

Objective

- Understanding Footprinting Concepts
- Footprinting through Search Engines
- Footprinting Using Advanced Google Hacking Techniques
- Footprinting through Social Networking Sites
- Understanding different techniques for Website Footprinting
- Understanding different techniques for Email Footprinting
- Understanding different techniques of Competitive Intelligence



- Understanding different techniques for WHOIS Footprinting
- Understanding different techniques for DNS Footprinting
- Understanding different techniques for Network Footprinting
- Understanding different techniques of Footprinting through Social Engineering
- Footprinting Tools
- Footprinting Countermeasures
- Overview of Footprinting Pen Testing



Flow



**Footprinting
Concepts**



**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



**Footprinting
Penetration
Testing**

What is Foot printing?

- Footprinting is the process of **collecting as much information as possible about a target network**, for identifying various ways to intrude into an organization's network system
- Footprinting is the first step of any attack on information systems; attacker gathers **publicly available sensitive information**, using which he/she performs social engineering, system and network attacks, etc. that leads to huge financial loss and loss of business reputation

Know Security Posture

Reduce Focus Area

Identify Vulnerabilities

Draw Network Map

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

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

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

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

Objective of Foot printing

Collect Network Information

- Domain name
- Internal domain names
- Network blocks
- IP addresses of the reachable systems
- Rogue websites/private websites
- TCP and UDP services running
- Access control mechanisms and ACL's
- Networking protocols
- VPN Points
- IDSees running
- Analog/digital telephone numbers
- Authentication mechanisms
- System enumeration

Collect System Information

- User and group names
- System banners
- Routing tables
- SNMP information
- System architecture
- Remote system type
- System names
- Passwords



Collect Organization's Information

- Employee details
- Organization's website
- Company directory
- Location details
- Address and phone numbers
- Comments in HTML source code
- Security policies implemented
- Web server links relevant to the organization
- Background of the organization
- News articles
- Press releases

Module Flow



**Footprinting
Concepts**



**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



**Footprinting
Penetration
Testing**

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Footprinting through Search Engines

- Attackers use search engines to **extract information about a target** such as technology platforms, employee details, login pages, intranet portals, etc. which helps in performing social engineering and other types of advanced system attacks
- **Search engine caches** and **internet archives** may also provide sensitive information that has been removed from the World Wide Web (WWW)



This is Google's cache of <http://en.wikipedia.org/wiki/Microsoft>. It is a snapshot of the page as it appeared on 5-Sep-2013 03:31:45 GMT. The [current page](#) could have changed in the meantime. [Learn more](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘+F** (Mac) and use the find bar

[Text only version](#)

Create account Log in

Article Talk Read View source View history Search

WIKIPEDIA The Free Encyclopedia

Main page Content Featured content Current events Random article Donate to Wikipedia Help About Wikipedia Community portal Recent changes Contact page Toolbox Print/export Languages Afrikaans Alemannisch

Let your voice be heard! Give your input on the draft of our new privacy policy. [Help with translation](#)

Microsoft

From Wikipedia, the free encyclopedia

Microsoft Corporation is an American multinational software corporation headquartered in Redmond, Washington that develops, manufactures, licenses, and supports a wide range of products and services related to computing. The company was founded by Bill Gates and Paul Allen on April 4, 1975. Microsoft is the world's largest software maker measured by revenues.^[1] It is also one of the world's most valuable companies.^[2]

Microsoft was established to develop and sell BASIC interpreters for the Altair 8800. It rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by the Microsoft Windows line of operating systems. The company's 1986 initial public offering, and subsequent rise in its share price, created an estimated three billionaires and 12,000 millionaires from Microsoft employees. Since the 1990s, it has increasingly diversified from the operating system market and has made a number of corporate acquisitions. In May 2011, Microsoft acquired Skype Technologies for \$8.5 billion in its largest acquisition to date.^[3] As of 2013, Microsoft is market dominant in both the PC operating system and office suite markets (the latter with Microsoft Office). The company also produces a wide range of other

Coordinates: 47°32'23.00"N 122°14'2.87"W

Microsoft Corporation

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



Determining the Operating System

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

Search Web by Domain

Explore 1,476,698 web sites visited by users of the Netcraft Toolbar 1st October 2013

Search: search tips
site contains lookup! example site contains .netcraft.com

Results for microsoft

First 500 sites returned

| Site | Site Report | First seen | Netblock | OS |
|---------------------------------|-------------|----------------|----------------------------|---------------------|
| 1. www.microsoft.com | | august 1995 | ms hotmail | citrix netscaler |
| 2. go.microsoft.com | | november 2001 | ms hotmail | windows server 2008 |
| 3. support.microsoft.com | | october 1997 | microsoft corporation | unknown |
| 4. technet.microsoft.com | | august 1999 | microsoft corporation | windows server 2003 |
| 5. windows.microsoft.com | | june 1998 | microsoft corporation | unknown |
| 6. msn.microsoft.com | | september 1998 | microsoft corporation | windows server 2003 |
| 7. social.technet.microsoft.com | | august 2008 | microsoft corporation | citrix netscaler |
| 8. answers.microsoft.com | | august 2005 | microsoft limited | windows server 2008 |
| 9. office.microsoft.com | | november 1998 | microsoft corporation | windows server 2008 |
| 10. social.msn.microsoft.com | | august 2008 | microsoft corporation | citrix netscaler |
| 11. download.microsoft.com | | august 1995 | animal technologies | linux |
| 12. login.microsoftonline.com | | december 2010 | microsoft corporation | windows server 2008 |
| 13. www.microsoftstore.com | | november 2008 | digital river ireland ltd. | fs big-ip |
| 14. search.microsoft.com | | january 1997 | animal technologies | linux |
| 15. www.update.microsoft.com | | may 2007 | microsoft corporation | windows server 2008 |
| 16. o15.officedir.microsoft.com | | may 2012 | microsoft corporation | fs big-ip |
| 17. r.office.microsoft.com | | november 2003 | microsoft corporation | windows server 2008 |

| Hosting History | | | | | |
|--|-------------------------|------------------|-------------------|-------------------|---------------------|
| Netblock owner | IP address | OS | Web server | Last seen | |
| Microsoft Corp One Microsoft Way Redmond WA US 98052 | 65.55.18.201 | unknown | Microsoft-IIS/7.5 | 30-Sep-2013 | |
| MS Hotmail One Microsoft Way Redmond WA US 98052 | 64.4.11.37 | unknown | Microsoft-IIS/7.5 | 4-May-2013 | |
| Microsoft Corp One Microsoft Way Redmond WA US 98052 | 65.55.58.201 | Citrix Netscaler | Microsoft-IIS/7.5 | 14-Apr-2013 | |
| MS Hotmail One Microsoft Way Redmond WA US 98052 | 64.4.11.37 | unknown | Microsoft-IIS/7.5 | 12-Apr-2013 | |
| Microsoft Corp One Microsoft Way Redmond WA US 98052 | 65.55.58.201 | Citrix Netscaler | Microsoft-IIS/7.5 | 11-Apr-2013 | |
| MS Hotmail One Microsoft Way Redmond WA US 98052 | 64.4.11.37 | unknown | Microsoft-IIS/7.5 | 10-Apr-2013 | |
| Microsoft Corp One Microsoft Way Redmond WA US 98052 | 65.55.58.201 | Citrix Netscaler | Microsoft-IIS/7.5 | 9-Apr-2013 | |
| MS Hotmail One Microsoft Way Redmond WA US 98052 | 64.4.11.37 | unknown | Microsoft-IIS/7.5 | 8-Apr-2013 | |
| Microsoft Corp One Microsoft Way Redmond WA US 98052 | 65.55.58.201 | Citrix Netscaler | Microsoft-IIS/7.5 | 7-Apr-2013 | |
| MS Hotmail One Microsoft Way Redmond WA US 98052 | 64.4.11.37 | unknown | Microsoft-IIS/7.5 | 6-Apr-2013 | |
| Rank | Site | Organisation | First Seen | Webserver | OS |
| - | www.emcarta.com | unknown | July 1995 | Microsoft-IIS/7.5 | Windows Server 2008 |
| 358 | modn.microsoft.com | unknown | September 1998 | Microsoft-IIS/8.0 | Citrix Netscaler |
| 245 | technet.microsoft.com | unknown | August 1999 | Microsoft-IIS/8.0 | Citrix Netscaler |
| - | www.microsoft.be | unknown | February 1999 | Microsoft-IIS/7.5 | unknown |
| - | adreport.msn.com | unknown | March 2000 | BigIP | F5 BIG-IP |
| - | www.solomon.com | unknown | October 1995 | Microsoft-IIS/7.5 | Windows Server 2008 |
| 183106 | www.rhn.co.uk | unknown | June 1997 | Microsoft-IIS/8.0 | Windows Server 2012 |
| - | www.microsoft.com | unknown | April 1999 | Microsoft-IIS/7.5 | Windows Server 2008 |
| 138898 | www.microsoft.com | unknown | July 2008 | Microsoft-IIS/7.0 | Windows Server 2008 |
| - | ads.msn.com | unknown | January 1997 | Microsoft-IIS/7.5 | unknown |
| - | www@hotmail.com | unknown | September 1999 | Microsoft-IIS/7.5 | Windows Server 2008 |
| 191698 | Watson.Microsoft.Com | unknown | March 2002 | Microsoft-IIS/8.0 | unknown |
| 425919 | schemas.xmlsoap.org | unknown | November 2001 | Microsoft-IIS/7.5 | unknown |
| - | bitalk.org | unknown | March 2000 | Microsoft-IIS/7.5 | unknown |
| - | activedesk.msn.com | unknown | April 1998 | Microsoft-IIS/7.5 | Citrix Netscaler |
| - | ads.jp.msn.com | unknown | August 1999 | Microsoft-IIS/7.5 | unknown |
| 315876 | technet.com | unknown | February 2010 | Microsoft-IIS/7.5 | unknown |
| 17708 | www.meistergooddeal.com | unknown | May 2000 | Microsoft-IIS/7.5 | Windows Server 2008 |
| - | mobile.msn.com | unknown | March 2000 | Microsoft-IIS/6.0 | unknown |

Determining the Operating System

(Cont'd)

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



Shodan Exploits Scanhub Research Anniversary Promotion

SHODAN [mitmattack.com](#)

Did you mean: [hostnamemicrosoft.com](#)

Services

| Service | Count |
|----------------|-------|
| HTTP | 2,700 |
| SNMP | 77 |
| FTP | 34 |
| HTTP Alternate | 30 |
| POP3 | 24 |

Top Countries

| Country | Count |
|----------------|-------|
| United States | 1,844 |
| China | 101 |
| Germany | 100 |
| United Kingdom | 97 |
| Taiwan | 82 |

Too Cities

| City | Count |
|----------------|-----------|
| Redmond | 463 |
| 70 | 70 |
| 54 | 54 |
| 42 | 42 |
| 33 | 33 |
| Windows 7 or 8 | 64,420,79 |
| MS Hotmail | 410 |
| Microsoft.com | 395 |
| 101 | 101 |
| 75 | 75 |
| 57 | 57 |

Disclosure: [Mitmsec...](#)

ME
and stay up to date
with the latest features of Shodan.

