



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

Gathering information about a target **without direct interaction**

### Active Footprinting

Gathering information about the target **with direct interaction**

## Information Obtained in Footprinting

### Organization Information

Employee details, telephone numbers, location, background of the organization, web technologies, etc.

### Network Information

Domain and sub-domains, network blocks, IP addresses of the reachable systems, Whois record, DNS, etc.

### System Information

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:

  
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.

The screenshot shows the Google Advanced Search interface at [https://www.google.com/advanced\\_search](https://www.google.com/advanced_search). The page title is "Advanced Search". It contains several input fields for specifying search criteria:

- Find pages with...
  - all these words: [text input]
  - this exact word or phrase: [text input]
  - any of these words: [text input]
  - none of these words: [text input]
  - numbers ranging from: [text input] to [text input]
- Then narrow your results by...
  - language: [dropdown: any language]
  - region: [dropdown: any region]
  - last update: [dropdown: anytime]
  - site or domain: [text input]
  - terms appearing: [dropdown: anywhere in the page]
  - SafeSearch: [dropdown: Show most relevant results]
  - file type: [dropdown: any format]
  - usage rights: [dropdown: not filtered by license]

At the bottom right is a blue "Advanced Search" button.

[https://www.google.com/advanced\\_search](https://www.google.com/advanced_search)

The screenshot shows the Google Advanced Image Search interface at [https://www.google.com/advanced\\_image\\_search](https://www.google.com/advanced_image_search). The page title is "Advanced Image Search". It contains several input fields for specifying image search criteria:

- Find Images with...
  - all these words: [text input]
  - this exact word or phrase: [text input]
  - any of these words: [text input]
  - none of these words: [text input]
- Then narrow your results by...
  - image size: [dropdown: any size]
  - aspect ratio: [dropdown: any aspect ratio]
  - colours in the image:
    - any colour
    - full colour
    - black & white
    - transparent
    - this colour
  - type of image: [dropdown: any type]
  - region: [dropdown: any region]
  - site or domain: [text input]
  - SafeSearch: [dropdown: Show most relevant results]
  - file type: [dropdown: any format]
  - usage rights: [dropdown: not filtered by license]

At the bottom right is a blue "Advanced Search" button.

[https://www.google.com/advanced\\_image\\_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



**EXPLOIT DATABASE**

Home    Exploits    Shellcode    Papers    Google Hacking Database    Submit    Search

Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

Any Category

Date	Title	Category
2017-07-17	Index of /htdocs	Sensitive Directories
2017-07-17	"You're successfully running JSON Server"	Files Containing Juicy Info
2017-07-14	Inurl:"ADVANCED COMMON TOP"	Various Online Devices
2017-07-14	Intitle:"Namenode information"	Various Online Devices
2017-07-14	Inurl:"wp/recuperadocumentosql.aspx"	Various Online Devices
2017-07-14	Inurl:login.cgi intitle:.NETGEAR	Various Online Devices
2017-07-07	filetype:ini "wordfence"	Advisories and Vulnerabilities
2017-06-27	"Sorting Logs;" "Please enter your password;" "Powered By" -uriscan -alamy	Footholds
2017-06-27	Intitle:"Index of" "Apache/2.4.7 (Ubuntu) Server"	Web Server Detection
2017-06-26	Intitle:"Index of /" "joomla_update.php"	Sensitive Directories

<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

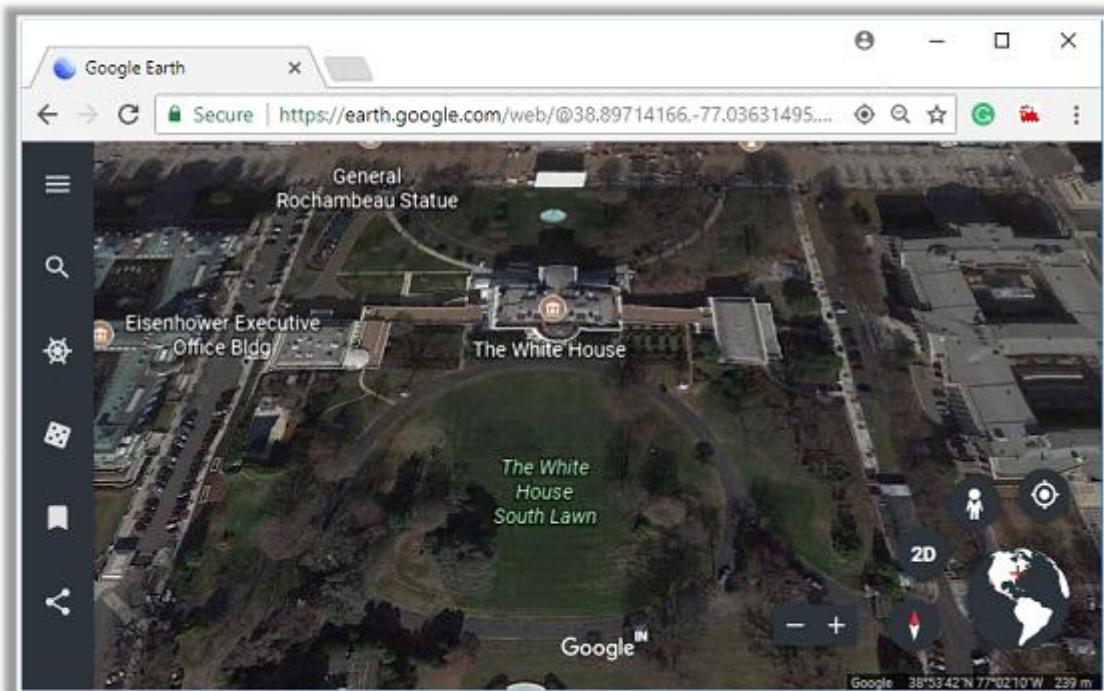
Site	Site Report	First seen
61. licensing.microsoft.com		june 2002
62. shopformusic.microsoft.com		may 2006
63. info.microsoft.com		june 2015
64. fail.music.metaservices.microsoft.com		february 2008
65. visualstudiodownload.microsoft.com		july 2009
66. partners.microsoft.com		november 2004
67. scan-microsoft.com.scan-viruse.website		march 2017
68. note0.microsoft.com		april 2016
69. download-support.webapps.microsoft.com		february 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.microsoft.com		december 2012

<https://www.netcraft.com>

```
root@kali:~# sublist3r -d google.com -p 80 -e Bing
# Coded By Ahmed Aboul-Ela - @abou3la
[-] Enumerating subdomains now for google.com
[-] Searching now in Bing..
[-] Total Unique Subdomains Found: 53
[-] Start port scan now for the following ports: 80
aboutme.google.com - Found open ports: 80
adssettings.google.com - Found open ports: 80
attribution.google.com - Found open ports: 80
baseline.google.com - Found open ports: 80
bookmarks.google.com - Found open ports: 80
audiencecenter.google.com - Found open ports: 80
console.cloud.google.com - Found open ports: 80
cast.google.com - Found open ports: 80
crowdsource.google.com - Found open ports: 80
contacts.google.com - Found open ports: 80
accounts.google.com - Found open ports: 80
analytics.google.com - Found open ports: 80
developers.google.com - Found open ports: 80
code.google.com - Found open ports: 80
adwords.google.com - Found open ports: 80
docs.google.com - Found open ports: 80
desktop.google.com - Found open ports: 80
drive.google.com - Found open ports: 80
earth.google.com - Found open ports: 80
signup.earthengine.google.com - Found open ports: 80
encrypted.google.com - Found open ports: 80
fonts.google.com - Found open ports: 80
express.google.com - Found open ports: 80
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**

The screenshot shows the pipl.com search interface. A search bar at the top contains "Nicolas Cage" and "United States". Below it, a "Search By" section has "First" set to "Nicolas" and "Last" set to "Cage". There are "MORE OPTIONS" and a search button. Below these are filters for "All Locations" and "United States". The results section is titled "Results for Nicolas Cage, United States". It shows two entries: "Nicolas Coppola Cage" (53 years old from Los Angeles & Encino, California) and "Nicolas Prorok Cage" (53 years old from Los Angeles & Long Beach, California). Both entries include a photo, a "SPONSORED" note, and links to "Contact Details", "Social Profile", and "Username Report". At the bottom right is the URL <https://pipl.com>.



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

```
root@kali:~
```

```
File Edit View Search Terminal Help
root@kali:~# inspy --empspy /usr/share/inspy/wordlists/title-list-large.txt google
InSpy 2.0.3

