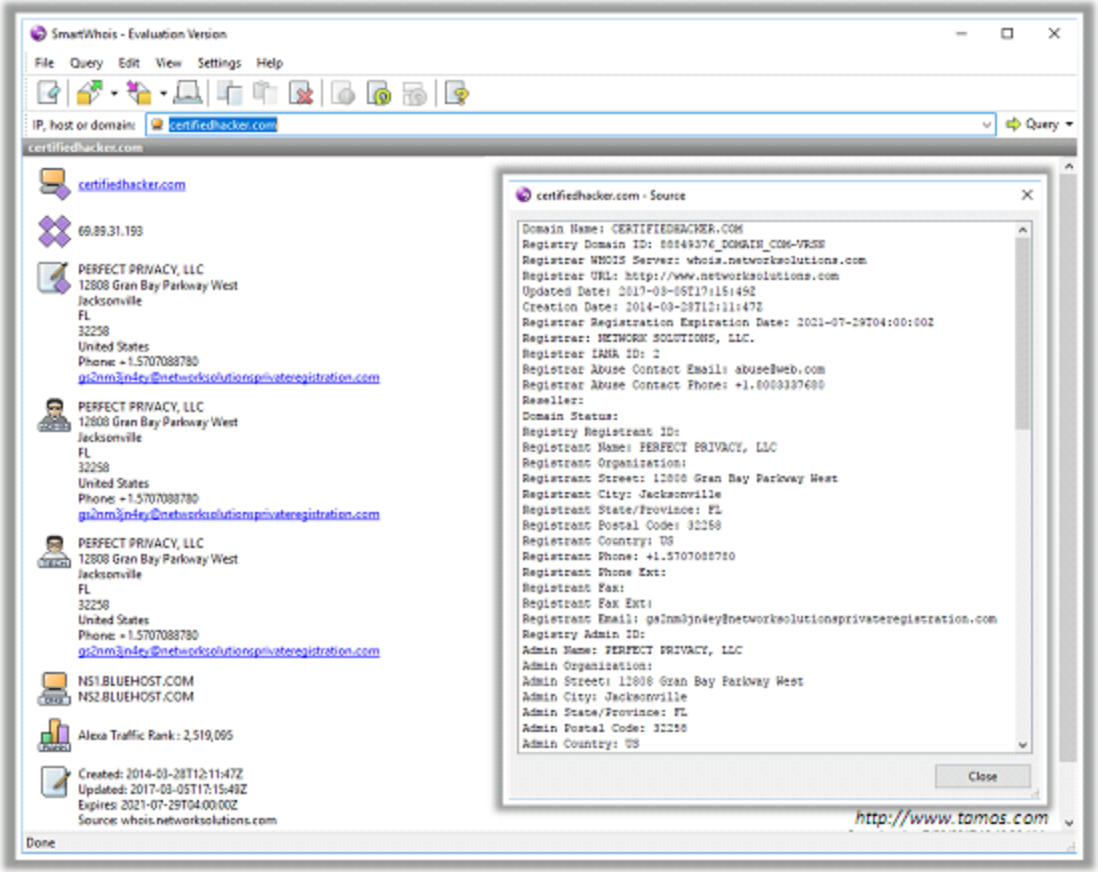
**Whois & Quick Stats**

| | |
|---|---|
| Email | abuse@web.com is associated with ~9,108,273 domains<br>gs2nm3j...@networksolutionsprivateregistration.com |
| Registrant Org | PERFECT PRIVACY, LLC was found in ~3,700,434 other domains |
| Registrar | NETWORK SOLUTIONS, LLC. |
| Registrar Status | clientTransferProhibited |
| Dates | Created on 2002-07-30 - Expires on 2021-07-30 - Updated on 2016-03-16 |
| Name Server(s) | NS1.BLUEHOST.COM (has 2,341,313 domains)<br>NS2.BLUEHOST.COM (has 2,341,313 domains) |
| IP Address | 69.89.31.193 - 1,316 other sites hosted on this server |
| IP Location | - Utah - Provo - Unified Layer |
| ASN | AS46606 UNIFIEDLAYER-AS-1 - Unified Layer, US (registered Oct 24, 2008) |
| Domain Status | Registered And Active Website |
| Whois History | 901 records have been archived since 2003-03-01 |
| IP History | 12 changes on 7 unique IP addresses over 11 years |
| Registrar History | 2 registrars with 1 drop |
| Hosting History | 6 changes on 4 unique name servers over 14 years |
| Whois Server | whois.networksolutions.com |

**Website**

| | |
|---|---|
| Website Title | // Certfied Hacker |
| Server Type | nginx/1.12.0 |
| Response Code | 200 |
| SEO Score | 98% |
| Terms | 36 (Unique: 28, Linked: 7) |

http://whois.domaintools.com




http://www.tamos.com

# Whois Lookup Tools



**Batch IP Converter**
*http://www.sabsoft.com*

**WhoIs Analyzer Pro**
*http://www.whoisanalyzer.com*

**Active Whois**
*http://www.johnru.com*

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

**Whois**
*https://docs.microsoft.com*

**WhoIs Lookup Multiple Addresses Software**
*https://www.sobolsoft.com*

**Whois Lookup**
*https://pentest-tools.com*

**ICANN WHOIS**
*https://whois.icann.org*

**IANA WHOIS**
*https://www.iana.org*

**WHOIS Lookup**
*https://www.whois.com*

**DNS Tools**
*https://www.dnssniffer.com*

**UltraTools Mobile**
*https://www.ultratools.com*

**Whois®**
*https://www.whois.com.au*

**Deep Whois**
*http://happymagenta.com/deepwhois*

**Whois Lookup Tool**
*https://www.znetlive.com*

# Finding IP Geolocation Information

- IP geolocation helps to identify information such as **country**, region/state, city, ZIP/postal code, time zone, **connection speed**, **ISP (hosting company)**, domain name, IDD country code, area code, mobile carrier, elevation, etc.
- **IP geolocation lookup tools** such as **IP2Location** helps to collect IP geolocation information about the target that helps the attackers to **launch social engineering attacks** such as spamming and phishing

## IP Geolocation Lookup Tools

- IP Location Finder (https://tools.keycdn.com)
- IP Address Geographical Location Finder (http://www.ipfingerprints.com)
- IP Location (https://www.iplocation.net)
- GeoIP Lookup Tool (https://www.ultratools.com)
- Geo IP Tool (https://geoiptool.com)