Object moved

201.19.66.138
Over The River Fly
Actions (13 of 20)


HTTP/1.1 302 Object moved
Date: Mon, 24 Sep 2012 20:38:50 GMT
Content-Type: text/html
Location: http://www.microsoft.com/en-us/banners/PX101049612.aspx
Server: Microsoft-IIS/7.5
Via: Cache, ASP.NET/4.0.30319.14929/CRSTUDIONE/EPG00RAID8MJCJCD09F0J0I/pw...
X-Powered-By: ASP.NET
Date: Sun, 23 Sep 2012 20:38:50 GMT

302 Found

306.162.152.143
Gringo Editorial Since 198
Actions (10 of 20)


HTTP/1.1 302 Found
Date: Sat, 28 Sep 2012 20:34:18 GMT
Server: Apache/2.2.17 (Ubuntu) PHP/5.4.17
Location: http://www.vandergrifts.musmus.it/home
Content-Length: 218
Content-Type: text/html; charset=UTF-8
Content-Length: 44

64.4.20.79

Windows 7 or 8
MS Hotmail
Actions (20 of 20)


HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: image/gif
Expires: -1
Server: Microsoft-IIS/7.5
Via: Cache, MCI=>OLD=>7ad848f11d4c811d4d2d48e1b6d8HASH=FBABLV-211P...
X-Powered-By: ASP.NET
PAP: CWP-CAD-DEP-TAN-QUR-EDN-PWY-ONL-UCD-PUR-COM-NXV-INT-DRM-CNT-
Date: Sun, 23 Sep 2012 20:31:18 GMT
Content-Length: 44

247.37.179.405

BT
Actions (10 of 20)


http://247.37.179.405/~addr@shapecontrol.com

HTTP/1.1 302
Date: Sun, 23 Sep 2012 20:31:31 GMT
Server: Microsoft-IIS/6.0
Microsoft-DiamondPrint-Server: 4.0.2.5488
X-Powered-By: ASP.NET
Location: /default.aspx
Cache-Control: private
Content-Length: 9
PAPL-Resource: http://schemas.microsoft.com/2003/10/.../http://schemas.microsoft.com/2003/10/...

Collect Location Information

Google Earth

Use **Google Earth** tool to get the physical location of the target



<http://www.google.com>

Tools for finding the geographical location

Google Maps

<https://maps.google.com>

Wikimapia

<http://www.wikimapia.org>

National Geographic Maps

<http://maps.nationalgeographic.com>

Yahoo Maps

<http://maps.yahoo.com>

Bing Maps

<http://www.bing.com/maps>

People Search: Social Networking Sites/People Search Services

- Social networking sites are the great source of personal and organizational information
 - Information about an individual can be found at various **people search websites**
 - The people search returns the following **information about a person or organization**:



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



in

Discover people, jobs, companies, and more

Profile Network Jobs Interests Advanced Search Business Services Update

View the world's largest inventory of Certified Reference Standards. [Read More](#)

Bill Gates
Co-chair, Bill & Melinda Gates Foundation
Greater Seattle Area - Philanthropy

Formerly: Bill & Melinda Gates Foundation, Microsoft, Harvard University

Follow [Follow](#) Connect [View 690,928 Pages](#)

www.linkedin.com/in/billgates

Published by Bill

We Need Our Brightest People Working on Our... [Read More](#)

August 26, 2010

Three Things I've Learned From Warren Buffett [Read More](#)

June 13, 2010

More Influencers

Gretchen Rubin
Best-selling author, Blogger, www.HappierNow.com
[+ Follow](#)

Grew Your Career By Following
Bill & Melinda Gates Foundation

BAUGAT get the latest on Bill & Melinda Gates Foundation Job, News & more! [+ Follow](#)

People Also Viewed

 **Barack Obama**
President of the United States of America

<http://www.linkedin.com>

<https://pipl.com>

People Search Online Services



AnyWho
<http://www.anywho.com>



US Search
<http://www.ussearch.com>



Intelius
<http://www.intelius.com>



411
<http://www.411.com>



PeopleFinders
<http://www.peoplefinders.com>



PeopleSmart
<http://www.peoplesmart.com>



Veromi
<http://www.veromi.net>



PrivateEye
<http://www.privateeye.com>



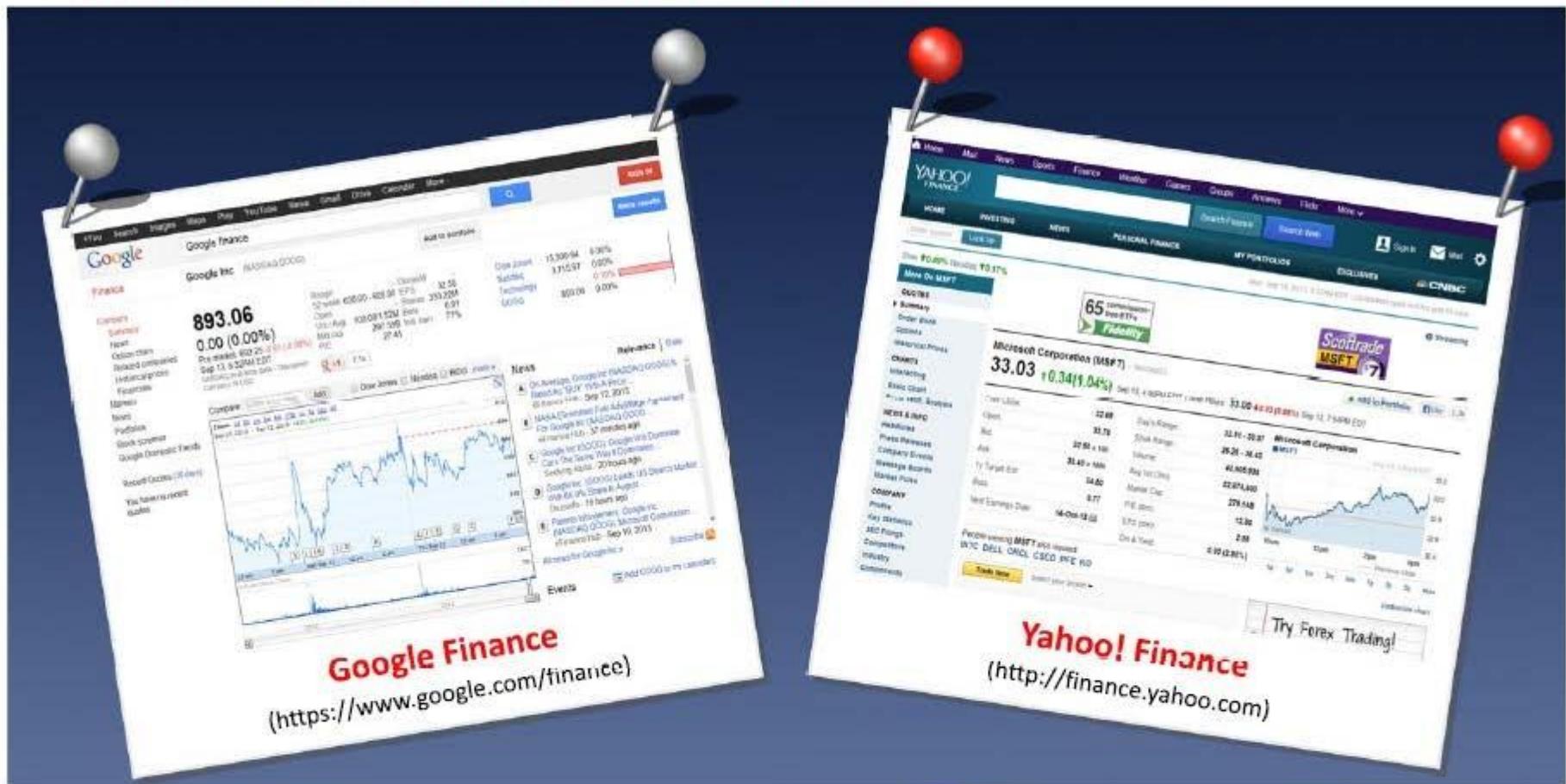
People Search Now
<http://www.peoplesearchnow.com>



Public Background Checks
<http://www.publicbackgroundchecks.com>

Gather 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.



Footprinting through Job Sites

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

Enterprise Applications Engineer/DBA

About Us:

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

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

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

Job Description:

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

Job Knowledge and Skills:

Position requires strong knowledge of Windows server 2003/2008 Active Directory administration and networking (TCP/IP 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

- ⌚ <http://www.linkedin.com>
- ⌚ <http://www.monster.com>
- ⌚ <http://www.careerbuilder.com>
- ⌚ <http://www.dice.com>
- ⌚ <http://www.simplyhired.com>
- ⌚ <http://www.indeed.com>
- ⌚ <http://www.usajobs.gov>



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 is a search bar with the placeholder "Search for groups or messages". Below the search bar, there is a message: "Access to public Google Groups has been restricted by your domain admin". There are two main buttons: "My groups" (with a green and blue icon) and "Browse all" (with a blue icon). On the left, there is a sidebar with "Groups" and "My groups" sections, and a "Favorites" section with a yellow call-to-action button that says "Click on a group's star icon to add it to your favorites". The main content area has several sections: "All of your discussions in one place", "Express yourself", "People power discussions", "Speed matters", and "Discuss from anywhere". Each section contains a brief description and a link to more information.