2017-11-27 01:29:13 737 Employees identified
2017-11-27 01:29:13 Jessica Myers Human Resources Business Partner at Google
2017-11-27 01:29:13 Claudia Worms Sciama Sales Director at Google Brasil
2017-11-27 01:29:13 Alexandros Fragkos Analytical Consultant at Google
2017-11-27 01:29:13 Yigit Boyar Staff Software Engineer at Google
2017-11-27 01:29:13 Muneera Shaik HR coordinator at Google Hyderabad
2017-11-27 01:29:13 Sindhu Reddy HR Specialist Deputed - Google
2017-11-27 01:29:13 Shana Simmons Corporate Counsel at Google Inc.
2017-11-27 01:29:13 Eric Schmidt Executive Chairman at Google
2017-11-27 01:29:13 Steven L. Gates President at Google Advertising For Any Budget
2017-11-27 01:29:13 John Woolard Vice President at Google
2017-11-27 01:29:13 Annemieke Ehlhardt EHS Technician at Google
2017-11-27 01:29:13 Kevin Mangan EMEA Tax at Google
2017-11-27 01:29:13 Raheem Kareem Site Coordinator at Google
2017-11-27 01:29:13 Seth Williams Program Manager at Google
2017-11-27 01:29:13 Pooja Lalwani People Consultant at Google
2017-11-27 01:29:13 Lucas Dixon Chief Scientist, Jigsaw at Google
2017-11-27 01:29:13 Ashley Gardner Customer Service Supervisor at Google Fiber
2017-11-27 01:29:13 Felix Krause Fastlane iOS developer at Google
2017-11-27 01:29:13 Megan Stull Counsel at Google Inc.
2017-11-27 01:29:13 Addy Osmani Engineering Manager at Google
2017-11-27 01:29:13 Nikhil Khemani Account Manager at Google
2017-11-27 01:29:13 Shriram Raju Potturi Supply Chain Procurement Analyst at Google Express
2017-11-27 01:29:13 Ankit Sharma Security Engineer at Google
2017-11-27 01:29:13 shashank gupta Software Engineer at Google
2017-11-27 01:29:13 Jeffrey R. Shephard Security Manager at Google
2017-11-27 01:29:13 Sriram Karra Product Manager at Google
2017-11-27 01:29:13 Susan E. Morgan Finance at Google
2017-11-27 01:29:13 Benyu Zhang Staff Engineer at Google
2017-11-27 01:29:13 Doug Woodward APP, NCTMB Therapeutic Massage Therapist at Google Inc
2017-11-27 01:29:13 Javier Martin Regional Human Resources Director at Google
```

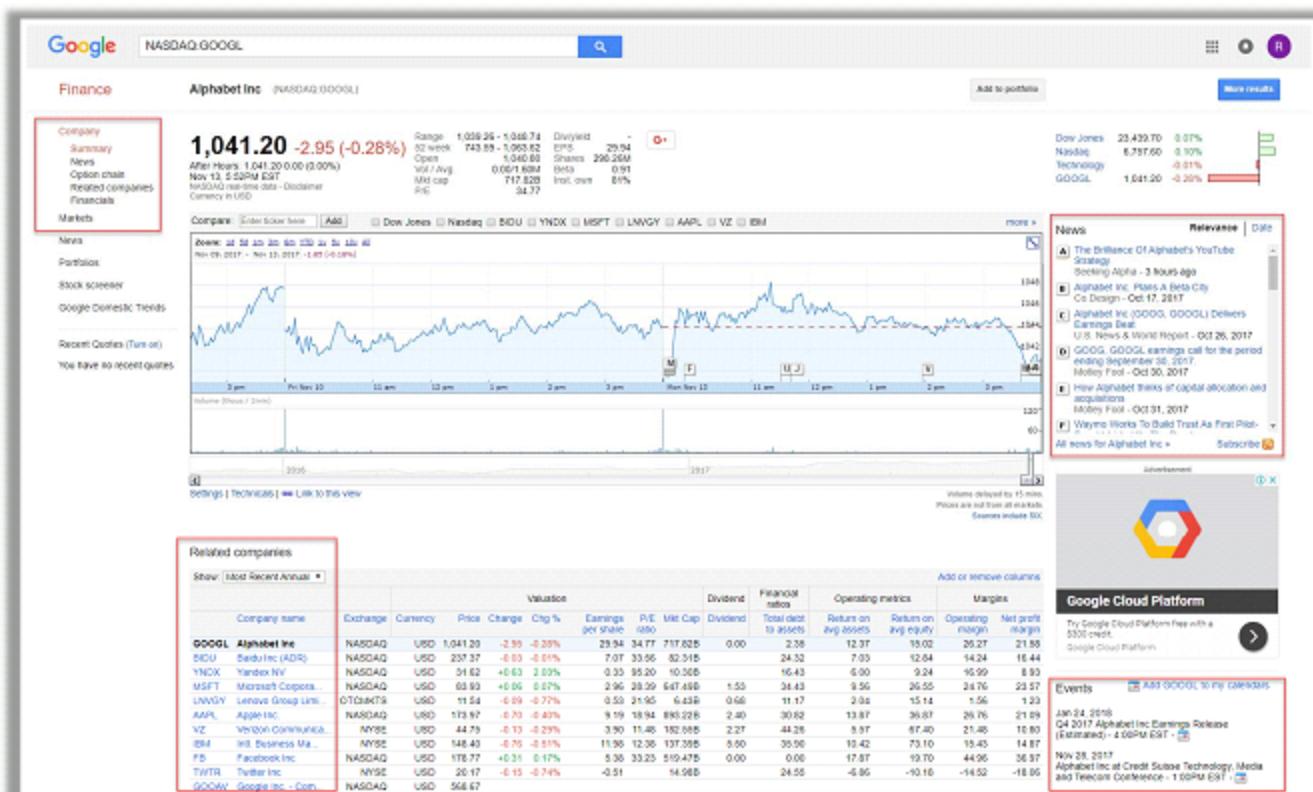
<https://github.com>

# 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)  
(<https://finance.yahoo.com>)
- [TheStreet](https://www.thestreet.com)  
(<https://www.thestreet.com>)
- [MarketWatch](https://www.marketwatch.com)  
(<https://www.marketwatch.com>)



# Footprinting through Job Sites

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

## Enterprise Applications Engineer/DBA

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

We extend this same level of service to our most important asset: our employees! We offer competitive salaries and benefits, but our strength is our family culture. We foster a safe 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:**  
 Ward & Brown Insurance Administrators Inc

**Location:**  
 Orange, CA 92888

**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:**  
 Ward & Brown Insurance Administrators Inc

**Reference Code:**  
 IT Operations

### Look for these:

- ➊ Job requirements
- ➋ Employee's profile
- ➌ Hardware information
- ➍ Software information

### Examples of Job Websites

- ➊ <https://www.indeed.com>
- ➋ <http://www.careerbuilder.com>
- ➌ <http://www.dice.com>
- ➍ <https://www.glassdoor.com>
- ➎ <https://www.linkedin.com>
- ➏ <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>)

The screenshot shows the Google Alerts interface. At the top, it says "Monitor the web for interesting new content". Below that, there's a search bar with "Q. microsoft.com". Underneath the search bar are several filter options: "How often" (set to "At most once a day"), "Sources" (set to "Automatic"), "Language" (set to "English"), "Region" (set to "Any Region"), "How many" (set to "Only the best results"), and "Deliver to" (set to "@ecouncil.org"). At the bottom of this section are two buttons: "Create Alert" and "Hide options". Below this form, the URL <https://www.google.com/alerts> is displayed.

**Alert preview**

**NEWS**

- Microsoft Teams in India, US Embedding AI into Tiny Devices  
India West  
SAN FRANCISCO — A team of 30 researchers at Microsoft labs in Redmond, Wash., and Bangalore are busy developing a new class of ...
- Microsoft Azure Has Another New Way to Compete With Amazon and Google - Fortune  
Microsoft finally releases its secret weapon in the cloud wars with Amazon and Google - Business Insider
- Microsoft's Azure Stack private cloud platform is ready for its first customers - TechCrunch

Full Coverage

- Waverton Investment Management LTD Has Upped Microsoft Com Us\$0.0000125 (MSFT)  
Position ...  
High Point Observer
- Waverton Investment Management Ltd increased Microsoft Corporation Com Us\$0.0000125 (MSFT) stake by 13.57% reported in 2016Q4 SEC filing.

Winfield Associates Upended Its Holding in Microsoft Com (MSFT) by \$327608 as Share Price Rose ...  
FlintDaily.com

Winfield Associates Upended Its Holding in Microsoft Com (MSFT) by \$327608 as Share Price Rose ... FlintDaily.com

# Information Gathering Using Groups, Forums, and Blogs



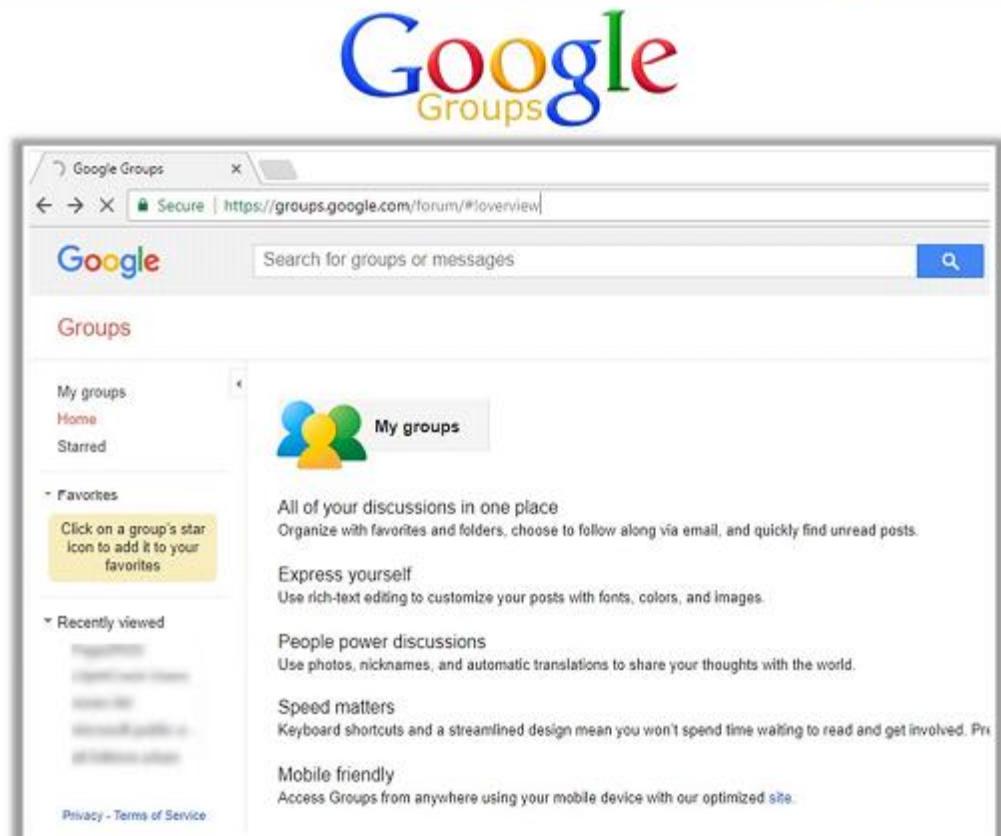
Groups, forums, and blogs provide sensitive information about a target such as **public network information**, **system information**, **personal information**, etc.



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



The screenshot shows the Google Groups homepage. At the top, there's a navigation bar with links for Home, Starred, and Favorites. The Favorites section has a callout box with the text "Click on a group's star icon to add it to your favorites". Below the navigation is a "My groups" section featuring a colorful icon of three people. To the right, there are several promotional sections: "All of your discussions in one place", "Express yourself", "People power discussions", "Speed matters", and "Mobile friendly". At the bottom of the page, there are links for Privacy and Terms of Service, and the URL https://groups.google.com is visible at the very bottom.

## Footprinting

### Footprinting through Web Services

# Determining the Operating System

**CEH**  
Certified Ethical Hacker

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

NETCRAFT PIPE Strategic Global Data Center Locations

### Search Web by Domain

Results for **microsoft.com**

Rank	Site	Site Report	First seen	Netblock	OS
1.	govmicrosoft.com	never	2000	global	Linux
2.	www.microsoft.com	never	1998	global	international, Linux
3.	msn.microsoft.com	never	1998	global	international, Linux
4.	download.microsoft.com	never	1998	global	international, Linux
5.	technet.microsoft.com	never	1998	global	Windows Server 2012
6.	media.microsoft.com	never	1998	global	Windows Server

<https://www.netcraft.com>

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

SHODAN microsoft.com

### TOTAL RESULTS

**13,047**

### TOP COUNTRIES

United States 3,765  
Brazil 2,540  
Germany 5,040  
Ireland 720  
Netherlands 480

### DMP

06.3.50.44  
06.3-30-44-dynamic.rndcs.net  
Microsoft Corporation - Microsoft  
Last updated: 2017-07-10 11:44:31 GMT  
United States, Bramhall, Details

### Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

### XenMobile - Console - Logon

Supported SSL Versions  
TLSv1, TLSv1.1, TLSv1.2

Details

HTTP/1.1 200 OK  
Server: Apache-Goyache/1.1  
Set-Cookie: JSESSIONID=4F7F276084C75425D05818F2842A77; Path: /;HttpOnly;SameSite: None  
Content-Security-Policy: default-src 'self' https://\*.cloud.ca...;frame-ancestors:...;

### TOP SERVICES

SSH 3,845  
HTTPS 2,483  
HTTP/1.1 (443) 2,187  
Symantec Data Center Se... 1,944  
8881 257

### TOP ORGANIZATIONS

Awsome.com 1,511  
Vive 5205  
Tia Celular S.A. 919  
Verizon Business 727  
Awanice Data Services Inc... 384

### TOP OPERATING SYSTEMS

Windows 7 or 8 95  
Linux 3.0 4  
Linux 2.6 1

<https://www.shodan.io>

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

Censys microsoft

### PvP Hosts

Filter by IP: United States, de.CN, MX, 199M  
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

24.192.174.201[234]  
192.174.120.computer-lanezawaws.com  
Amazon.com, Inc. [14618] Houston, Texas, United States  
Amazon [22.255.44.3] 80[http]  
Free Online Translation [free-translation.net, www.free-translation.net]

8.20.78.123[pahealthcoverage.com]  
Level 3 Communications, Inc. [2356] United States  
Windows [21.170.60.11] 80[http]  
PA Health Coverage [21.170.60.11] 80[http]  
beeserver18 [beeserver18] Microsoft FTP

157.56.219.64  
Microsoft Corporation [6075] Redmond, Washington, United States  
44.233.192.44[https]  
infecteddvdemo[com]  
autonomous\_system[organization]: Microsoft Corporation

52.178.177.35  
Microsoft Corporation [6075] Dublin, Leinster, Ireland  
44.233.192.44[https]  
taanboxoperations[dynamics.com]  
autonomous\_system[organization]: Microsoft Corporation

52.178.107.94  
Microsoft Corporation [6075] Amsterdam, North Holland, Netherlands  
44.233.192.44[https]  
operations[dynamics.com]  
autonomous\_system[organization]: Microsoft Corporation

<https://censys.io>

## Footprinting

### Footprinting through Web Services

# VoIP and VPN Footprinting through SHODAN



**SHODAN** **voip** **vpn**

**Exploits** **Maps**

**TOTAL RESULTS** **63,614**

**RELATED TAGS:** **inetdbshodan**

**173.196.228.212**  
mcu-173-196-228-212.west.bctr.com  
Time Warner Cable  
Added on 2017-11-26 13:00:37 GMT  
**United States, Los Angeles**  
**Details**

Ubiquiti Networks Device  
IP: 173.196.228.212  
MAC: 44:d9:e7:40:af:90  
Alternate IP: 10.32.208.1  
Alternate MAC: 44:d9:e7:40:af:51  
Hostname: **voip-router**  
Product: EMLite-3  
Version: EdgeRouter.ER-e100.v1.2.0.4574253.138626.1248

**TOP COUNTRIES**

Italy	49,464
Germany	5,373
Taiwan	1,000
Korea, Republic of	1,000
United States	728

**TOP SERVICES**

SIP	68,388
SNMP	2,971
HTTP	2,164
Telnet	1,096
Telnet + SSL	1,476

**TOP ORGANIZATIONS**

Wind Telecommunications	48,981
Deutsche Telekom AG	3,597
WIND	3,518
Wind Telecommunicazioni ...	2,465
Telecom Italia	444

**TOP OPERATING SYSTEMS**

Unix	21
Linux 3.x	15
Linux 2.6.x	14

**41.221.251.154**  
MSTELCOM  
Added on 2017-11-26 12:36:15 GMT  
**Angola, Luanda**  
**Details**

AS-VOIP-ON Login:

**SHODAN** **vpn** **voip**

**Exploits** **Maps**

**TOTAL RESULTS** **41,659,021**

**RELATED TAGS:** **inetdbshodan**

**174.116.80.205**  
CPE700d7473021-  
CM733a77473290.xpe.net.cable.rogers.com  
Rogers Cable  
Added on 2017-11-27 06:46:34 GMT  
**Canada, Brampton**  
**Details**

VPN (IKE)  
Initiator SPI: e5f858a8874af526  
Responder SPI: f16c807a2ee84f28  
Next Payload: Notification (N)  
Version: 1.0  
Exchange Type: Informational  
Flags:  
Encryption: False  
Commit: False  
Authentication: False  
Message ID: ab821a8e  
Length: 48

**TOP COUNTRIES**

China	32,526,128
United States	2,896,137
Germany	756,490
Canada	711,158
United Kingdom	416,448

**TOP SERVICES**

IKE	37,616,988
IKE-NAT-T	4,240,354
HTTPS	26,292
PPTP	16,485
HTTP	15,927

**TOP ORGANIZATIONS**

Alesta, S. de R.L. de C.V.	static-251-151-177-00.alesta.net.mx
Mexico, Tlaxcala	Added on 2017-11-26 13:28:36 GMT
Plaza Arboledas	Login:

**TOP OPERATING SYSTEMS**

China Telecom Guangdong	1,945,129
China Telecom	1,556,328
China TieTong	1,506,144
China Mobile Guangdong	1,284,207
China Mobile	1,204,149

**201.151.177.90**  
static-251-151-177-00.alesta.net.mx  
Alesta, S. de R.L. de C.V.  
Added on 2017-11-26 13:28:36 GMT  
**Mexico, Tlaxcala**  
**Details**

DD-WRT v24 vpn (c) 2007 NewMedia-NET GmbH  
Release: 11/22/07 (SVN revision: 8428)

**203.145.135.134**  
Bharti Broadband  
Added on 2017-11-26 13:17:38 GMT  
**India, New Delhi**  
**Details**

16/100 4-Port VPN Router

**85.126.138.42**  
85.126.138.42.static.upcbusiness.at  
UPC Austria  
Added on 2017-11-26 13:12:38 GMT  
**Austria**  
**Details**

#  
| LANCOM 1711+ VPN  
| Ver. 8.04.0132Prel / 31.01.2014  
| SN: 171781880310  
| Copyright (c) LANCOM Systems

# 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

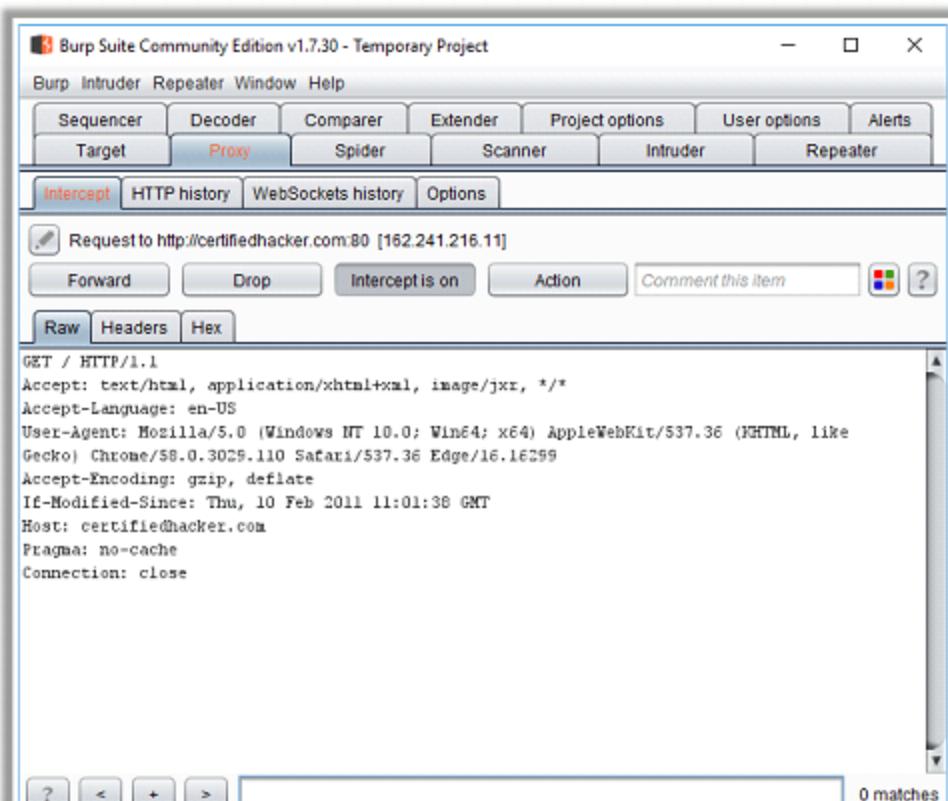
- Website footprinting refers to **monitoring and analyzing the target organization's website** for information

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