## IP2Location

| | |
|---|---|
| IP Address | 207.46.232.182 |
| Location | Singapore, Singapore, Singapore |
| Latitude & Longitude of City | 1.289670, 103.850070 (1°17'23"N 103°51'0"E) |
| ISP | Microsoft Corporation |
| Local Time | 20 Sep, 2017 05:11 PM (UTC +08:00) |
| Domain | microsoft.com |
| Net Speed | (COMP) Company/T1 |
| IDD & Area Code | (65) 06 |
| ZIP Code | 179431 |
| Weather Station | Singapore (SNXX0006) |
| Mobile Country Code (MCC) | - |
| Mobile Network Code (MNC) | - |
| Carrier Name | - |
| Elevation | 20m |
| Usage Type | (DCH) Data Center/Web Hosting/Transit |
| Anonymous Proxy | No |
| Proxy Type | (DCH) Hosting Provider, Data Center or CDN Range |

*http://www.ip2location.com*

# Extracting DNS Information

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

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

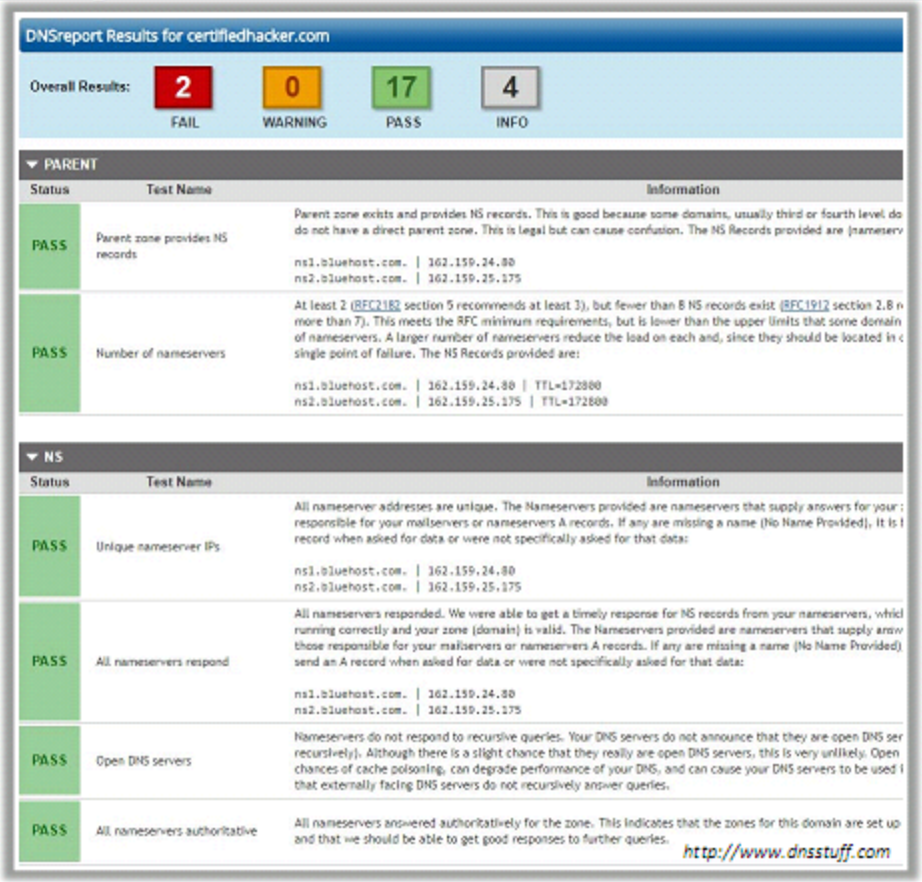
DNS records provide important information about the location and types of servers

**DNS Interrogation Tools**

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

# DNS Interrogation Tools

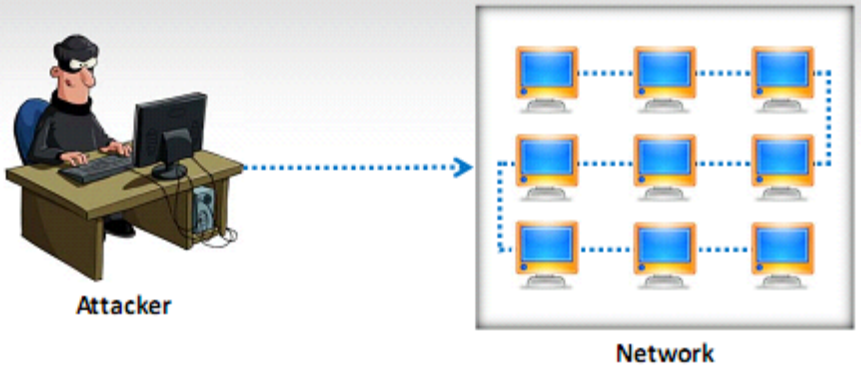
**Professional Toolset**




- **DIG**
  *http://www.kloth.net*
- **myDNSTools**
  *http://www.mydnstools.info*
- **Domain Dossier**
  *https://centralops.net*
- **DNSDataView**
  *http://www.nirsoft.net*
- **DNSWatch**
  *https://www.dnswatch.info*

# Locate the Network Range

- Network range information assists attackers in creating a **map of the target network**
- Find the **range of IP addresses** using **ARIN whois database search** tool
- You can find the range of IP addresses and the subnet mask used by the target organization from **Regional Internet Registry (RIR)**