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Footprint Using Advanced Google Hacking Techniques

Query String

Google hacking refers to **creating complex search queries** in order to extract sensitive or hidden information



Vulnerable Targets

It helps attackers to **find vulnerable targets**



Google Operators

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





Google Dorks

- A Google dork query, sometimes just referred to as a dork, is a search string or custom query that uses advanced search operators to find information not readily available on a website.
- Google dorking, also known as Google hacking, can return information difficult to locate through simple search queries.
- There are different places to find ready to use Google Dorks. The first place is Google Hacking Database. This is a free public database containing thousands of Google Dorks for finding sensitive publicly available information



Is It legal ?

- Google dorking is completely legal —
- it's just another form of searching after all.
- Google was built to handle advanced searches, and banning this functionality would limit information access.

Google Dorks

A Google dork is an employee who unknowingly exposes sensitive corporate information on the Internet. The word dork is slang for a slow-witted or in-ept person.

Margaret Rouse

Director, WhatIs.com at TechTarget



Purpose of Dorks Queries

WHAT

Google dorks is a powerful advanced search, an instrument to perform queries on Google search engine.

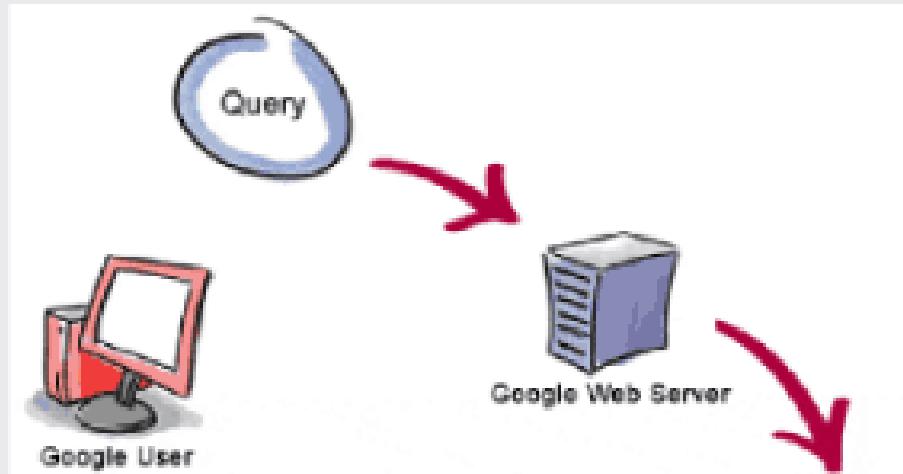
HOW

That queries allows the user to find detailed information over the internet, such files, hidden pages, sensitive documents and so on.

WHY

But...dork queries are considered by many an "hacking technique". Because of his nature, the dorks can be used for different purposes, often **bad purpose** and we shall then see...

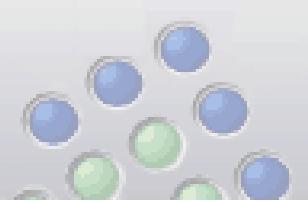
How Google works



3. The search results are returned to the user in a fraction of a second.

1. The web server sends the query to the index servers. The content inside the index servers is similar to the index in the back of a book--it tells which pages contain the words that match any particular query term.

2. The query travels to the doc servers, which actually retrieve the stored documents. Snippets are generated to describe each search result.



Special Characters

CYBER SECURITY



Star [*]

Substitution with
any other word in
the query

Tilde [~]

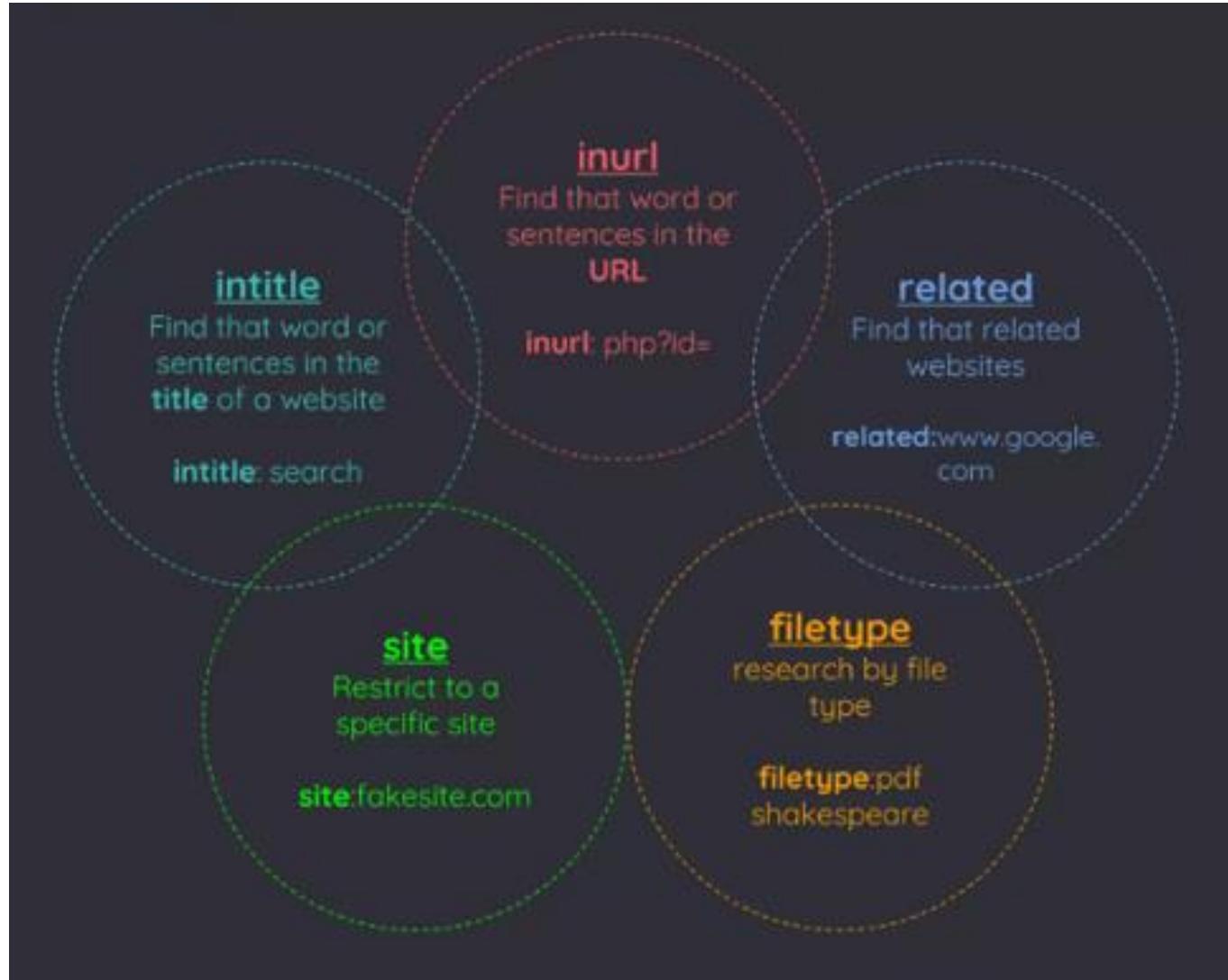
Also research
synonyms of that
word

Minus [-]

Remove that word
from the research



Operators



● Google Hacking Database - Exploit Database

The Exploit Database is maintained by [Offensive Security](#), an information security training company that provides various Information Security Certifications as well as high end penetration testing services. Categories of dork queries by [GHDB](#):

- Footholds
- Files Containing Usernames
- **Sensitive Directories**
- Web Server Detection
- Vulnerable Files
- **Vulnerable Servers**
- Error Messages
- Files Containing Juicy Info
- **Files Containing Passwords**
- Sensitive Online Shopping Info
- Network or Vulnerability Data
- **Pages Containing Login Portals**
- Various Online Devices
- Advisories and Vulnerabilities

Let's see those underlined...

File containing passwords example

site: [REDACTED].com intext:@gmail.com | @yahoo.com | @hotmail.com dat

Tutti Notizie Shopping Video Altro Impostazioni Strumenti

Circa 34.500 risultati (0,74 secondi)

kathryndaniels@gmail.com: [REDACTED] m.vroom@gmail.com ...
[REDACTED] com/sDpyATHX ▾ Traduci questa pagina
10 set 2016 - m.vroom@gmail.com: [REDACTED] amelia.a.presley@gmail.com: [REDACTED]
chriswpalm@gmail.com: [REDACTED] micah1powell@gmail.com: ...

@Gmail.com - [REDACTED].com
[REDACTED] com/jWuGDPhn ▾ Traduci questa pagina
10 nov 2016 - kodi022@yahoo.com: [REDACTED] ztaxen@hotmail.com: [REDACTED] gps.sadala@
hotmail.com: [REDACTED] pranay.rana@gmail.com: [REDACTED]

@gmail.com - [REDACTED].com
[REDACTED] com/2BShU14Z ▾ Traduci questa pagina
17 mar 2016 - christophercampion@yahoo.com: [REDACTED] rakesh_kalia_vancouver@hotmail.
com: [REDACTED] thmsmith@gmail.com: [REDACTED]

List of pastes (username and password). Check your email status on haveibeenpwned.com by **Troy Hunt**.

- Pages containing login portal example

Google search results for the query `site:www.comune.*.* inurl:login`:

Tutti Immagini Notizie Video Maps Altra Impostazioni Strumenti

Circa 6.420 risultati (0,42 secondi)

login - Comune di Mercato Saraceno
www.comune.mercatosaraceno.fc.it/login ▾
Torna alla Home | Testo più piccolo Testo piccolo | Testo normale | Testo più grande Testo grande | Versione grafica | Solo testo | Alto contrasto |.