```

view-source:https://www.microsoft.com/en-in/
Secure | view-source:https://www.microsoft.com/en-in/
3
4 <!DOCTYPE html>
5 <html lang="en-in" dir="ltr">
6   <head data-info="(quot;&quot;1.0.6466.35035&quot;,&quot;a&quot;,&quot;d5b9e19c-b0f5-498b-ab57-
7 2b312cd86b2&quot;,&quot;c&quot;:&quot;3&quot;,&quot;az&quot;:&quot;(did:23c3ad49bf3c4e0aa045d269bf1c857d,
8  rids: 3, msn_marketingSites:msn-prod, dt: 2017-09-19T21:04:45.8700663Z, bt: 2017-09-
9 14T19:27:50.0000000Z)&quot;,&quot;ddpi&quot;:&quot;1&quot;,&quot;dplo&quot;:&quot;&quot;,&quot;dpi&quot;:&qu
10 uot;"&quot;,&quot;dg&quot;:&quot;uplevel.web.pc.webkit.chrome&quot;,&quot;th&quot;:&quot;default&quot;,&qu
11 t;"&quot;:&quot;en-in&quot;,&quot;1&quot;:&quot;en-in&quot;,&quot;mu&quot;:&quot;en-
12 in&quot;,&quot;rp&quot;:&quot;/en-
13 in&quot;,&quot;f&quot;:&quot;freeshippinganonb,muidflt364cf,xboxcontentondesktop,openxbl,marketingaat&quot;
14 ;">
15   <meta charset="UTF-8" />
16
17   <meta http-equiv="X-UA-Compatible" content="IE=edge" />
18   <meta name="viewport" content="width=device-width, initial-scale=1" />
19   <title>Microsoft - Official Home Page</title>
20
21     <meta property="og:url" content="https://www.microsoft.com/en-in" />
22     <meta name="twitter:title" content="Microsoft - Official Home Page" />
23     <meta property="og:title" content="Microsoft - Official Home Page" />
24     <meta name="twitter:description" content="At Microsoft our mission and values are to
25 help people and businesses throughout the world realize their full potential." />
26     <meta property="og:description" content="At Microsoft our mission and values are to
27 help people and businesses throughout the world realize their full potential." />
28     <meta name="twitter:card" content="summary" />
29     <meta property="og:type" content="website" />
30   <meta name="description" content="At Microsoft our mission and values are to help people and
31 businesses throughout the world realize their full potential."/>
32
33   <link rel="SHORTCUT ICON" href="https://c.s-microsoft.com/favicon.ico?v2" type="image/x-icon"/>

```

## Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used

All cookies and site data	
	c1.microsoft.com 2 cookies
	docs.microsoft.com 1 cookie, Local storage
	login.microsoftonline.com 1 cookie
	microsoft.com 12 cookies
	msdn.microsoft.com 2 cookies, Local storage
	technet.microsoft.com 1 cookie, Local storage
	www.microsoft.com 3 cookies, Local storage

# 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**

URL	Title	Keywords	Description	Host	Domain	Page size	Page last index
<a href="http://certifiedhacker.com/">http://certifiedhacker.com/</a>	CertifiedHacker	Keywords, or phrase A brief description	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	9680	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/01.htm">http://certifiedhacker.com/corporate-learning-website/01.htm</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5845	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/index.htm">http://certifiedhacker.com/Online Booking/index.htm</a>	Online Booking	booking, hotel, ho Online Booking	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	20280	12/27/2017	
<a href="http://certifiedhacker.com/Policy/index.html">http://certifiedhacker.com/Policy/index.html</a>	Policy			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	11606	12/27/2017	
<a href="http://certifiedhacker.com/Real Estates/index.html">http://certifiedhacker.com/Real Estates/index.html</a>	Professional Real Estate, real estate Professional Re	Professional Re	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5381	2/10/2011	
<a href="http://certifiedhacker.com/Recipes/index.html">http://certifiedhacker.com/Recipes/index.html</a>	Your company - Ho Some keywords & A short descrip	re	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5889	2/10/2011	
<a href="http://certifiedhacker.com/Social Media/index.html">http://certifiedhacker.com/Social Media/index.html</a>	Unite - Together is: keywords, or phrase A brief descrip	re	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	15094	12/27/2017	
<a href="http://certifiedhacker.com/Tubo Max/index.htm">http://certifiedhacker.com/Tubo Max/index.htm</a>	Tubo Max Theme   Tubo max , ovite   Tubo max power			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	12125	12/27/2017	
<a href="http://certifiedhacker.com/Under Construction/index.htm">http://certifiedhacker.com/Under Construction/index.htm</a>	Clear Construction			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5151	12/27/2017	
<a href="http://certifiedhacker.com/Under the trees/index.htm">http://certifiedhacker.com/Under the trees/index.htm</a>	Under the Tree			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	3653	12/27/2017	