**Network Whois Record**

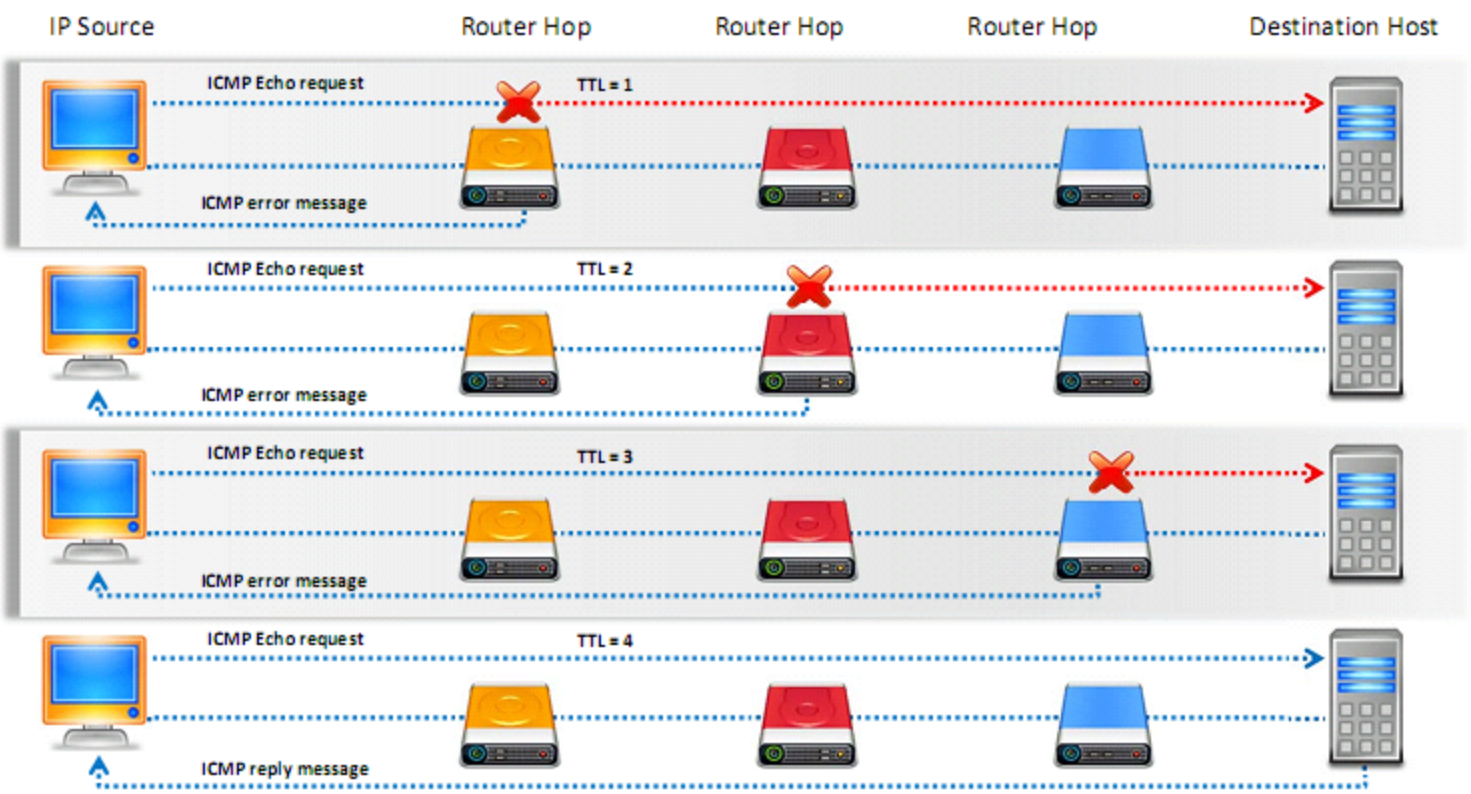
**Queried whois.arin.net with "207.46.232.182"**

| Network | |
|---|---|
| Net Range | 207.46.0.0 - 207.46.255.255 |
| CIDR | 207.46.0.0/16 |
| Name | MICROSOFT-GLOBAL-NET |
| Handle | NET-207-46-0-0-1 |
| Parent | NET207 (NET-207-0-0-0-0) |
| Net Type | Direct Assignment |
| Origin AS | |
| Organization | Microsoft Corporation (MSFT) |
| Registration Date | 1997-03-31 |
| Last Updated | 2013-08-20 |
| Comments | |
| RESTful Link | https://whois.arin.net/rest/net/NET-207-46-0-0-1 |
| See Also | Related organization's POC records. |
| See Also | Related delegations. |

| Organization | |
|---|---|
| Name | Microsoft Corporation |
| Handle | MSFT |
| Street | One Microsoft Way |
| City | Redmond |
| State/Province | WA |
| Postal Code | 98052 |
| Country | US |
| Registration Data | 1998-07-09 |
| Last Updated | 2017-01-28 |
| Comments | To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to:<br>* https://cert.microsoft.com.<br><br>For SPAM and other abuse issues, such as Microsoft Accounts, please contact:<br>* abuse@microsoft.com. |

# Traceroute

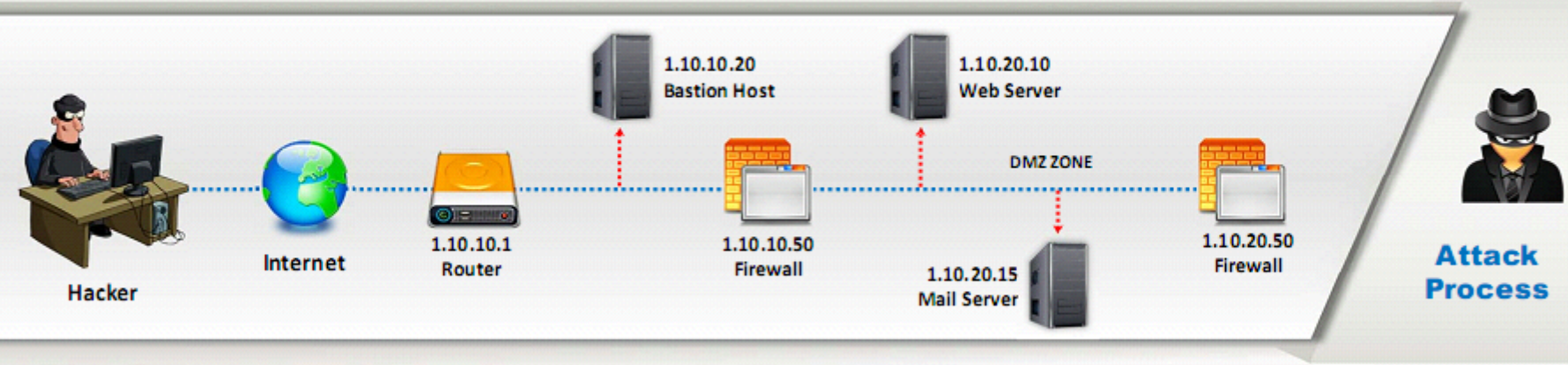
Traceroute programs work on the concept of **ICMP protocol** and **use the TTL field in the header of ICMP packets** to discover the routers on the path to a target host