Login / Utente - Comune di Riva del Garda
www.comune.rivadelgarda.tn.it/user/login?url=
Comune di Riva del Garda. Login: Ricordami. Login. Hai dimenticato la password? © 2016 Comune di Riva del Garda powered by ComunWEB con il supporto ...

[site:www.comune.*.* inurl:login](#)

In this case, the star character have been changed with “.fc” and “.it” domain in the first one, and “.tn” and “.it” for the second one.

Vulnerable server example

The screenshot shows a Google search results page with the query "inurl:index.php?id=". The search bar has the query "inurl:index.php?id=" entered. Below the search bar, there are navigation links for "Tutti", "Shopping", "Notizie", "Video", "Libri", "Altro", "Impostazioni", and "Strumenti". A status message indicates "Circa 545.000.000 risultati (0,67 secondi)". The search results list three entries:

- Visual Artist - Salla Tykkä - Power**
www.sallatykka.com/web/index.php?id=31 ▾ Traduci questa pagina
Salla Tykkä was born in 1973 in Helsinki, Finland, where she lives and works today. She graduated from the Academy of Fine Arts in Helsinki 2003. She has ...
- Visual Artist - Salla Tykkä - Retrospective - Salla Tykka**
sallatykka.com/web/index.php?id=21 ▾ Traduci questa pagina
Salla Tykkä was born in 1973 in Helsinki, Finland, where she lives and works today. She graduated from the Academy of Fine Arts in Helsinki 2003. She has ...
- Provincia di Grosseto**
www.provincia.grosseto.it/index.php?id=183 ▾
Una descrizione per questo risultato non è disponibile a causa del file robots.txt di questo sito
Ulteriori informazioni

inurl:index.php?id=

Looking for SQL Injection point on the websites.

The following websites *could be* affected by this vulnerability !

Sensitive directory example

The screenshot shows a Google search results page. The search query is "inurl:admin inurl:uploads". The results are filtered under the "Tutti" tab. It displays approximately 535,000 results found in 0.49 seconds. A suggestion is shown: "Suggerimento: Cerca risultati solo in Italiano. Puoi specificare la lingua di ricerca in Preferenze." Below the suggestion, two search results are listed:

- Index of /admin/uploads - Mediamax**
www.mediamaxargentina.com/admin/uploads/ ▾ Traduci questa pagina
Index of /admin/uploads. Parent Directory . 1/ . 10/ . 13/ . 15/ . 16/ . 8/ . 9/
- Index of /rivista/admin/uploads - Senzacornice**
senzacornice.org/rivista/admin/uploads/ ▾
Index of /rivista/admin/uploads. Parent Directory .DS_Store .archivio/ articoli/ artisti/ pdf/ .prossimo/

[inurl:admin inurl:uploads](#)

The following folders probably contains sensitive data !

DEMO



1. *Finding exposed FTP servers*

- Google can index open FTP servers. Use the following Google Dork to find open FTP servers.
- [intitle:"index of" inurl:ftp](#)
- To make the query more interesting, we can add the "intext" Google Dork, which is used to locate a specific word within the returned pages

https://www.google.com/advanced_search

DEMO



2. *Find email lists*

- It is relatively easy to find email lists using Google Dorks. In the following example, we are going to find text files that contain email lists.
- [filetype:txt inurl:"email.txt"](#)

DEMO



3. *Getting live streams of Cameras*

- Live cameras We can use Google to find open cameras that are not access restricted by IP address. The following Google dorks retrieve live cameras web pages.
- [inurl:"view.shtml" "Network Camera"](#)
- ["Camera Live Image" inurl:"guestimage.html"](#)

DEMO: Finding Passwords



- Finding passwords is the most attractive task for both legitimate and ill-intentioned online searchers. The following Google Dorks retrieve exposed passwords.
- [site:pastebin.com intext:admin.password](#)
(find the text "admin.password" in the Pastebin website; this site is used by hackers to publish sensitive leaked information)
- ["admin password" ext:txt | ext:log | ext:cfg](#)
(find the text “admin-password” in exposed files of the following types: TXT, LOG, CFG)
- [filetype:log intext:password after:2016 intext:@gmail.com | @yahoo.com | @hotmail.com](#)
(search for all files of type "log" that contain the word "password" within them, are indexed after 2016, and contain any of the following text in their body: @gmail.com, @yahoo.com, or @hotmail.com)



Some Examples of Dorking Queries

- 1) site:static.ow.ly/docs/ intext:@gmail.com | Password
- 2) filetype:sql intext:wp users phpmyadmin
- 3) intext:"Dumping data for table orders"
- 4) "Index of /wp-content/uploads/backupbuddy backups" zip
- 5) Zixmail inurl:/s/login?
- 6) inurl:/remote/login/ intext:"please login" | intext:"FortiToken clock drift detected"
- 7) inurl:/WebInterface/login.html
- 8) inurl:dynamic.php?page=mailbox
- 9) inurl:/sap/bc/webdynpro/sap/ | "sap-system-login-oninputprocessing"
- 10) intext:"Powered by net2ftp"

Google Advance Search Operators

Google supports several advanced operators that help in modifying the search

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

Google Hacking Databases

The screenshot shows a web browser window displaying the GHDB - Hackers For Charity website. The page features a banner for "HACKERS FOR CHARITY.ORG" and a search bar. Below the search bar is a table titled "GHDB :: Advisors and Vulnerabilities". The table lists several entries:

| Date | Title | Summary |
|------------|--|--|
| 2004-01-04 | EarlyImpact Productcart | The EarlyImpact Productcart contains multiple vulnerabilities, which could exploited to allow an attacker to steal user credentials or mount other attacks ... |
| 2004-03-04 | missSearch vulnerability | According to Http://www.securityfocus.com/bid/16567 , certain versions of missSearch contain a buffer overflow vulnerability which allow an attacker to ... |
| 2004-05-12 | intelle guestbook, "advanced guestbook 2.2 now..." | Advanced Guestbook v2.2 has an SQL injection problem which allows unauthorized access. Attacking from there, hit 'Admin' then do the following ... |
| 2004-06-25 | VP-ASP Shopping Cart XSS | VP-ASP (Virtual Programming - ASP) has won awards both in the US and France. It is now in use in over 70 countries. VP-ASP can be used to build any type of ... |

Google Hacking Database (GHDB)

<http://www.hackersforcharity.org>

The screenshot shows a web browser window displaying the Google Hacking Database (GD) website. The page has a dark theme with red and white text. At the top, it says "Welcome to the google hacking database". Below that is a search bar with "Search Google Dorks" and a dropdown for "Category: All". To the right is a "Free text search:" input field and a "Search" button. The main content area is titled "Latest Google Hacking Entries" and shows a list of recent findings. On the right side, there's a sidebar titled "Google Hacking Database Categories" with a section for "Footholds (31)".

Google Dorks

<http://www.exploit-db.com>

Information Gathering Using Google Advanced Search

Use Google Advanced Search option to find sites that may link back to the target company's website

This may extract information such as partners, vendors, clients, and other affiliations for target website

With Google Advanced Search option, you can search web more precisely and accurately

The screenshot shows the Google Advanced Search interface. At the top, the URL is https://www.google.com/advanced_search?hl=en&lg=1. Below the address bar, the Google logo is visible. The main title is "Advanced Search". The search form includes fields for "Find pages with..." (containing "target"), "language" (set to "any language"), "reading level" (set to "no reading level displayed"), and "file type" (set to "any format"). There are also dropdown menus for "region" (set to "any region") and "last update" (set to "anytime"). Other options include "site or domain", "terms appearing", "SafeSearch" (set to "Show most relevant results"), and "usage rights" (set to "not filtered by license"). A blue "Advanced Search" button is located at the bottom right.

Google

Conclusion

Actually the best way to protect us against Google hacking, is to test our website to figure out what could harm us, then patch/fix/remove the problem if possible.

As we can see, it's not difficult to find sensitive folders or file over the network. Because of his simplicity, security skills are not required to steal information.



Be careful and protect your data!

Footprinting Methodology

- 1 Footprinting through Search Engines
- 2 Footprinting Using Advanced Google Hacking Techniques
- 3 Footprinting through Social Networking Sites
- 4 Website Footprinting
- 5 Email Footprinting
- 6 Competitive Intelligence
- 7 WHOIS Footprinting
- 8 DNS Footprinting
- 9 Network Footprinting
- 10 Footprinting through Social Engineering

Collect Information through Social Engineering on Social Networking Sites



Attackers use social engineering trick to gather sensitive information from social networking websites such as **Facebook**, **MySpace**, **LinkedIn**, **Twitter**, **Pinterest**, **Google+**, etc.