<a href="http://certifiedhacker.com/Index.html">http://certifiedhacker.com/Index.html</a>	CertifiedHacker	Keywords, or phrase A brief descrip	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	9680	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/about">http://certifiedhacker.com/corporate-learning-website/about</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	3642	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/article">http://certifiedhacker.com/corporate-learning-website/article</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	4638	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/contact">http://certifiedhacker.com/corporate-learning-website/contact</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	7324	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/faq.htm">http://certifiedhacker.com/corporate-learning-website/faq.htm</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	3991	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/host">http://certifiedhacker.com/corporate-learning-website/host</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5028	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/host2">http://certifiedhacker.com/corporate-learning-website/host2</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5950	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/host3">http://certifiedhacker.com/corporate-learning-website/host3</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	5487	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/service">http://certifiedhacker.com/corporate-learning-website/service</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	3039	2/10/2011	
<a href="http://certifiedhacker.com/corporate-learning-website/support">http://certifiedhacker.com/corporate-learning-website/support</a>				<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	3651	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/about-us.htm">http://certifiedhacker.com/Online Booking/about-us.htm</a>	Online Booking   Sil booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	11985	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/checkout.htm">http://certifiedhacker.com/Online Booking/checkout.htm</a>	Online Booking   Cf booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	12968	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/browse.htm">http://certifiedhacker.com/Online Booking/browse.htm</a>	Online Booking   B1 booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	16031	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/contact.htm">http://certifiedhacker.com/Online Booking/contact.htm</a>	Online Booking   Cz booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	14163	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/faqs.htm">http://certifiedhacker.com/Online Booking/faqs.htm</a>	Online Booking   F1 booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	14047	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/partners.htm">http://certifiedhacker.com/Online Booking/partners.htm</a>	Online Booking   S4 booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	11689	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/search.htm">http://certifiedhacker.com/Online Booking/search.htm</a>	Online Booking   S5 booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	27877	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/terms-conditions">http://certifiedhacker.com/Online Booking/terms-conditions</a>	Online Booking   Tj booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	12661	2/10/2011	
<a href="http://certifiedhacker.com/Online Booking/hotel.htm">http://certifiedhacker.com/Online Booking/hotel.htm</a>	Online Booking   H1 booking, hotel, ho Online Booking			<a href="http://certifiedhacker.com.com">http://certifiedhacker.com.com</a>	39498	2/10/2011	

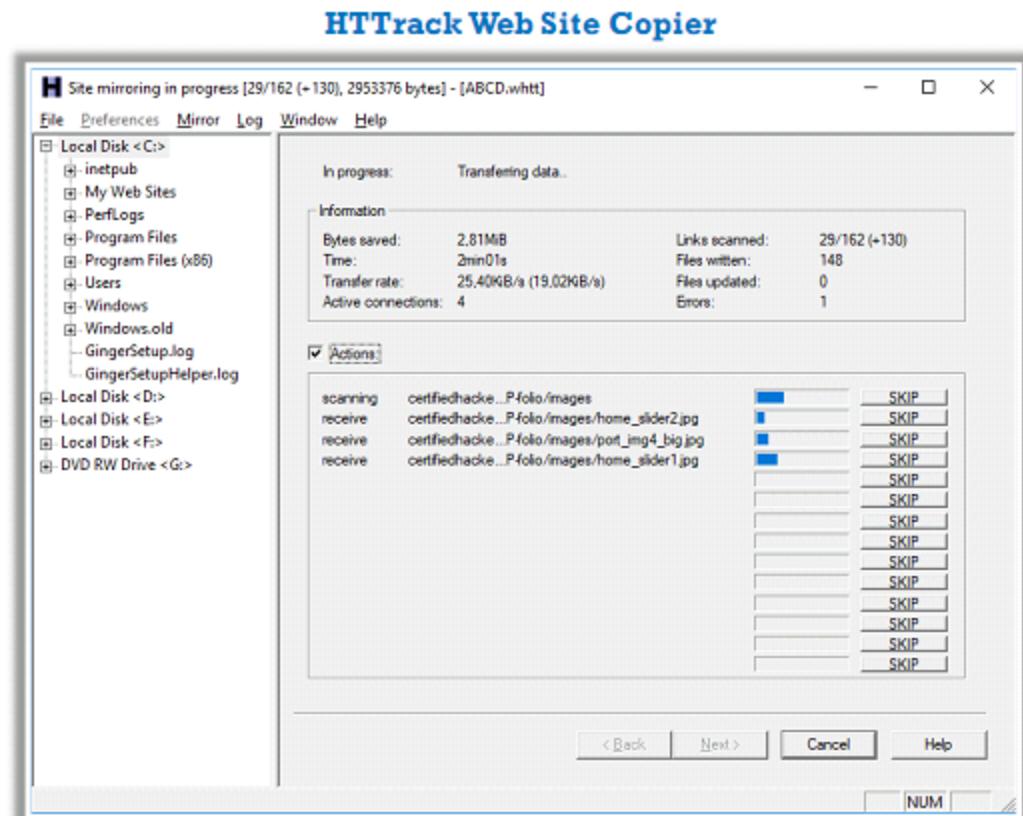
<http://www.webextractor.com>

# 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

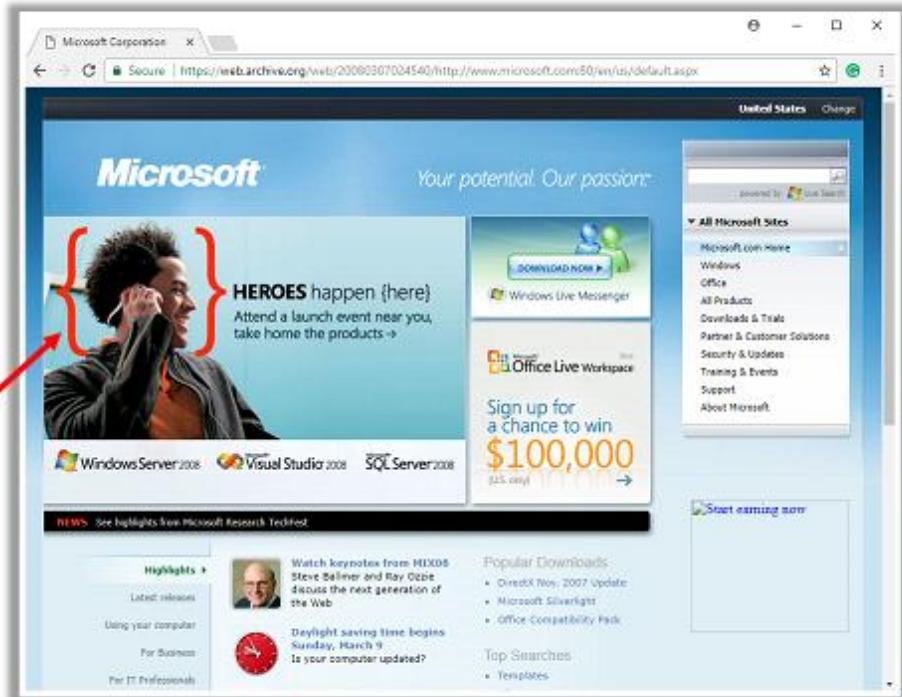
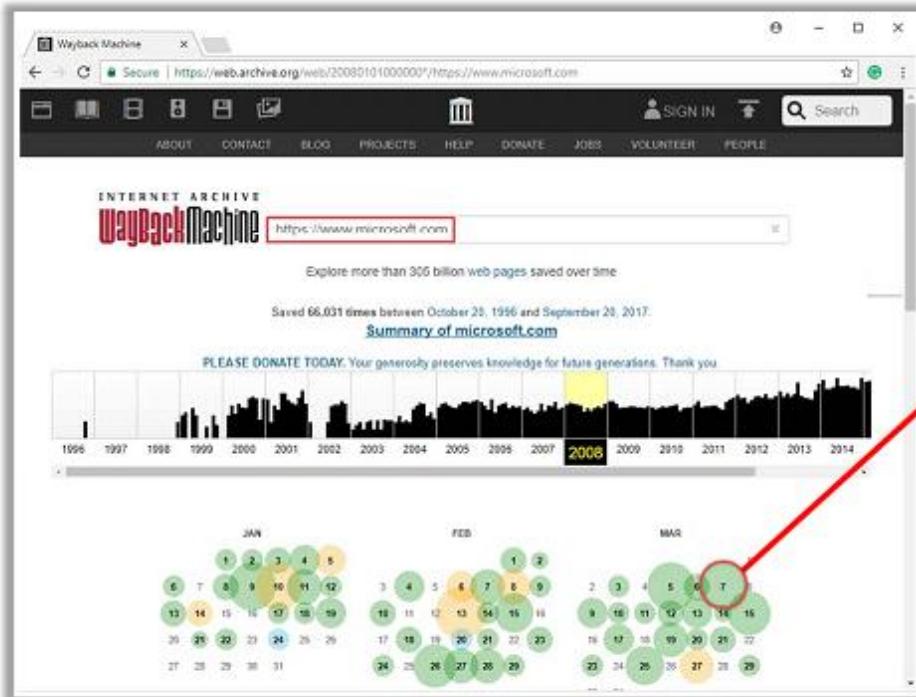
- NCollector Studio (<http://www.calluna-software.com>)
- Teleport Pro (<http://www.tenmax.com>)
- Portable Offline Browser (<http://www.metaproducts.com>)
- Website Ripper Copier (<http://www.tensons.com>)
- Gnu Wget (<https://www.gnu.org>)



<http://www.hcouncil.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, ptx, 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>)

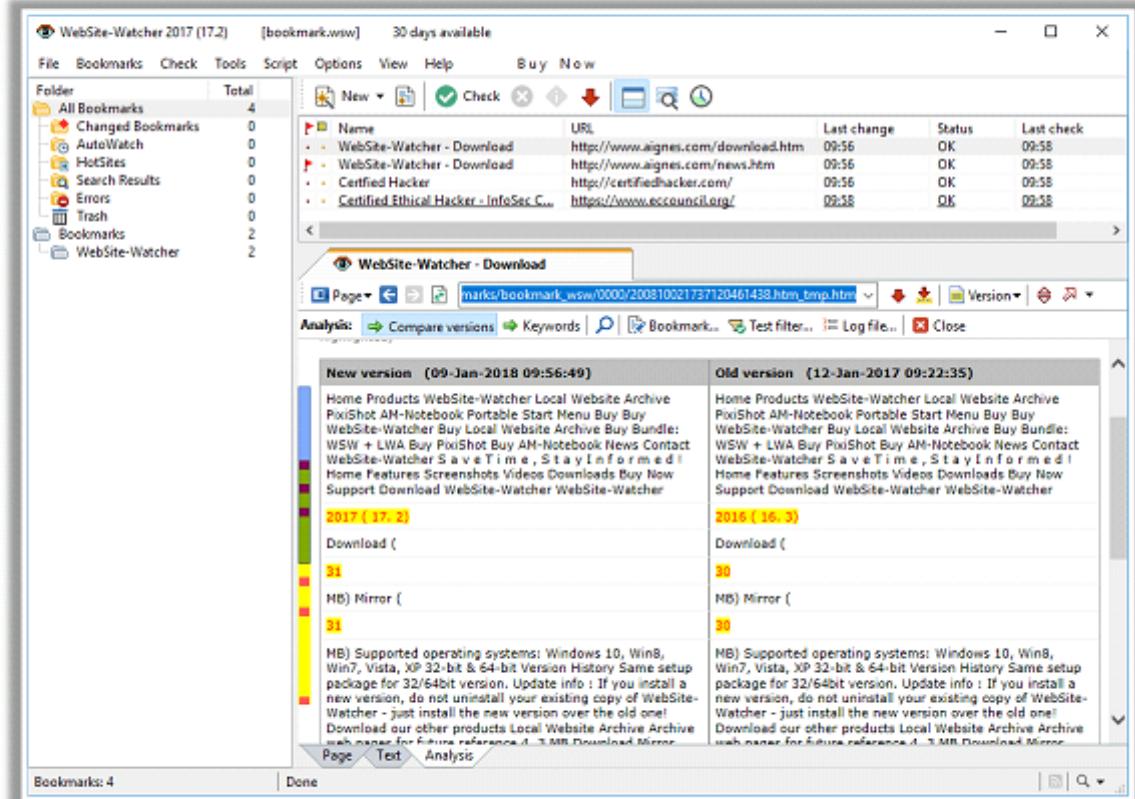
# Monitoring Web Pages for Updates and Changes

## WebSite-Watcher

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

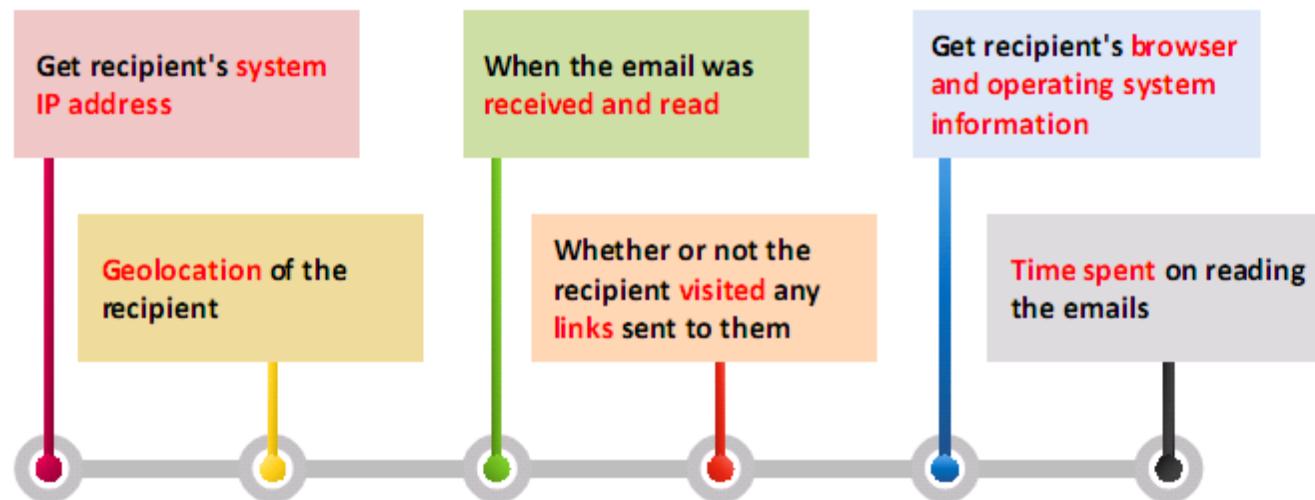
## Web Updates Monitoring Tools

- 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



## Collecting Information from Email Header

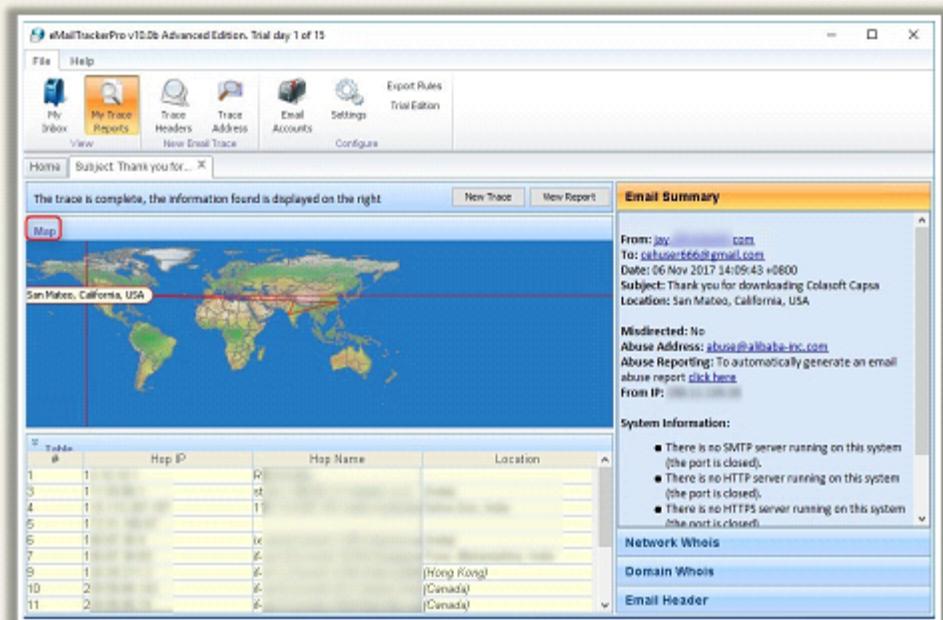
Delivered-To: Mirza@gmail.com  
Received: by 10.112.39.167 with SMTP id q7  
Thu, 1 Jun 2017 21:24:01 -0700  
Return-Path: <Mirza@gmail.com>  
Received-SPF: pass (google.com: domain of Mirza@gmail.com designates 10.224.205.137 as permitted sender) client-ip=10.224.205.137;  
Authentication-Results: mr.google.com; dkim=pass (domain of Mirza@gmail.com designates 10.224.205.137 as permitted sender) smtp.mailfrom=mirza@gmail.com  
header.i=Mirza@gmail.com  
Received: from mr.google.com ([10.224.205.137])  
by 10.224.205.137 with SMTP id fg9mr8578570qab.39.  
Thu, 01 Jun 2017 21:24:00 -0700 (PDT)  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=gmail.com; s=20120113;  
h=mime-version:in-reply-to:references  
:content-type;  
bh=TGEIPb4t1gQFQG+ghh7OkPjkx+Tt/iAC1  
b-KguZLTlf2+Q2XzEKe1NnvRcnD/+P4+Nk  
b1PK3eJ3Uf/CsaBZWdIT0XLaKOAGrP3B0t92MCZFxeUUQ9uL/xHALSNkeUIEEeKGqOC  
oa9hD59D3oXI8KAC7zmkb1GzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqtlfP  
ZhrWFKh5xSn2XsE73xZPEYzp7yecCeQuYHZNgs1KcO7xQjeZuw+HWK/vR6xChDjap24  
K5ZAfY2mkIkFX+VdL2qu7YGFzy6oHcuP16yS/C2fxHVdsuYamMT/yecvhCVo8Og7FKt6  
/Kzw==  
MIME-Version: 1.0  
Received: by 10.224.205.137 with SMTP id 1338611040318;  
Thu, 01 Jun 2017 21:24:00 -0700 (PDT)  
Received: by 10.229.230.79 with HTTP; Thu, 01 Jun 2017 21:24:59 -0700 (PDT)  
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhE4Ber2...> <subp8Eg@mail.gmail.com>  