# Traceroute Analysis

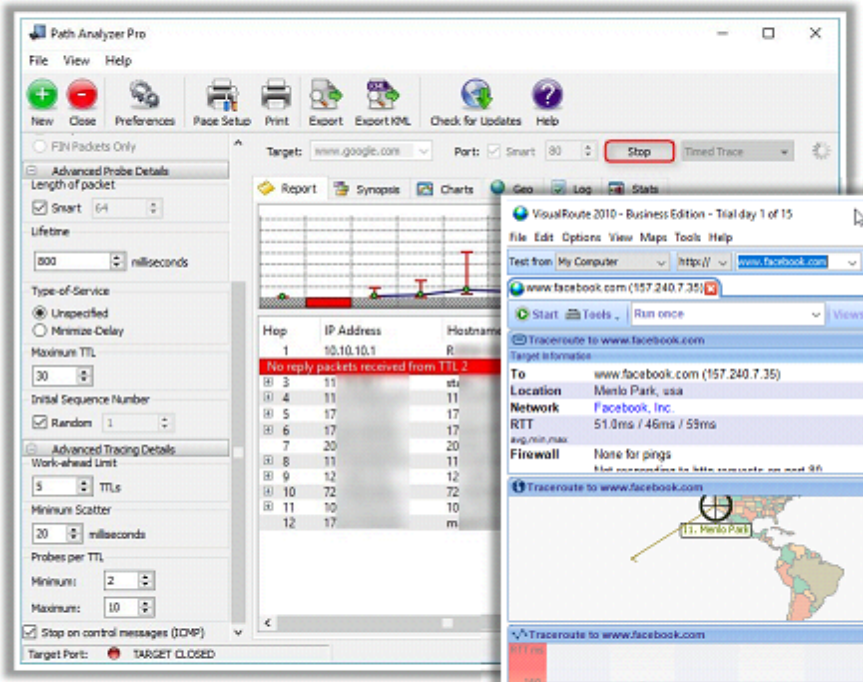


- Attackers conduct traceroute to extract information about network topology, trusted routers, and firewall locations
  - For example: after running several traceroutes, an attacker might obtain the following information:
    - traceroute 1.10.10.20, second to last hop is 1.10.10.1
    - traceroute 1.10.20.10, third to last hop is 1.10.10.1
    - traceroute 1.10.20.10, second to last hop is 1.10.10.50
    - traceroute 1.10.20.15, third to last hop is 1.10.10.1
    - traceroute 1.10.20.15, second to last hop is 1.10.10.50
  - By putting this information together, attackers can draw the network diagram



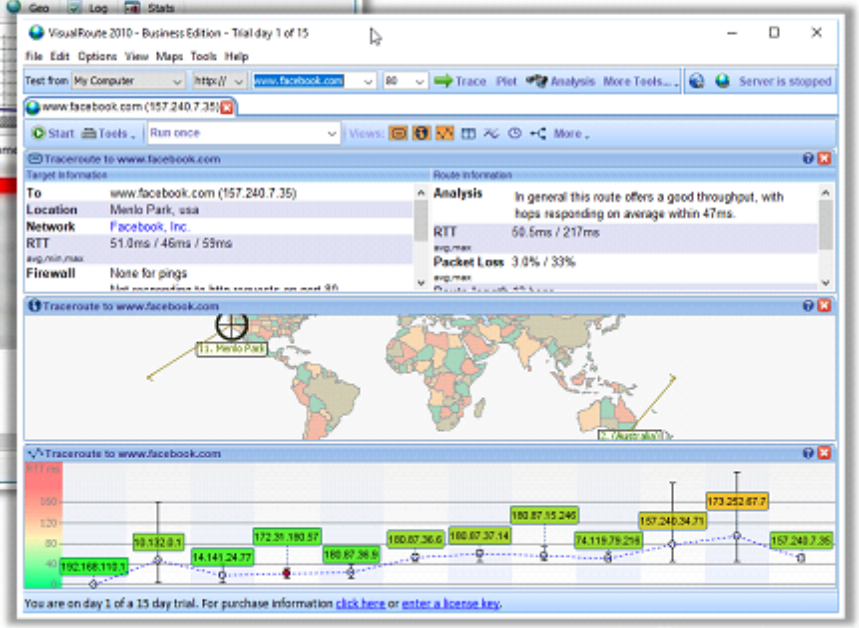
# Traceroute Tools

## Path Analyzer Pro




http://www.pathanalyzer.com

## VisualRoute




http://www.visualroute.com

- **GEO Spider** — http://www.oreware.com
- **Trout** — https://www.mcafee.com
- **Magic NetTrace** — http://www.tialsoft.com
- **Ping Plotter** — http://www.pingplotter.com
- **Traceroute Tool** — https://tools.keycdn.com

# Footprinting through Social Engineering

- Social engineering is an art of exploiting human behaviour to **extract confidential information**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it

## Social engineers attempt to gather:

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

## Some of the Social engineering techniques:

- Eavesdropping
- Shoulder surfing
- Dumpster diving
- Impersonation

# Collecting Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving



## Eavesdropping

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

## Shoulder Surfing

- Shoulder surfing is a technique, where **attackers secretly observe the target** to gain critical information
- Attackers gather information such as **passwords**, **personal identification number**, account numbers, credit card information, etc.