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

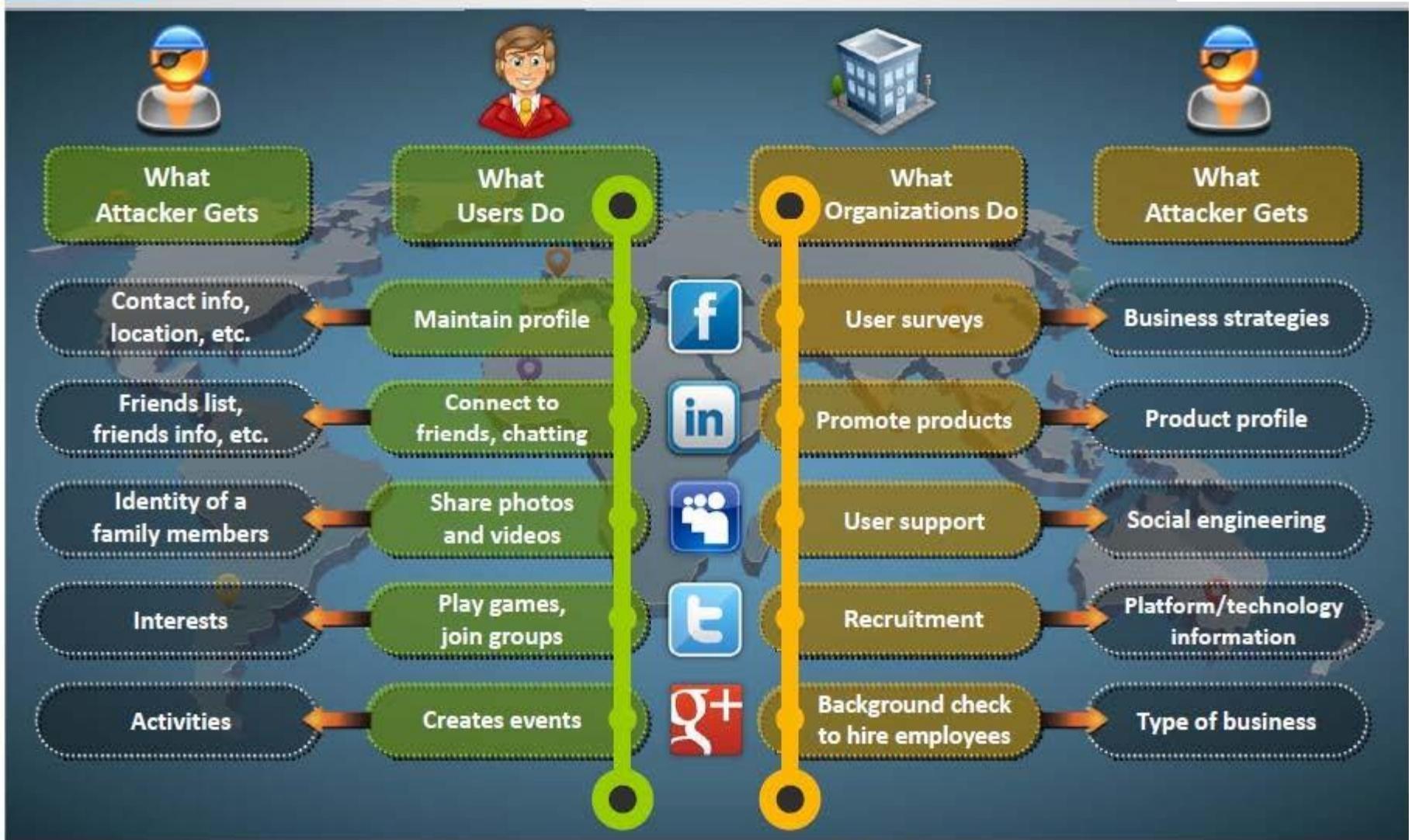


Employees may **post personal information** such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.



Attackers collect information about employee's interests by **tracking their groups** and then trick the employee to reveal more information

Information Available on Social Networking Sites



Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Website Footprinting

1

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



2

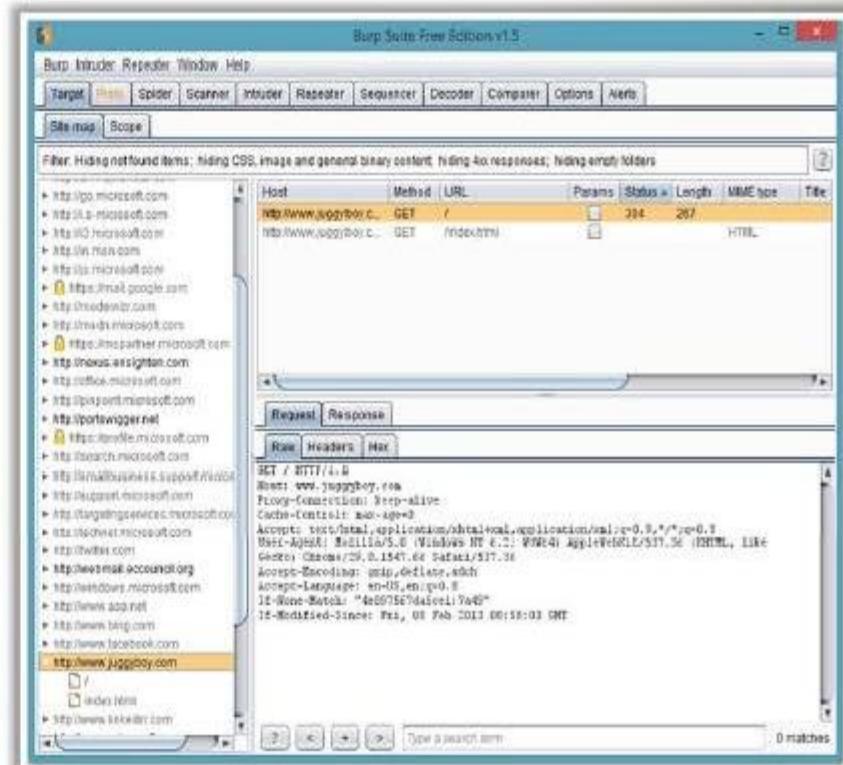
Browsing the target website may provide:

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

3

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

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



Website Footprinting

(Cont'd)

Examining HTML source provide:

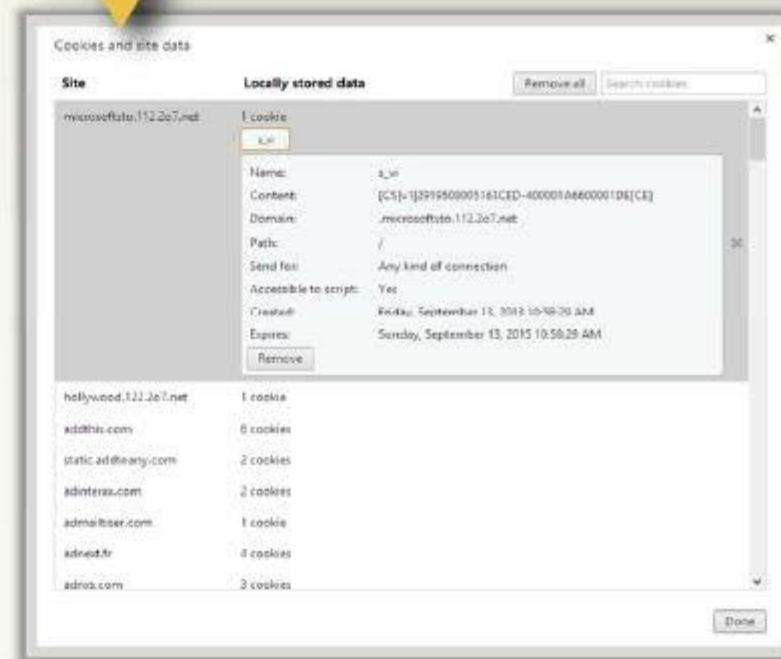
- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type



A screenshot of Microsoft Internet Explorer displaying the source code of a Microsoft website. The code includes standard HTML tags like <head> and <title>, as well as numerous CSS and JavaScript files being linked from the page. A copyright notice at the bottom states: "Microsoft Home Page | Devices and Services © 2015 Microsoft Corporation. All rights reserved. This product contains software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)".

Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used



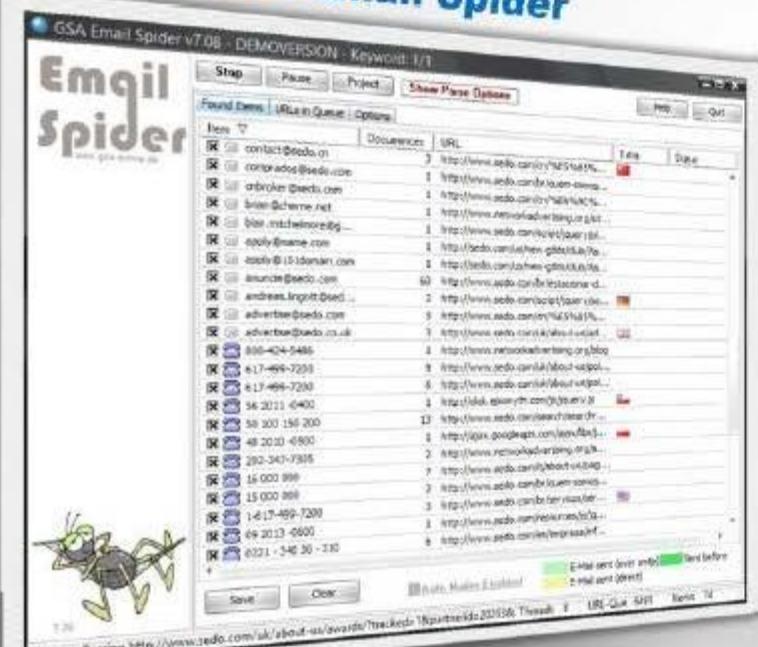
A screenshot of a 'Cookies and site data' dialog box. It shows a list of sites and their cookie counts. The top entry is 'microsoftto.112.207.net' with 1 cookie. The cookie details are as follows:

| Name | Value | Content | Domain | Path | Send for | Accessible to script | Created | Expires |
|-------|------------|------------|-------------------------|------|------------------------|----------------------|--|--|
| __utn | [REDACTED] | [REDACTED] | microsoftto.112.207.net | / | Any kind of connection | Yes | Friday, September 18, 2015 10:59:29 AM | Sunday, September 13, 2015 10:59:28 AM |

Other sites listed include 'hollywood.112.207.net' (1 cookie), 'edothis.com' (6 cookies), 'static.adthearty.com' (2 cookies), 'hdinteras.com' (2 cookies), 'adminUser.com' (1 cookie), 'adreal.fr' (8 cookies), and 'adns.com' (3 cookies).