References: <CAOYWATT1zdDXE3o8D2rhE4Ber2...> <vUhro6r+7Mu7c8ubp8Eg@mail.gmail.com>  
Date: Fri, 2 Jun 2017 09:53:59 +0530  
Message-ID: <CAMSVoxTUQejnfwswJdSzQhNhO=EMJcgfGX+mUFjB\_tt2sy2dxA@mail.gmail.com>  
Subject: ::: S O L U T I O N S :::  
From: Mirza <Mirza@gmail.com>  
To: an@gmail.com,  
S O L U T I O N S <solutions@gm...> need <...er@yahoo.com>,

# 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

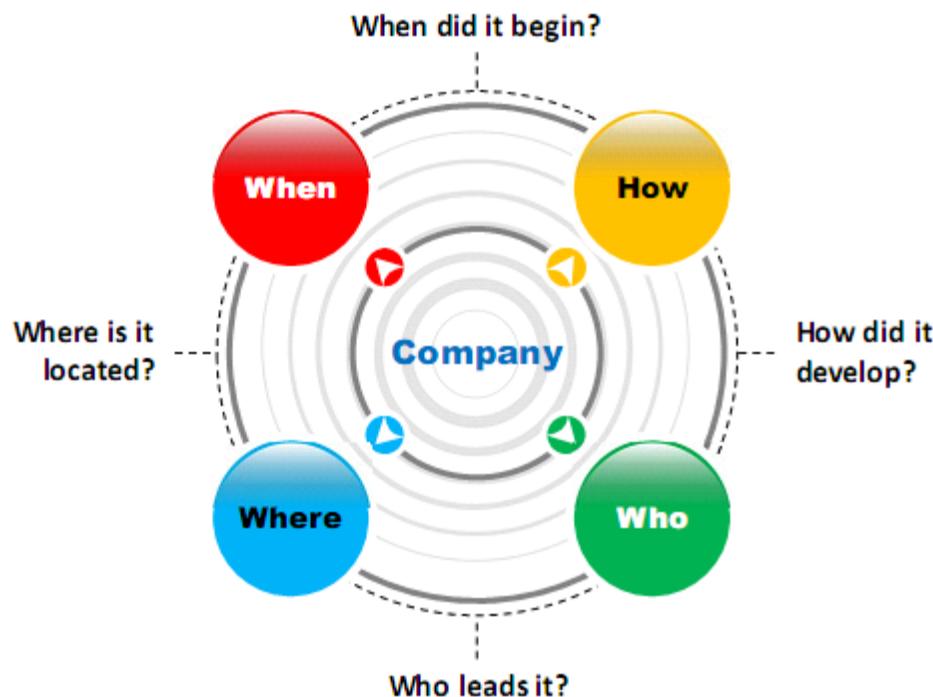
- Competitive intelligence gathering is the process of **identifying, gathering, analyzing, verifying**, and using information about your competitors from resources such as the Internet
- Competitive intelligence is **non-interfering** and **subtle in nature**



## Sources of Competitive Intelligence

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

# 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?



- 01 **MarketWatch** (<https://www.marketwatch.com>)  
- 02 **The Wall Street Transcript** (<https://www.twst.com>)  
- 03 **Alexa** (<https://www.alexa.com>)  
- 04 **Euromonitor** (<http://www.euromonitor.com>)  
- 05 **Experian** (<http://www.experian.com>)  
- 06 **SEC Info** (<http://www.secinfo.com>)  
- 07 **The Search Monitor** (<https://www.thesearchmonitor.com>)  

# Competitive Intelligence - What Expert Opinions Say About the Company

**ABI/INFORM Global**

<http://www.proquest.com>

**SEMRush**

<https://www.semrush.com>

**SimilarWeb**

<https://www.similarweb.com>

**Copernic Tracker**

<http://www.copernic.com>

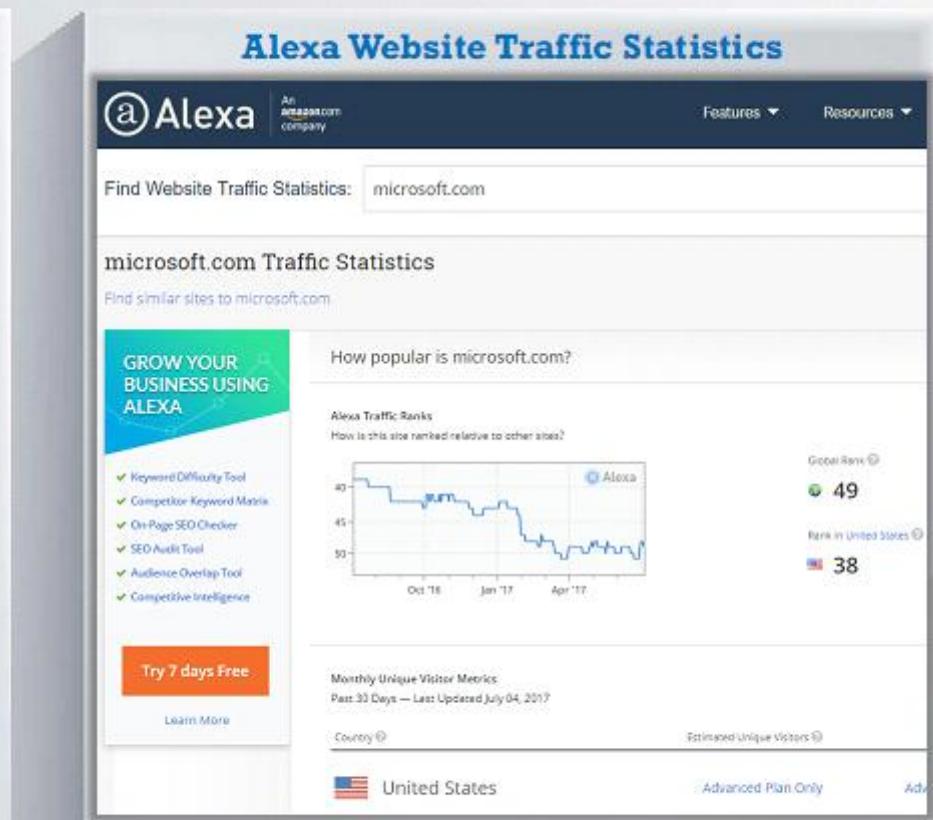
**AttentionMeter**

<http://www.attentionmeter.com>

**AttentionMeter**

# 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



# 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

The screenshot shows the Trackur web application interface. At the top, there is a navigation bar with links for 'Dashboard', 'Settings', and 'Help'. Below the navigation bar, a banner displays a message: 'Your free Premium trial has 10 days left. Upgrade now.' and a 'Logout' link. On the left side, there are two dropdown menus: 'Profiles' (set to 'Main Account') and 'Keyword' (set to 'facebook'). Below these menus is a search bar with the text 'facebook' and a 'Save Search' button. The main content area is titled 'Results for: facebook'. It features a table with columns for 'Source', 'Snippet', 'Influence' (with a color-coded scale from green to red), 'Date', and 'Sentiment'. The table lists several search results, each with a small icon indicating the source (e.g., Facebook, YouTube, Twitter). The results include:

Source	Snippet	Influence	Date	Sentiment
FACEBOOK AND OTHER MEDIA USERS PLEASE GO TO WEBSITE FOR COMPLETE FORECAST OUTLOOK. SUBSC	NA	07/11/17	green	
...	NA	07/11/17	red	
The consensus in Igualt seems to be that everyone with a credit card has an Ama	NA	07/11/17	yellow	
<a href="https://www.facebook.com/groups/OcalahorseSales/permalink/698628623655718/">https://www.facebook.com/groups/OcalahorseSales/permalink/698628623655718/</a>	NA	07/11/17	yellow	
Another video exclusively from beauties cafe.	NA	07/11/17	yellow	
Click here to watch - <a href="https://www.youtube.com/watch?v=90iElSeb0ag">https://www.youtube.com/watch?v=90iElSeb0ag</a>	49	07/11/17	yellow	
from Facebook via IFTTT <a href="https://youtu.be/yW1-W04xml">https://youtu.be/yW1-W04xml</a> <a href="https://youtu.be/90iElSeb0ag">https://youtu.be/90iElSeb0ag</a>	NA	07/11/17	red	
2013 Nissan Qashqai 1.6 Acenta Limited Edition Crystal Sunroof 82,000km Manual Gear, Leather	NA	07/11/17	red	

<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)



## Footprinting

## Whois Footprinting

## Whois Lookup Result Analysis

## Whois Record for CertifiedHacker.com

Whois & Quick Stats	
Email	abuse@web.com is associated with ~9,108,273 domains gs2nm3j...@networksolutionspvtaregistration.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) NS2.BLUEHOST.COM (has 2,341,313 domains)
IP Address	69.89.31.193 - 1,316 other sites hosted on this server
IP Location	USA - 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	// Certified Hacker
Server Type	nginx/1.12.0
Response Code	200
SEO Score	98%
Terms	36 (Unique: 28, Linked: 7)

<http://whois.domaintools.com>

SmartWhois - Evaluation Version

File Query Edit View Settings Help

I, host or domain: certifiedhacker.com

certifiedhacker.com

certifiedhacker.com

69.89.31.193

PERFECT PRIVACY, LLC  
12808 Gran Bay Parkway West  
Jacksonville  
FL  
32258  
United States  
Phone: +1.5707088780  
gs2nm3j...@networksolutionspvtaregistration.com

PERFECT PRIVACY, LLC  
12808 Gran Bay Parkway West  
Jacksonville  
FL  
32258  
United States  
Phone: +1.5707088780  
gs2nm3j...@networksolutionspvtaregistration.com

PERFECT PRIVACY, LLC  
12808 Gran Bay Parkway West  
Jacksonville  
FL  
32258  
United States  
Phone: +1.5707088780  
gs2nm3j...@networksolutionspvtaregistration.com

NS1.BLUEHOST.COM  
NS2.BLUEHOST.COM

Alexa Traffic Rank: 2,519,095

Created: 2014-03-28T12:11:47Z  
Updated: 2017-03-05T17:15:49Z  
Expires: 2021-07-29T04:00:00Z  
Source: whois.networksolutions.com

Done

certifiedhacker.com - Source

Domain Name: CERTIFIEDHACKER.COM  
Registry Domain ID: 68849376\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.networksolutions.com  
Registrar URL: http://www.networksolutions.com  
Updated Date: 2017-03-05T17:15:49Z  
Creation Date: 2014-03-28T12:11:47Z  
Registrar Registration Expiration Date: 2021-07-29T04:00:00Z  