## Dumpster Diving

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

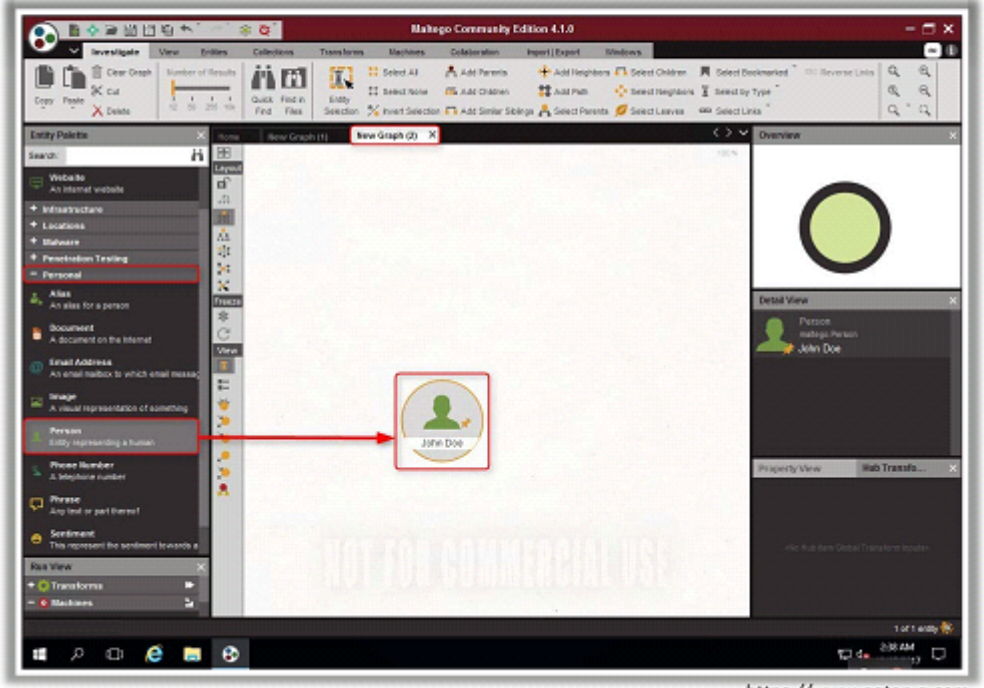
# Module Flow

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures
5. Footprinting Penetration Testing

# Footprinting Tools: Maltego and Recon-ng

**Maltego**

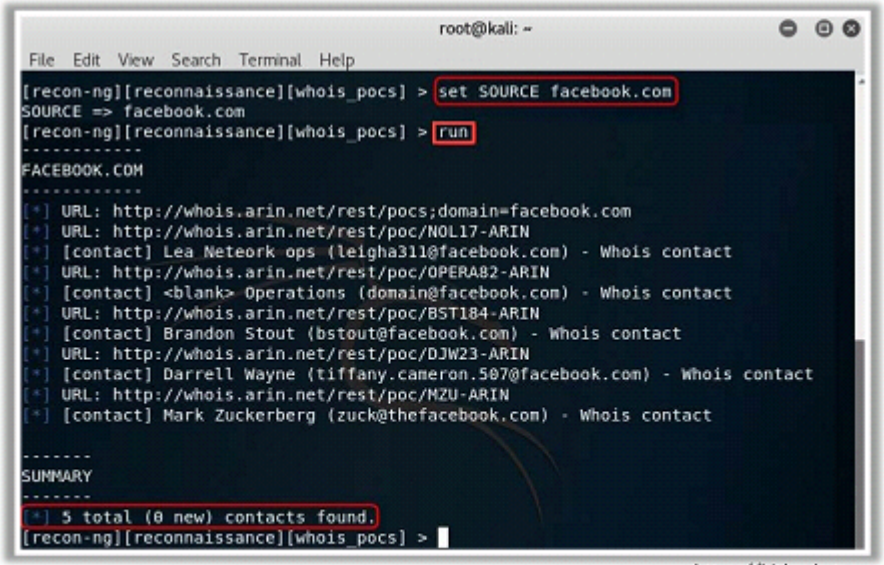
Maltego is a program that can be used to determine the relationships and real world links between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files




https://www.paterva.com

**Recon-ng**

Recon-ng is a Web Reconnaissance framework with independent modules, database interaction, built in convenience functions, interactive help, and command completion, that provides an environment in which open source web-based reconnaissance can be conducted