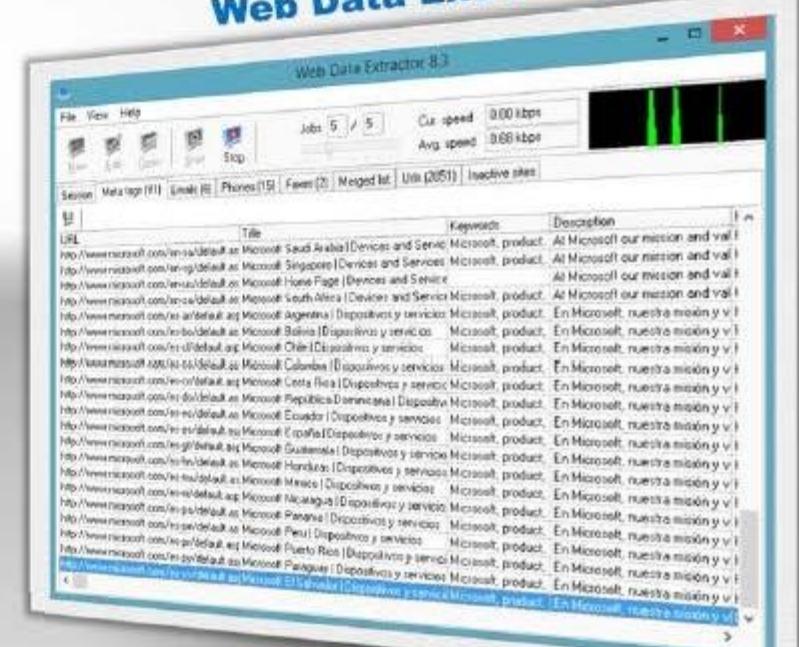
Website Footprinting using Web Spiders

- 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**



GSA Email Spider
www.gsa-online.de

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



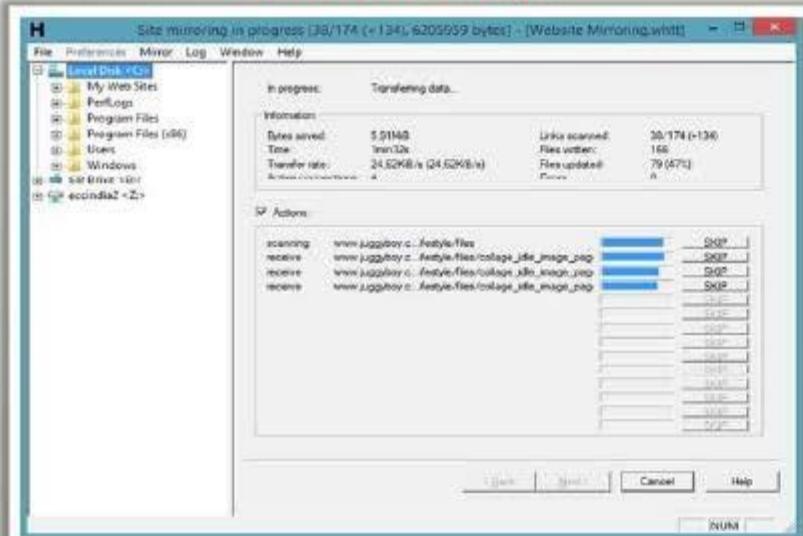
Web Data Extractor
www.webextractor.com

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

HTTrack Web Site Copier



(<http://www.httrack.com>)

SurfOffline



(<http://www.surfoffline.com>)

Website Mirroring Tools



BlackWidow

<http://softbytelabs.com>



NCollector Studio

<http://www.calluna-software.com>



Website Ripper Copier

<http://www.tensons.com>



Teleport Pro

<http://www.tenmax.com>



Portable Offline Browser

<http://www.metaproducts.com>



PageNest

<http://www.pagenest.com>



Backstreet Browser

<http://www.spadixbd.com>



Offline Explorer Enterprise

<http://www.metaproducts.com>



GNU Wget

<http://www.gnu.org>



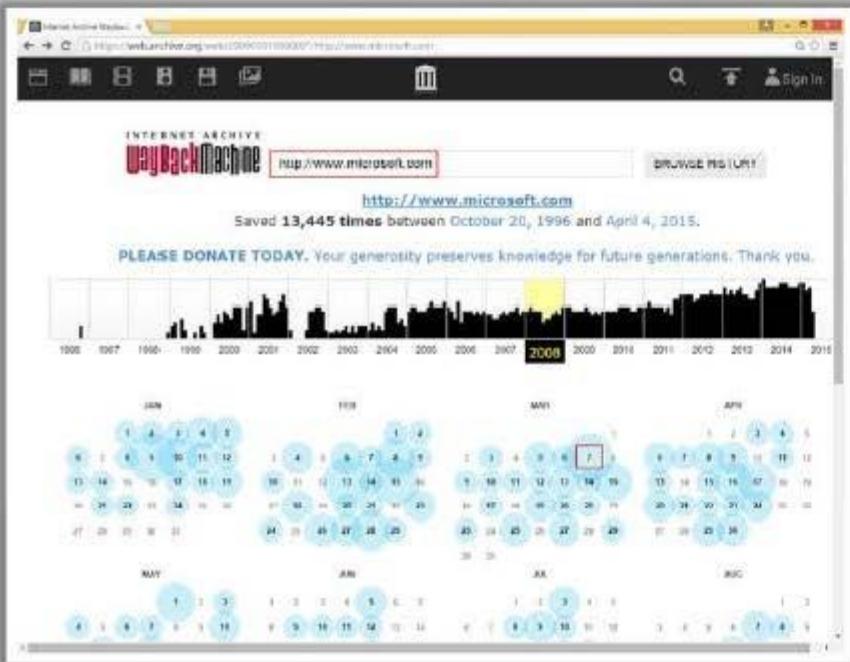
Hooeey Webprint

<http://www.hooeeywebprint.com>

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

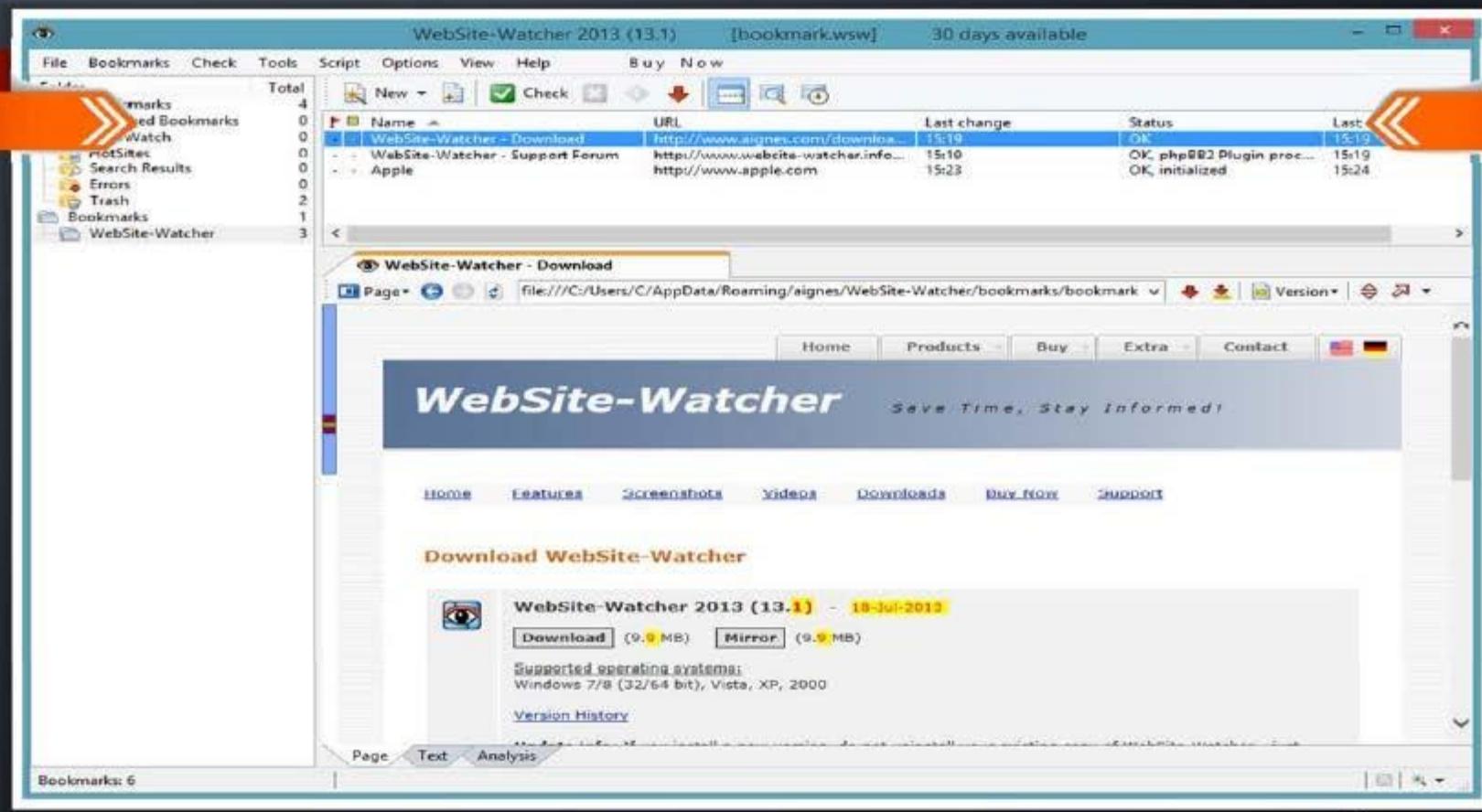


Internet Archive's Wayback Machine allows you to visit **archived versions** of websites



Monitoring Web Updates Using Website-Watcher

Website-Watcher automatically checks web pages for updates and changes



<http://aignes.com>

Web Updates Monitoring Tools



Change Detection

<http://www.changedetection.com>



Follow That Page

<http://www.followthatpage.com>



Page2RSS

<http://page2rss.com>



Watch That Page

<http://www.watchthatpage.com>



Check4Change

<https://addons.mozilla.org>



OnWebChange

<http://onwebchange.com>



Infominder

<http://www.infominder.com>



TrackedContent

<http://trackedcontent.com>



Websnitcher

<http://websnitcher.com>



Update Scanner

<https://addons.mozilla.org>

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Collecting Information from Email Header