Registrar: NETWORK SOLUTIONS, LLC.  
Registrar IANA ID: 2  
Registrar Abuse Contact Email: abuse@web.com  
Registrar Abuse Contact Phone: +1.8003387680  
Reseller:  
Domain Status:  
Registry Registrant ID:  
Registrant Name: PERFECT PRIVACY, LLC  
Registrant Organization:  
Registrant Street: 12808 Gran Bay Parkway West  
Registrant City: Jacksonville  
Registrant State/Province: FL  
Registrant Postal Code: 32258  
Registrant Country: US  
Registrant Phone: +1.5707088780  
Registrant Phone Ext:  
Registrant Fax:  
Registrant Fax Ext:  
Registrant Email: gs2nm3j...@networksolutionspvtaregistration.com  
Registry Admin ID:  
Admin Name: PERFECT PRIVACY, LLC  
Admin Organization:  
Admin Street: 12808 Gran Bay Parkway West  
Admin City: Jacksonville  
Admin State/Province: FL  
Admin Postal Code: 32258  
Admin Country: US

<http://www.tamos.com>

# Whois Lookup Tools



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



**Whois Lookup Multiple Addresses Software**  
<https://www.sabsoft.com>



**DNS Tools**  
<https://www.dnsniffer.com>



**Whois Analyzer Pro**  
<http://www.whoisanalyzer.com>



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



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



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



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



**Whois®**  
<https://www.whois.com.au>



**WhoisThisDomain**  
<http://www.nrsoft.net>



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



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



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



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



**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) 08
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

**DNSreport Results for certifiedhacker.com**

Overall Results:			
FAIL	WARNING	PASS	INFO
2	0	17	4

**PARENT**

Status	Test Name	Information
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are [nameserv]
PASS	Number of nameservers	At least 2 ( <a href="#">RFC2182</a> section 5 recommends at least 3), but fewer than 8 NS records exist. ( <a href="#">RFC1912</a> section 2.8 is more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in a single point of failure. The NS Records provided are:

ns1.bluehost.com. | 162.159.24.80  
ns2.bluehost.com. | 162.159.25.175

**NS**

Status	Test Name	Information
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your; responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), It is record when asked for data or were not specifically asked for that data:
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which running correctly and your zone [domain] is valid. The Nameservers provided are nameservers that supply answers those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), send an A record when asked for data or were not specifically asked for that data:
PASS	Open DNS servers	Nameservers do not respond to recursive queries. Your DNS servers do not announce that they are open DNS servers recursively). Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used that externally facing DNS servers do not recursively answer queries.
PASS	All nameservers authoritative	All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up and that we should be able to get good responses to further queries. <a href="http://www.dnsstuff.com">http://www.dnsstuff.com</a>

 **DIG**  
<http://www.kloth.net>

 **myDNSTools**  
<http://www.mydnstools.info>

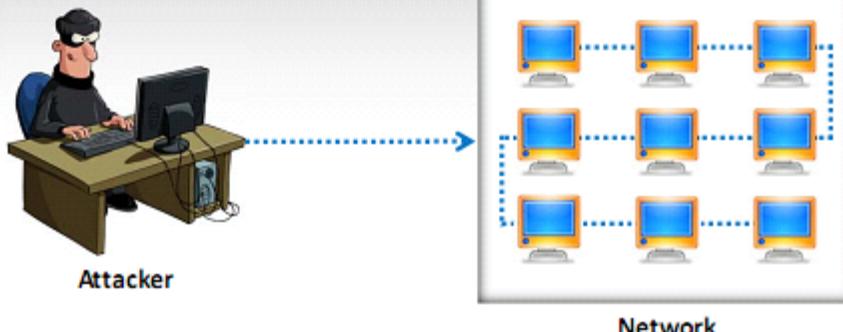
 **Domain Dossier**  
<https://centralops.net>

 **DNS DataView**  
<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	
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	<a href="https://whois.arin.net/rest/net/NET-207-46-0-0-1">https://whois.arin.net/rest/net/NET-207-46-0-0-1</a>
See Also	<a href="#">Related organization's POC records</a>
See Also	<a href="#">Related delegations</a>

Organization	
Name	Microsoft Corporation
Handle	MSFT
Street	One Microsoft Way
City	Redmond
State/Province	WA
Postal Code	98052
Country	US
Registration Date	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: * <a href="https://cert.microsoft.com">https://cert.microsoft.com</a> .

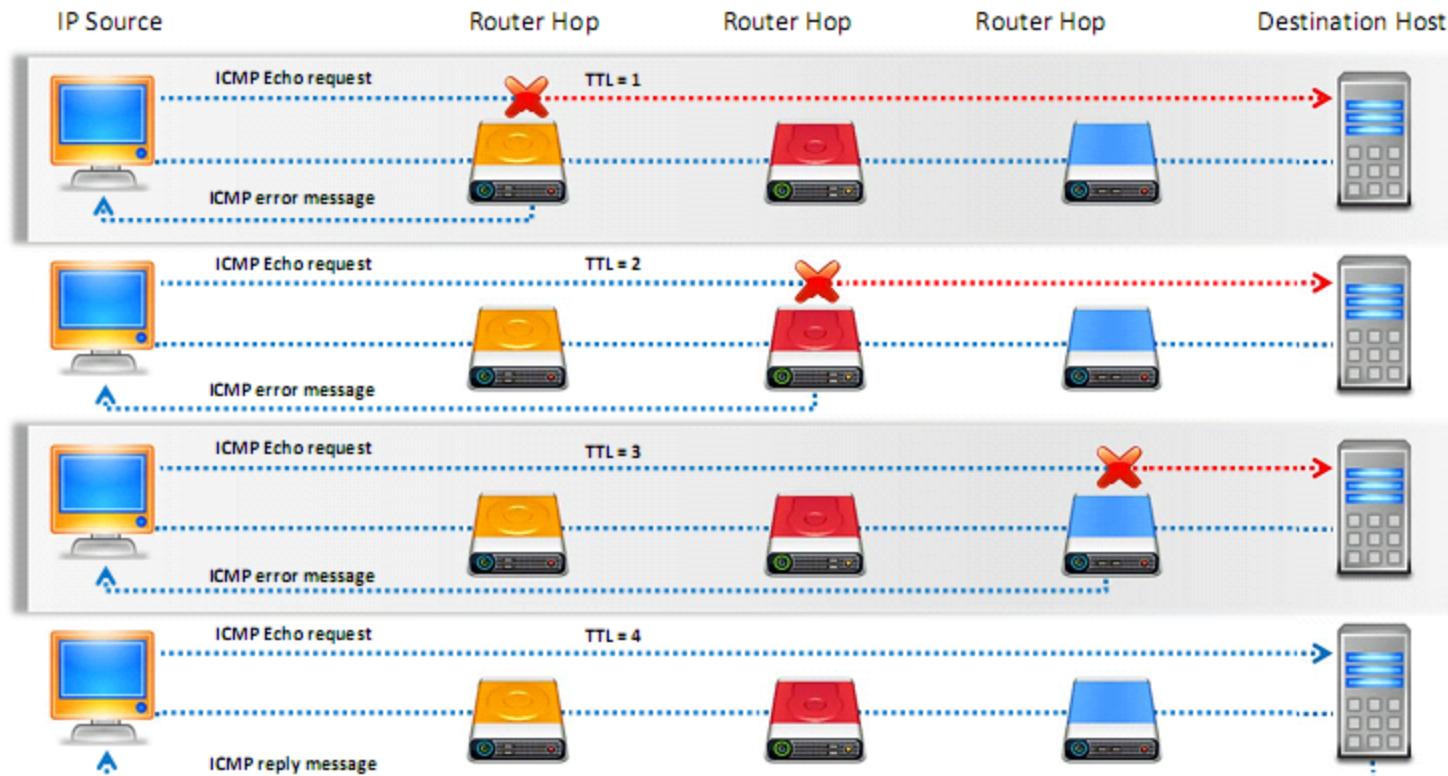
**Network Whois Record**

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

For SPAM and other abuse issues, such as Microsoft Accounts, please contact:  
\* [abuse@microsoft.com](mailto:abuse@microsoft.com).

# Traceroute

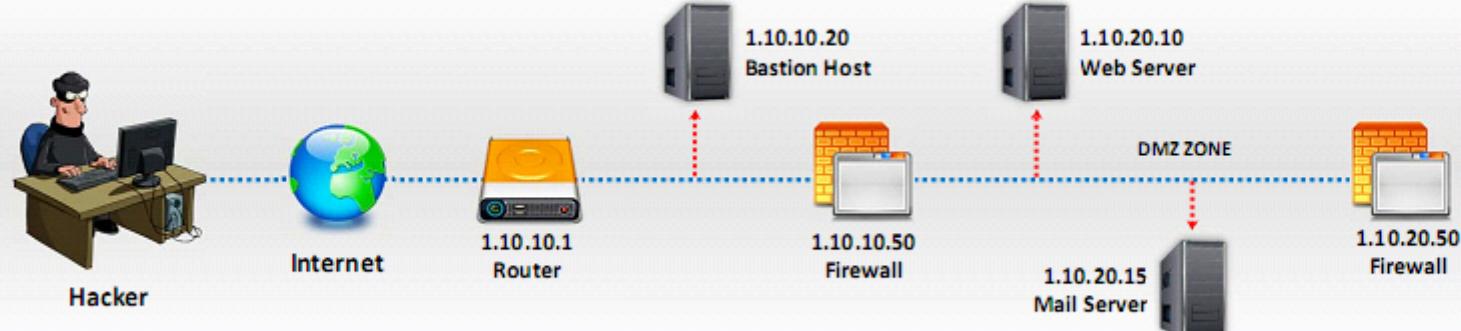
Traceroute programs work on the concept of **ICMP protocol** and use the TTL field in the header of ICMP packets to discover the routers on the path to a target host



# Traceroute Analysis



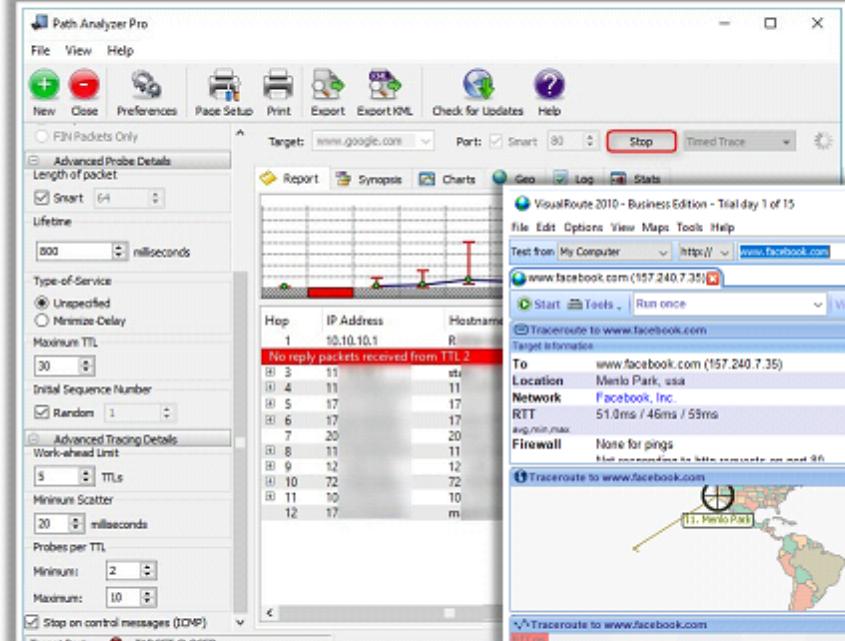
- Attackers conduct traceroute to extract information about **network topology**, **trusted routers**, and **firewall locations**
  - For example: after running several **traceroutes**, an attacker might obtain the following information:
    - traceroute 1.10.10.20, second to last hop is 1.10.10.1
    - 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**



**Attack Process**

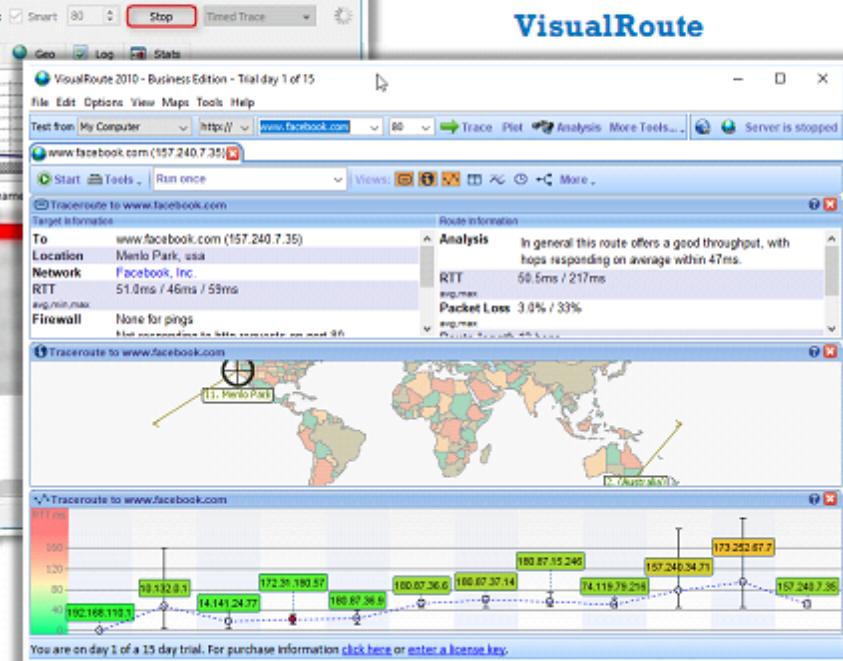
# Traceroute Tools

## 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.tlsoft.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**

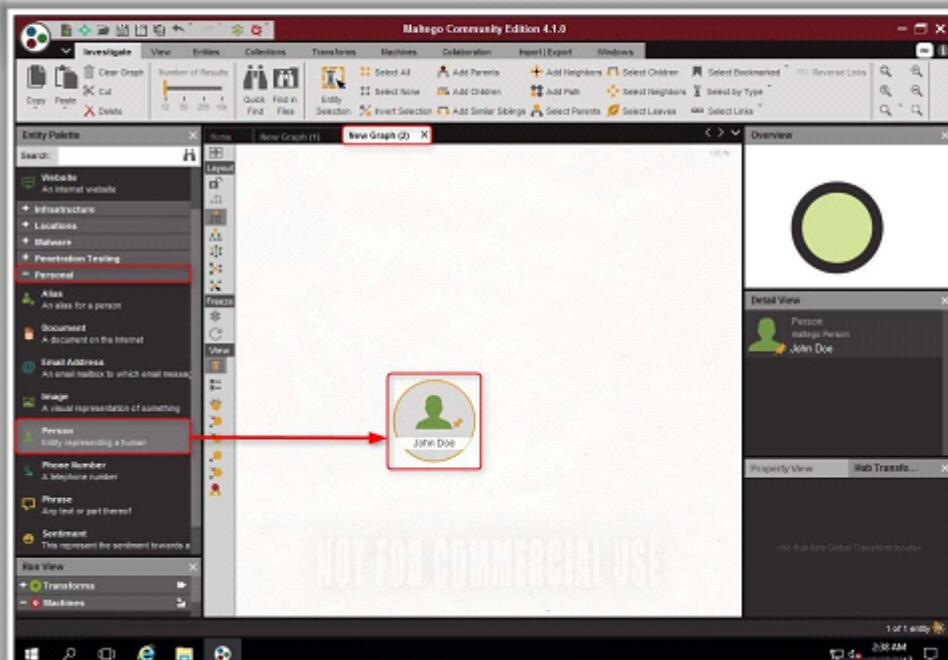
5

**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



## 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