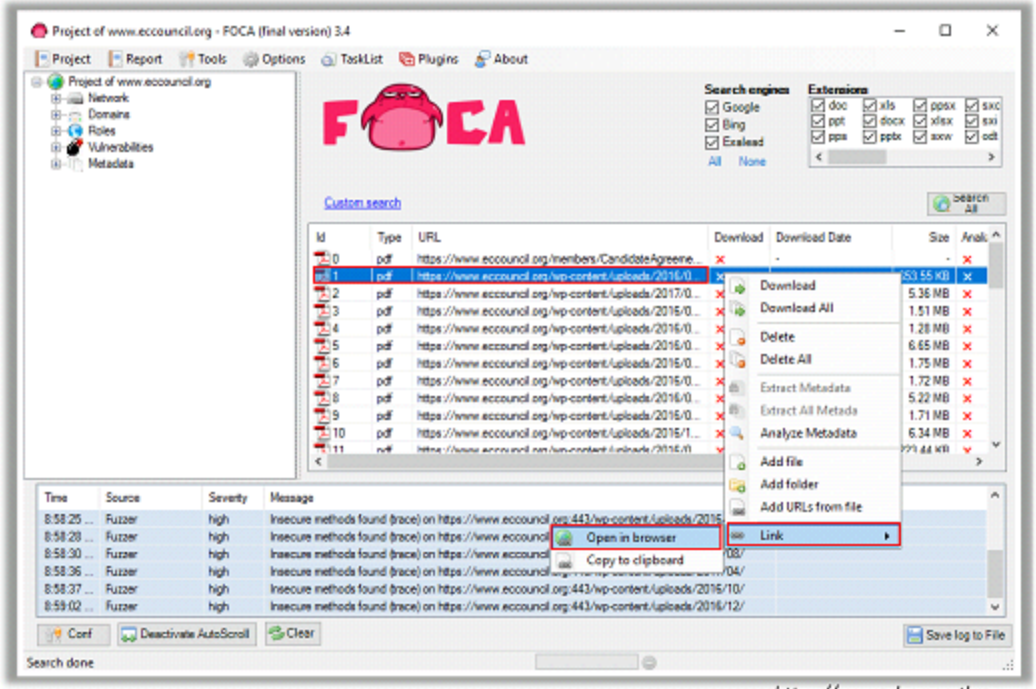



https://bitbucket.org

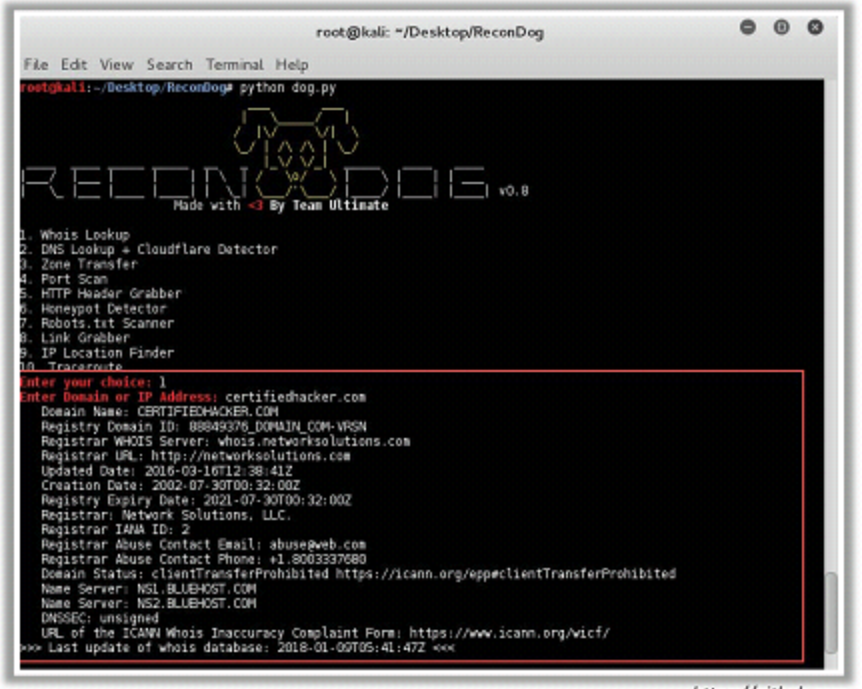
# Footprinting Tools: FOCA and Recon-Dog

- **FOCA (Fingerprinting Organizations with Collected Archives)** is a tool used mainly to find metadata and hidden information in the documents its scans

- **Recon Dog** is an all-in-one tool for all basic information gathering needs. It uses APIs to gather all the information so your identity is not exposed




https://www.elevenpaths.com



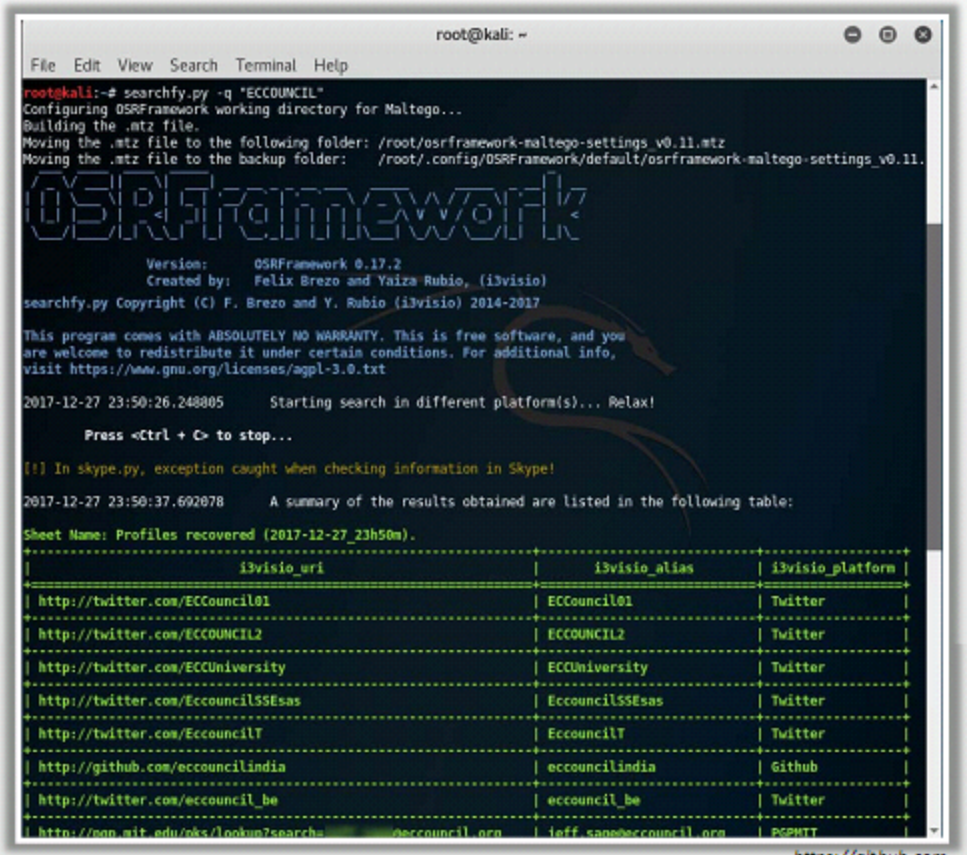

https://github.com

# Footprinting Tools: OSRFramework

- OSRFramework is a set of libraries developed by i3visio to **perform Open Source Intelligence tasks**
- It is a bunch of different applications related to **username checking**, **DNS lookups**, information leaks research, **deep web search**, regular expressions extraction, and many others

## Tools included in the OSRFramework package

- **usufy.py** – Checks for a user profile in up to 290 different platforms
- **mailfy.py** – Check for the existence of a given mail
- **searchfy.py** – Performs a query on the platforms in OSRFramework
- **domainfy.py** – Checks for the existence of domains
- **phonefy.py** – Checks for the existence of a given series of phones




https://github.com

# Additional Footprinting Tools



**Prefix Whois**
*http://pwhois.org*

**LHF (Low Hanging Fruit)**
*https://github.com*

**Sni1per**
*https://github.com*

**CloudFail**
*https://github.com*

**Aquatone**
*https://github.com*

**GMapCatcher**
*https://github.com*

**DNS-Digger**
*http://www.dnsdigger.com*

**Reconnoitre**
*https://github.com*

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

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

**Robtex**
*https://www.robtex.com*

**SearchBug**
*https://www.searchbug.com*

**Zaba Search**
*http://www.zabasearch.com*

**Metasploit**
*https://www.metasploit.com*

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

# Module Flow

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures
5. Footprinting Penetration Testing

# Footprinting Countermeasures




Restrict the employees to access social networking sites from organization's network


Configure web servers to avoid information leakage


Educate employees to use pseudonyms on blogs, groups, and forums


Do not reveal critical information in press releases, annual reports, product catalogues, etc.