Delivered-To: [REDACTED]@gmail.com
Received: by 10.112.39.167 with SMTP id q7c...
Sat, 1 Jun 2013 21:24:01 -0700 (PDT)
Return-Path: <[REDACTED]erma@gmail.com>
Received-SPF: pass (google.com: domain of [REDACTED]
sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=pass
10.224.205.137 as permitted sender) smtp.mail
header.i=[REDACTED]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
by 10.224.205.137 with SMTP id fa9mr8570570qab.39.1
Sat, 01 Jun 2013 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=TGEIPb4ti7gfQG+ghh70kPjkx+Tt/iAC1
b=KguZLTLfg2+QZXzKex1NnvRcnD/+P4+Nk5NKSpTg7uHXd9fv/hGH46e2P+75MxD
b1PK3ej3UF/CsaBZWDT0XLaK0AGrP3BoT92MCZFxeUUQ9uwL/xHALSneUEEEeKGqOC
oa9hd59D3oXI8KAC7ZmkblGzXmV4D1WffCL894RaMBOUoMzRwOWWlib95a1I38cqtlfP
ZhrWFKh5xSn2XsE73x2PEYzp7yecCeQuYHZNGs1Kxc07xQjeZuw+HWK/vR6xChDap24
K5ZAfyZmkIKF+VdLZqu7YGFzy6oHcuP16yS/C2fxHVdsuYamMT/yecvhCVo8Og7FKt6
/Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9m...
Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Sat, 1...
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhIE4Ber2...v...>
References: <CAOYWATT1zdDXE3o8D2rhIE4Ber2MtV0uhro6r+7Mu7c8ubp8Eg@mail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAM5voXT0qEjnFW8WJdszQnNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.com>
Subject: ...
From: [REDACTED] Mirza <[REDACTED]erma@gmail.com>
To: [REDACTED]an@gmail.com,
[REDACTED]OLUTIONS <[REDACTED]olutions@gmail.com>

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

Email Tracking Tools



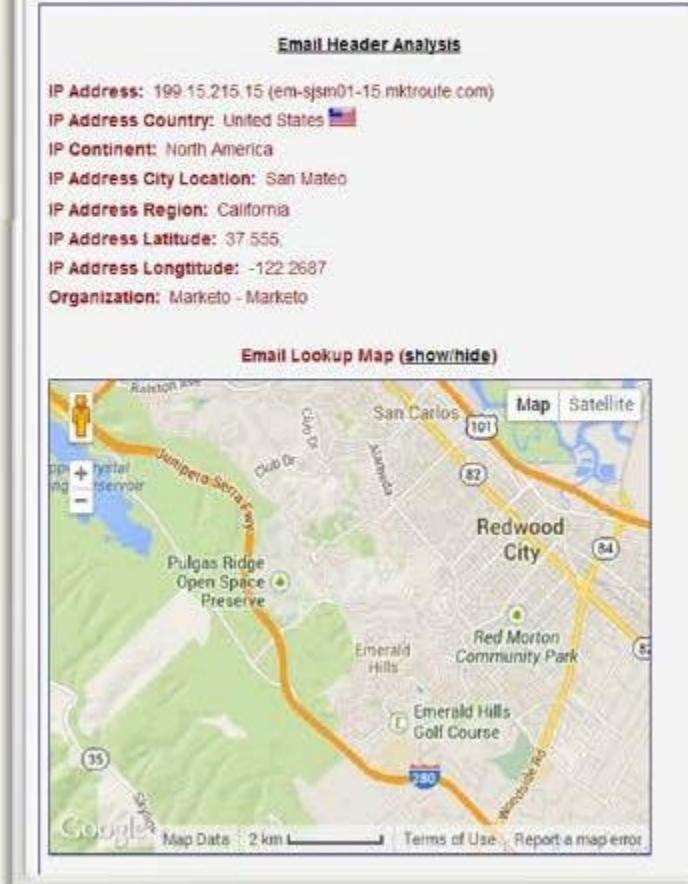
eMailTrackerPro (<http://www.emailtrackerpro.com>)



PoliteMail (<http://www.politemail.com>)

Email Lookup - Free Email Tracker

Trace Email - Track Email



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

Email Tracking Tools

(Cont'd)



Yesware
<http://www.yesware.com>



ContactMonkey
<https://contactmonkey.com>



Read Notify
<http://www.readnotify.com>



DidTheyReadIt
<http://www.didtheyreadit.com>



Trace Email
<http://whatismyipaddress.com>



Zendio
<http://www zendio com>



Pointofmail
<http://www.pointofmail.com>



WhoReadMe
<http://whoreadme.com>



GetNotify
<http://www.getnotify.com>



G-Lock Analytics
<http://glockanalytics.com>

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Competitive Intelligence Gathering

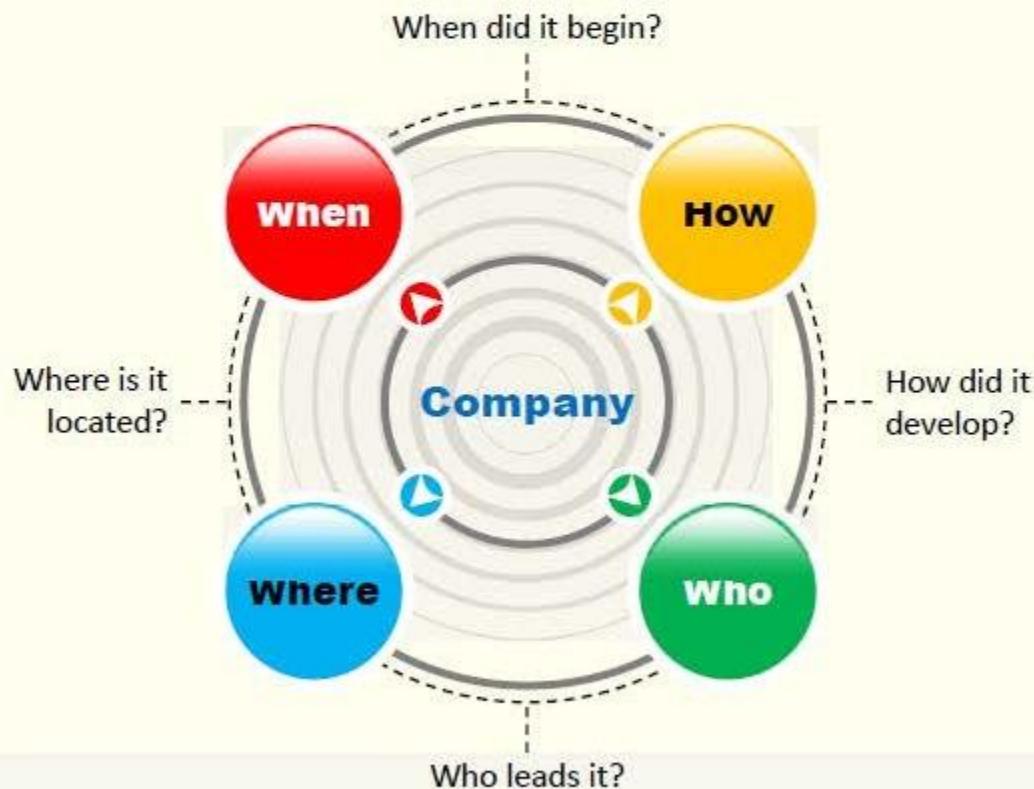
- Competitive intelligence gathering is the process of **identifying, gathering, analyzing, verifying**, and using information about your competitors from resources such as the Internet
- Competitive intelligence is **non-interfering** and **subtle in nature**



Sources of Competitive Intelligence

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

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



Visit These Sites

01. EDGAR Database

<http://www.sec.gov/edgar.shtml>

02. Hoovers

<http://www.hoovers.com/about-us.html>

03. LexisNexis

<http://www.lexisnexis.com>

04. Business Wire

<http://www.businesswire.com>

Competitive Intelligence - What Are the Company's Plans?

01

Market Watch (<http://www.marketwatch.com>)



02

The Wall Street Transcript (<http://www.twst.com>)



03

Lipper Marketplace (<http://www.lippermarketplace.com>)



04

Euromonitor (<http://www.euromonitor.com>)



05

Experian (<http://www.experian.com>)



06

SEC Info (<http://www.secinfo.com>)



07

The Search Monitor (<http://www.thesearchmonitor.com>)



Competitive Intelligence - What Expert Opinions Say About the Company

ABI/INFORM Global

<http://www.proquest.com>



SEMRush

<http://www.semrush.com>



Compete PRO™

<http://www.compete.com>



Copernic Tracker

<http://www.copernic.com>



copernic



AttentionMeter

<http://www.attentionmeter.com>



Jobitorial

<http://www.jobitorial.com>



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

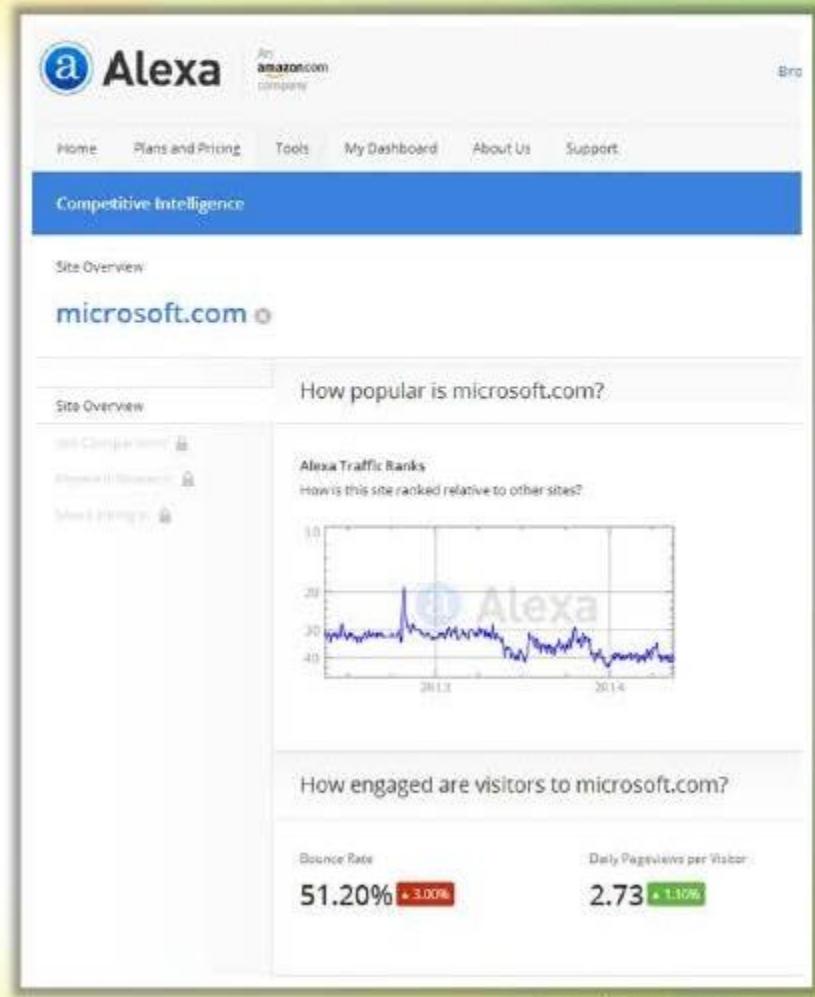
Page views

Bounce rate

Live visitors map

Site ranking

- Traffic monitoring helps to collect information about the **target's customer base** which help attackers to disguise as a customer and launch social engineering attacks on the target