```
root@kali: ~
File Edit View Search Terminal Help
[recon-ng][reconnaissance][whois_pocs] > set SOURCE facebook.com
SOURCE => facebook.com
[recon-ng][reconnaissance][whois_pocs] > run
-----
FACEBOOK.COM
-----
[*] URL: http://whois.arin.net/rest/pocs;domain=facebook.com
[*] URL: http://whois.arin.net/rest/poc/NOL17-ARIN
[*] [contact] Lea Neteork ops (leigha311@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/OPERA82-ARIN
[*] [contact] <blank> Operations (domain@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/BST184-ARIN
[*] [contact] Brandon Stout (bstout@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/DJW23-ARIN
[*] [contact] Darrell Wayne (tiffany.cameron.507@facebook.com) - Whois contact
[*] URL: http://whois.arin.net/rest/poc/MZU-ARIN
[*] [contact] Mark Zuckerberg (zuck@facebook.com) - Whois contact
-----
SUMMARY
-----
[*] 5 total (0 new) contacts found.
[recon-ng][reconnaissance][whois_pocs] >
```

<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

The screenshot shows the FOCA application interface. On the left, there's a sidebar with project management options like Project, Report, Tools, Options, TaskList, Plugins, and About. Below that is a tree view of the project structure under "Project of www.ecouncil.org". The main area features a large pink cartoon character logo with the word "FOCA" on it. A table lists 11 PDF files found at various URLs. A context menu is open over the first file, listing options like Download, Download All, Delete, Delete All, Extract Metadata, Extract All Metadata, Analyze Metadata, Add file, Add folder, and Add URLs from file. At the bottom, there's a log table showing Fuzzer activity and a message about insecure methods found.

Time	Source	Severity	Message
8:58:25 ...	Fuzzer	high	Insecure methods found (trace) on https://www.ecouncil.org/443/wp-content/uploads/2015/10/
8:58:28 ...	Fuzzer	high	Insecure methods found (trace) on https://www.ecouncil.org/443/wp-content/uploads/2015/10/
8:58:30 ...	Fuzzer	high	Insecure methods found (trace) on https://www.ecouncil.org/443/wp-content/uploads/2015/10/
8:58:36 ...	Fuzzer	high	Insecure methods found (trace) on https://www.ecouncil.org/443/wp-content/uploads/2015/10/
8:58:37 ...	Fuzzer	high	Insecure methods found (trace) on https://www.ecouncil.org/443/wp-content/uploads/2015/10/
8:59:02 ...	Fuzzer	high	Insecure methods found (trace) on https://www.ecouncil.org/443/wp-content/uploads/2016/12/

**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

The screenshot shows the Recon-Dog terminal interface running on a Kali Linux system. The command "python dog.py" is entered, followed by the domain "certifiedhacker.com". The output displays a menu of 10 options: Whois Lookup, DNS Lookup + Cloudflare Detector, Zone Transfer, Port Scan, HTTP Header Grabber, Honeypot Detector, Robots.txt Scanner, Link Grabber, IP Location Finder, and Traceroute. The WHOIS lookup results for the domain are then displayed, including the domain name, registrar information, creation date, expiration date, and nameservers.