Limit the amount of information that you are publishing on the website/ Internet


Use footprinting techniques to discover and remove any sensitive information publicly available


Prevent search engines from caching a web page and use anonymous registration services

# Footprinting Countermeasures (Cont'd)



**Develop and enforce security policies** to regulate the information that employees can reveal to third parties

Set apart internal and external DNS or use split DNS, and **restrict zone transfer** to authorized servers

**Disable directory listings** in the web servers

Conduct periodically security awareness training to educate employees about various **social engineering tricks and risks**

Opt for privacy services on **Whois Lookup database**

**Avoid domain-level cross-linking** for the critical assets

**Encrypt** and **password protect** sensitive information

# Module Flow

1. Footprinting Concepts
2. Footprinting Methodology
3. Footprinting Tools
4. Footprinting Countermeasures
5. Footprinting Penetration Testing

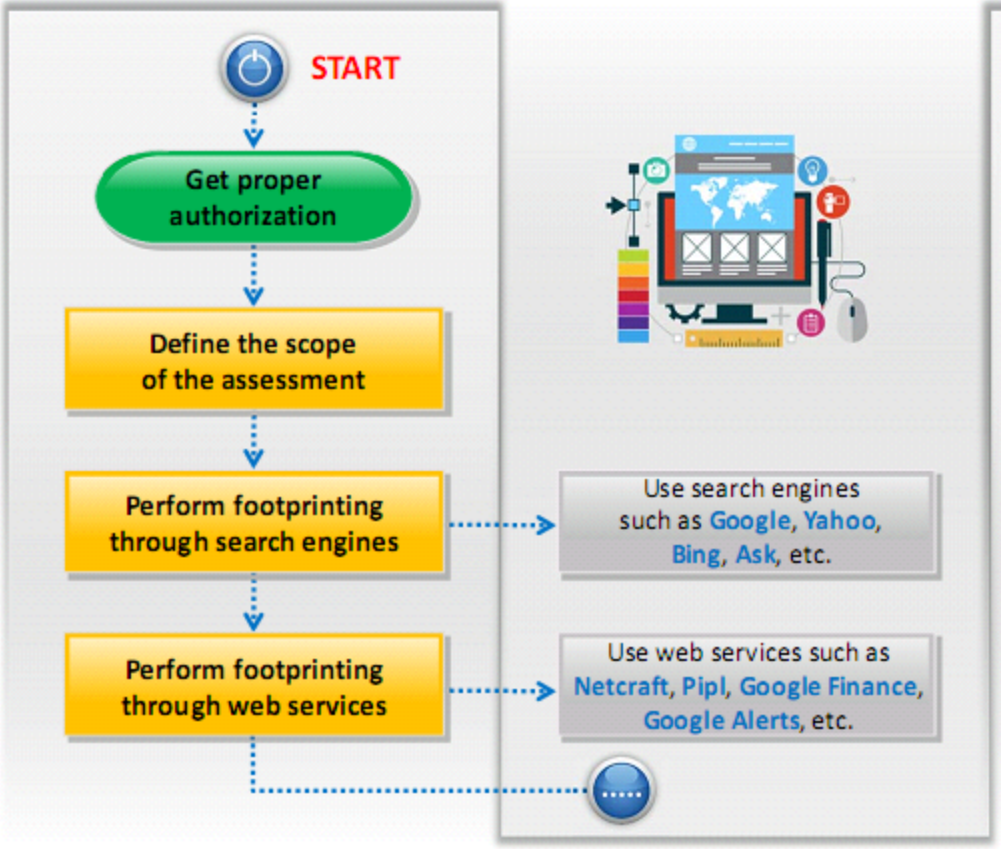
# Footprinting Pen Testing

- Footprinting pen testing is used to **determine an organization's information**
- The tester attempts to gather as much information as possible about the target organization from the **Internet and other publicly accessible sources**

**Footprinting pen testing helps organization to:**

- Prevent information leakage
- Prevent social engineering attempts
- Prevent DNS record retrieval from publically available servers

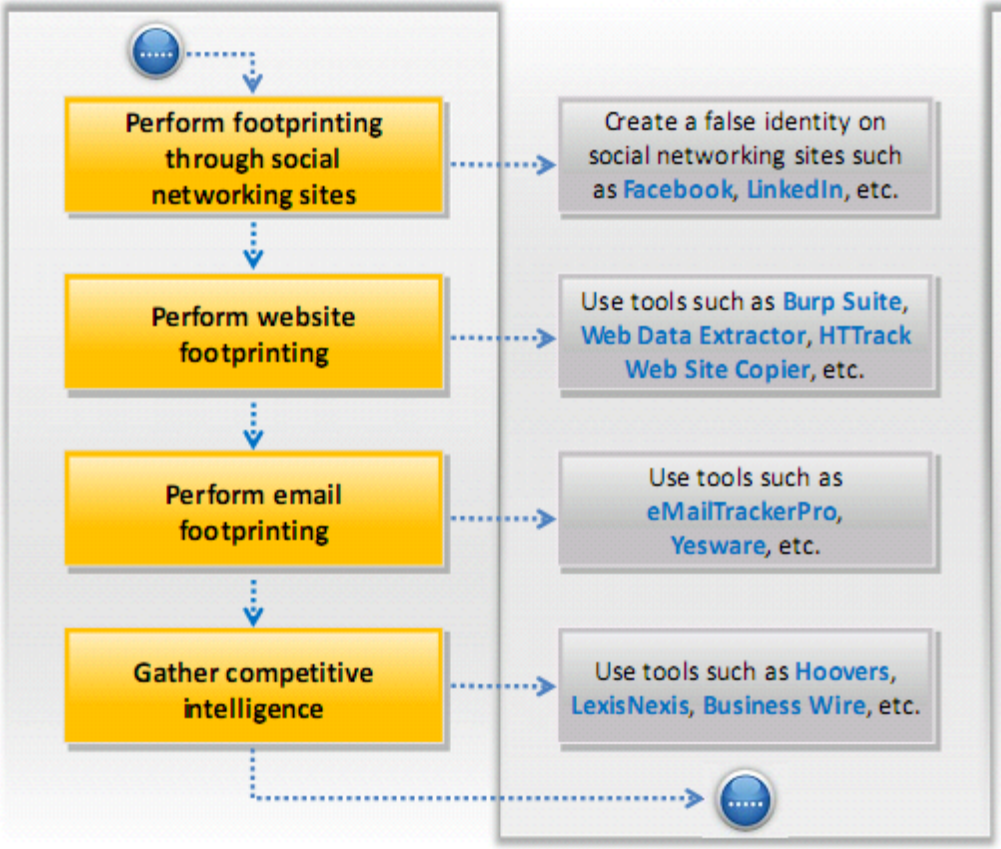
# Footprinting Pen Testing (Cont'd)