```

root@kali: ~/Desktop/ReconDog
File Edit View Search Terminal Help
root@kali:~/Desktop/ReconDog$ python dog.py
RECONDOG v0.8
Made with <3 By Team Ultimate

1. Whois Lookup
2. DNS Lookup + Cloudflare Detector
3. Zone Transfer
4. Port Scan
5. HTTP Header Grabber
6. Honeypot Detector
7. Robots.txt Scanner
8. Link Grabber
9. IP Location Finder
10. Traceroute
Enter your choice: 1
Enter Domain or IP Address: certifiedhacker.com
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2016-03-16T12:38:41Z
Creation Date: 2002-07-30T00:32:00Z
Registry Expiry Date: 2021-07-30T00:32:00Z
Registrant: Network Solutions, LLC.
Registrant IANA ID: 2
Registrant Abuse Contact Email: abuse@web.com
Registrant Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/eppclientTransferProhibited
Name Servers: NS1.BLUEHOST.COM
Name Servers: NS2.BLUEHOST.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
Last update of whois database: 2018-01-00T05:41:47Z

```

# 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

```

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# searchfy.py -q "ECCOUNCIL"
Configuring OSRFramework working directory for Maltego...
Building the .mtz file.
Moving the .mtz file to the following folder: /root/osrframework-maltego-settings_v0.11.mtz
Moving the .mtz file to the backup folder: /root/.config/OSRFramework/default/osrframework-maltego-settings_v0.11.
OSRFramework
Version: OSRFramework 0.17.2
Created by: Felix Brezo and Yaiza Rubio, (i3visio)
searchfy.py Copyright (C) F. Brezo and Y. Rubio (i3visio) 2014-2017

This program comes with ABSOLUTELY NO WARRANTY. This is free software, and you
are welcome to redistribute it under certain conditions. For additional info,
visit https://www.gnu.org/licenses/agpl-3.0.txt

2017-12-27 23:50:26.248005      Starting search in different platform(s)... Relax!
Press <Ctrl + C> to stop...

[[ In skype.py, exception caught when checking information in Skype! ]]

2017-12-27 23:50:37.692078      A summary of the results obtained are listed in the following table:

Sheet Name: Profiles recovered (2017-12-27_23h50m).
+-----+-----+-----+
| i3visio_uri | i3visio_alias | i3visio_platform |
+-----+-----+-----+
| http://twitter.com/ECCouncil01 | ECCouncil01 | Twitter |
| http://twitter.com/ECCOUNCIL2 | ECCOUNCIL2 | Twitter |
| http://twitter.com/ECCUniversity | ECCUniversity | Twitter |
| http://twitter.com/EccouncilSSESas | EccouncilSSESas | Twitter |
| http://twitter.com/EccouncilIT | EccouncilIT | Twitter |
| http://github.com/eccouncilindia | eccouncilindia | Github |
| http://twitter.com/eccouncil_be | eccouncil_be | Twitter |
| http://mon.mit.edu/eks/lookup?search= | @eccouncil.org | PGPMT |
+-----+-----+-----+

```

<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

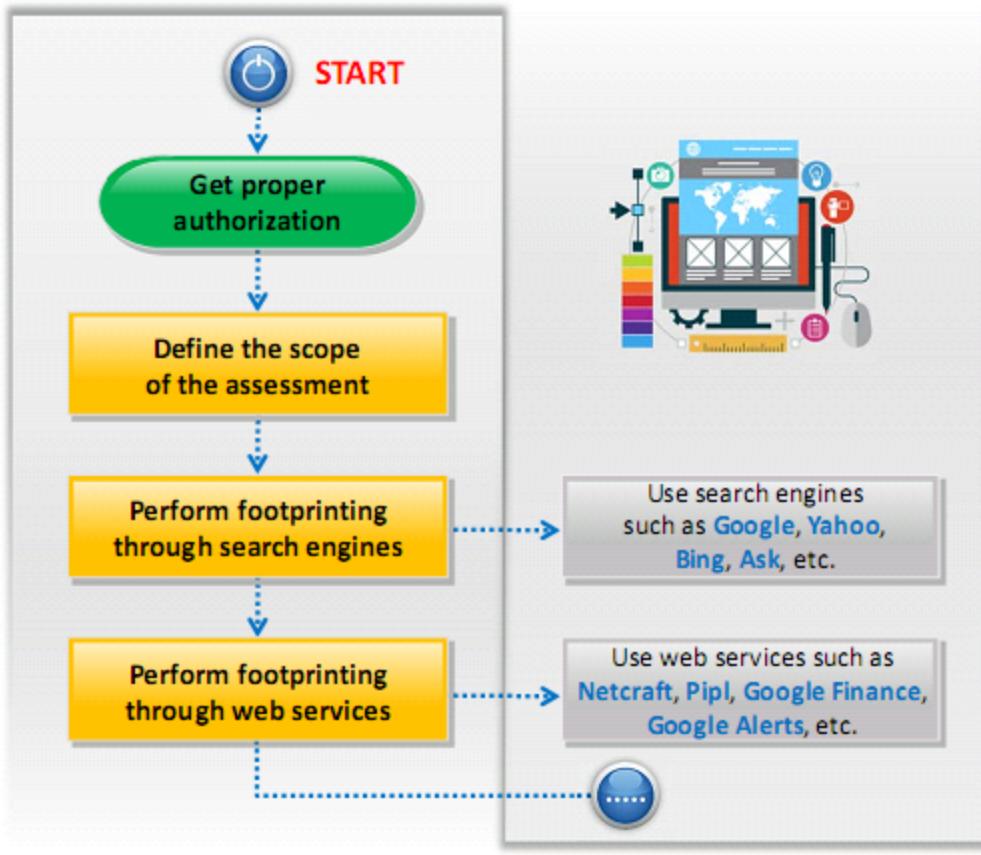
- Footprinting pen testing is used to **determine an organization's information**
- The tester attempts to gather as much information as possible about the target organization from the **Internet and other publicly accessible sources**

**Footprinting pen testing helps organization to:**

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

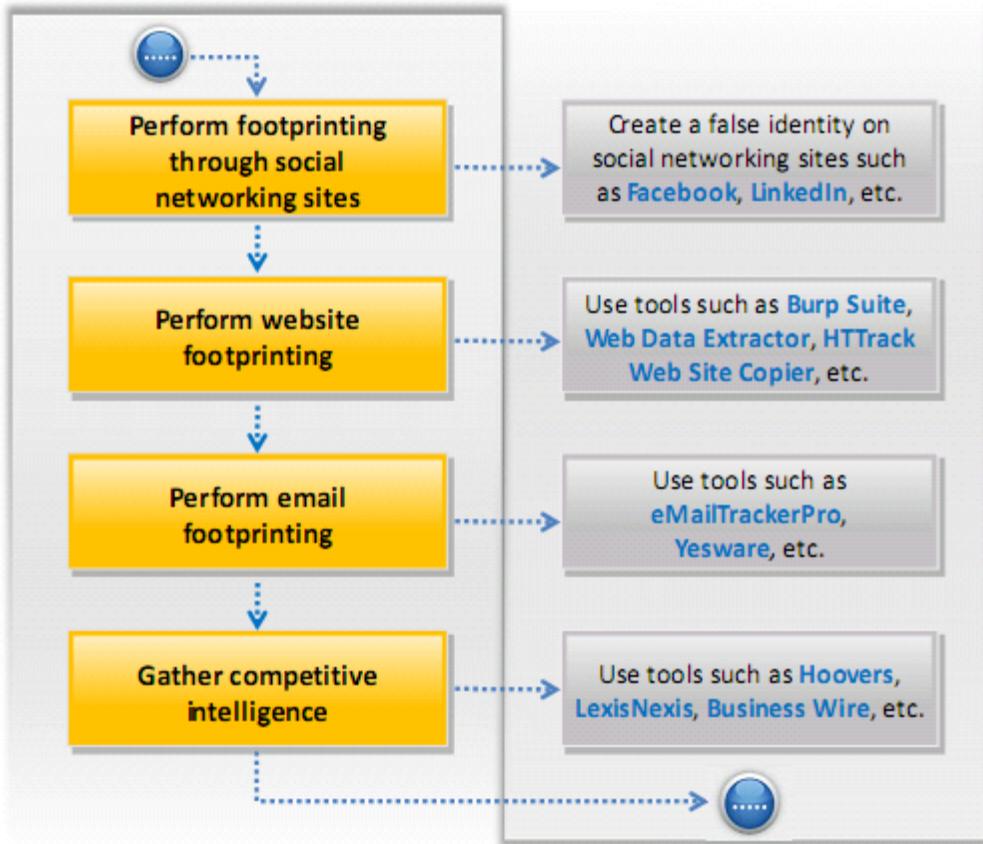


# Footprinting Pen Testing (Cont'd)



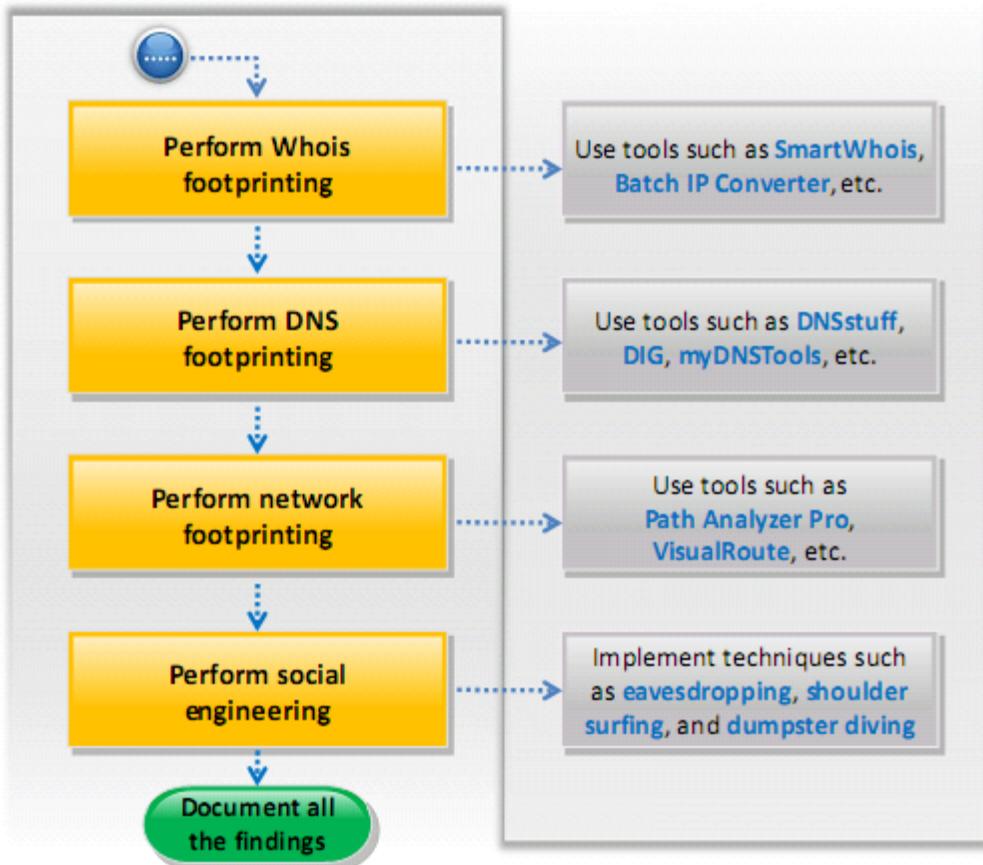
- Get proper authorization and define the scope of the assessment
- Footprint search engines such as **Google**, **Yahoo**, **Ask**, **Bing**, **Aol**, etc. to gather target organization's information such as employee details, login pages, intranet portals, operating systems used, financial information, 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 network footprinting

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

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

### Information obtained through DNS footprinting

-  Location of DNS servers:
-  Type 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