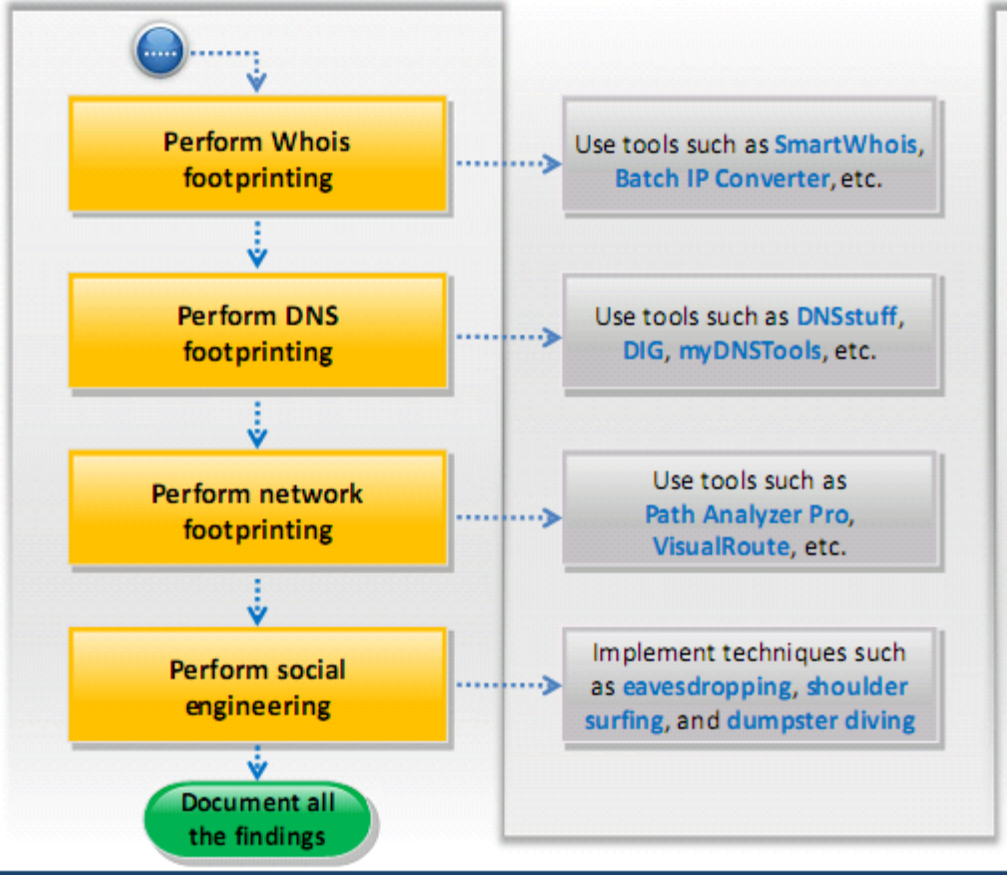

- Get proper authorization and define the scope of the assessment
- Footprint search engines such as **Google**, **Yahoo**, **Ask**, **Bing**, **Aol**, etc. to gather target organization's information such as employee details, login pages, intranet portals, operating systems used, financial information, etc. that helps in performing social engineering and other types of advanced system attacks
- Perform Google hacking using tools such as **Google Hacking Database (GHDB)**, etc.
- Perform footprinting through web services such as **Netcraft**, **Pipl**, **Google Finance**, **Google Alerts**, etc. to gather information about target organization's website, employees, competitor, infrastructure, operating systems, etc.

# Footprinting Pen Testing (Cont'd)




- Gather target organization employees information from their personal profiles on social networking sites such as **Facebook**, **MySpace**, **LinkedIn**, **Twitter**, **Google+**, **Pinterest**, etc. that assist in performing social engineering
- Perform website footprinting using tools such as **Burp Suite**, **Web Data Extractor**, **HTTrack Web Site Copier**, **Metagoofil**, **WebSite-Watcher**, etc. to build a detailed map of website's structure and architecture
- Perform email footprinting using tools such as **eMailTrackerPro**, **Yesware**, **ContactMonkey**, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping the target organization's network
- Gather competitive intelligence using tools such as **Hoovers**, **LexisNexis**, **Business Wire**, etc.

# Footprinting Pen Testing (Cont'd)




- Perform Whois footprinting using tools such as **Whois Lookup**, **SmartWhois**, **Batch IP Converter**, etc. to create a detailed map of organizational network, gather personal information that assists in performing social engineering, and gather other internal network details, etc.
- Perform DNS footprinting using tools such as **DNSstuff**, **DIG**, **myDNSTools**, etc. to determine key hosts in the network and perform social engineering attacks
- Perform network footprinting using tools such as **Path Analyzer Pro**, **VisualRoute**, **GEO Spider**, etc. to create a map of the target's network
- Implement social engineering techniques such as **eavesdropping**, **shoulder surfing**, **dumpster diving**, and **phishing** that may help to gather more critical information about the target organization
- At the end of pen testing, **document all the findings**

# Footprinting Pen Testing Report Templates

## Pen Testing Report

### Information obtained through search engines

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

### Information obtained through Google Hacking Database (GHDB)

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

### Information obtained through web services

- Sub-domains:
- Physical location:
- Email ID:
- Photos:
- Others:

### Information obtained through social networking sites

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

### Information obtained through website footprinting

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

### Information obtained through email footprinting

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

# Footprinting Pen Testing Report Templates (Cont'd)

## Pen Testing Report

### Information obtained through competitive intelligence

- Financial details:
- Project plans:
- Others:

### Information obtained through WHOIS footprinting

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

### Information obtained through DNS footprinting

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

### Information obtained through network footprinting

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

### Information obtained through social engineering

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

# Module Summary

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