<http://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

The screenshot shows the Trackur dashboard with the following details:

- Profiles:** Shows a dropdown menu for "Main Account".
- Keyword:** Set to "Twitter".
- Saved Searches:** Shows a list of saved searches.
- Results for: Twitter**:
 - Incidents from the past 24 hours:** 1189
 - New Results:** 201
 - 7 Day Trend:** A line graph showing the trend over 7 days.
 - Result Sources:** A table showing the number of incidents by source.
 - Details:** A list of 20 recent tweets mentioning "Twitter" with their respective influence scores (ranging from 0.00 to 1.00).



<http://www.trackur.com>

Tools for Tracking Online Reputation of the Target



Rankur
<http://rankur.com>



Social Mention
<http://www.socialmention.com>



ReputationDefender
<https://www.reputation.com>



Naymz
<http://www.naymz.com>



Brandyourself
<https://brandyourself.com>



Google Alerts
<http://www.google.com>



WhosTalkin
<http://www.whostalkin.com>



PR Software
<http://www.cision.com>



BrandsEye
<http://www.brandseye.com>



Talkwalker
<http://www.talkwalker.com>

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

WHOIS Lookup

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

WHOIS query returns:

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

Information obtained from WHOIS database assists an attacker to:

- Gather personal information that assists to perform social engineering

Regional Internet Registries (RIRs)



WHOIS Lookup Result Analysis

Whois Record for Microsoft.com

- Whois & Quick Stats

Email domains@microsoft.com is associated with ~88,592 domains
msnhst@microsoft.com is associated with ~44,295 domains
abusecomplaints@markmonitor.com is associated with ~659,607 domains

Registrant Org Microsoft Corporation is associated with ~67,950 other domains

Registrar MARKMONITOR INC.

Registrar Status clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited

Dates Created on 1991-05-02 - Expires on 2021-05-03 -
Updated on 2014-10-09

Name Server(s) NS1.MSFT.NET (has 30,782 domains)
NS2.MSFT.NET (has 30,782 domains)
NS3.MSFT.NET (has 30,782 domains)
NS4.MSFT.NET (has 30,782 domains)

IP Address 23.198.159.184 - 16 other sites hosted on this server

IP Location WA - Washington - Seattle - Akamai Technologies Inc.

ASN AS20940 AKAMAI-ASN1 Akamai International B.V. (registered Jul 10, 2001)

Domain Status Registered And Active Website

Whois History 4,374 records have been archived since 2001-12-19

IP History 203 changes on 38 unique IP addresses over 11 years

Registrar History 4 registrars

SmartWhois - Evaluation Version

File Query Edit View Settings Help

IP, host or domain: microsoft.com Query

Results microsoft.com

- microsoft.com
- 64.411.37
- Domain Administrator Microsoft Corporation One Microsoft Way Redmond WA 98052 United States domains@microsoft.com +1.4258828090 Fax +1.4259367326
- Domain Administrator Microsoft Corporation One Microsoft Way Redmond WA 98052 United States domains@microsoft.com +1.4258828080 Fax +1.4259367326
- MSN Hostmaster Microsoft Corporation One Microsoft Way Redmond WA 98052 United States msnit@microsoft.com +1.4258828080 Fax +1.4259367326
- ns2.msft.net ns1.msft.net ns4.msft.net ns5.msft.net ns3.msft.net
- Google Page Rank : 8 Alexa Traffic Rank : 35
- Created: 1991-05-01 Updated: 2013-08-11 Expires: 2021-05-02 Source: whois.markmonitor.com

Completed at 9/10/2013 6:53:25 PM Processing time: 10.17 seconds

WHOIS Lookup Tools



LanWhois
<http://lantricks.com>



Batch IP Converter
<http://www.networkmost.com>



CallerIP
<http://www.callerippro.com>



Whois Lookup Multiple Addresses
<http://www.sobelsoft.com>



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



HotWhois
<http://www.tialsoft.com>



ActiveWhois
<http://www.johnru.com>



WhoisThisDomain
<http://www.nirsoft.net>



SoftFuse Whois
<http://www.softfuse.com>



Whois
<http://technet.microsoft.com>

WHOIS Lookup Tools

(Cont'd)



Domain Dossier

<http://centralops.net>



Whois

<http://tools.whois.net>



BetterWhois

<http://www.betterwhois.com>



DNSstuff

<http://www.dnsstuff.com>



Whois Online

<http://whois.online-domain-tools.com>



Network Solutions Whois

<http://www.networksolutions.com>



Web Wiz

<http://www.webwiz.co.uk/domain-tools/whois-lookup.htm>



WebToolHub

<http://www.webtoolhub.com/tn56138-1-whois-lookup.aspx>



Network-Tools.com

<http://network-tools.com>



UltraTools

<https://www.ultratools.com/whois/home>

WHOIS Lookup Tools for Mobile

DNS Tools

The screenshot shows the 'DNS Report' section of the app. It includes a 'Domain' input field containing 'whois.com.au', a 'Lookup' button, and a 'Parent' section. The 'Parent' section displays NS records for the domain, listing four nameservers: ns2.google.com, ns1.google.com, ns3.google.com, and ns4.google.com, all with TTL values of 172800. Below this, it says 'These records come from: + m.gid-servers.net.' and 'Glue records.' with a note that all are sending glue.

DNS Report

Domain: whois.com.au

Lookup

Parent

Parent NS Records:

The nameserver record's known by the parent servers are:

- ns2.google.com. [216.239.34.10] [TTL=172800]
- ns1.google.com. [216.239.32.10] [TTL=172800]
- ns3.google.com. [216.239.36.10] [TTL=172800]
- ns4.google.com. [216.239.38.10] [TTL=172800]

These records come from:
+ m.gid-servers.net.

Glue records.

✓ OK: All your parent nameservers are sending glue.

Nameservers

NS records from your nameservers

The following NS records are listed at your nameservers

- ns4.google.com. [216.239.38.10] [TTL=345600]
- ns2.google.com. [216.239.34.10] [TTL=345600]
- ns1.google.com. [216.239.32.10] [TTL=345600]
- ns3.google.com. [216.239.36.10] [TTL=345600]

Multiple NS records

✓ OK: You have 4 nameservers.

UDP Respond

✓ OK: All your nameservers respond to (udp) dns requests.

UltraTools Mobile

The screenshot shows the 'UltraTools' mobile application's dashboard. It features a grid of 12 icons representing different tools: Domain Health Report, DNS Speed Test, DNS Lookup, WHOIS Lookup, IPv4 to IPv6 Conversion, IPv6 Compatibility, SSL Examination, Device Information, Connection Speed, Visual Traceroute, Ping, and GeoIP Lookup.

Whois® Lookup Tool

The screenshot shows the 'Dig (DNS) Lookup' screen for the domain 'whois.com.au'. It displays the following information:

Dig (DNS) Lookup
Domain: whois.com.au

Dig Lookup

A Records

Record Type A IP address 64.62.140.72 TTL 1 hours (3600 seconds)

AAAA (IPv6 address) Records

Record Type AAAA IPV6 2001:470:208:0:403e:8c48 TTL 1 hours (3600 seconds)

NS (Name Server) Records

| Server | TTL |
|--------------------|--------------------------|
| ns2.p26.dynect.net | 24 hours (86400 seconds) |
| ns1.p26.dynect.net | 24 hours (86400 seconds) |
| ns3.p26.dynect.net | 24 hours (86400 seconds) |
| ns4.p26.dynect.net | 24 hours (86400 seconds) |

MX (Mail eXchanger) Records

| Server | Priority | TTL |
|--------------|----------|------------------------|
| whois.com.au | 10 | 1 hours (3600 seconds) |

SOA (Start of Authority) Records

| Server | TTL | Data |
|--------|----------------|--|
| | 1 hours (3600) | ns1.p26.dynect.net hostmaster.whois.com.au 29 3600 600 |

<https://www.dnssniffer.com>

<https://www.ultratools.com>

<http://www.whois.com.au>

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

Network Footprinting

10

Footprinting through Social Engineering

Extracting DNS Information

Attacker 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 |
| SDA | 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 location and type of servers

DNS Interrogation Tools

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

Extracting DNS Information

(Cont'd)

Domain Dossier

DNS records

| name | class | type | data | time to live |
|-----------------------------|-------|------|---|----------------------|
| yahoo.com | IN | SOA | server: ns1.yahoo.com email: hostmaster@yahoo-inc.com serial: 2015040304 refresh: 3600 retry: 300 expire: 1814400 minimum ttl: 600 | 1800s (00:30:00) |
| yahoo.com | IN | A | 98.138.253.109 | 1800s (00:30:00) |
| yahoo.com | IN | A | 206.190.36.45 | 1800s (00:30:00) |
| yahoo.com | IN | A | 98.139.183.24 | 1800s (00:30:00) |
| yahoo.com | IN | MX | preference: 1 exchange: mta5.am0.yahoodns.net | 1800s (00:30:00) |
| yahoo.com | IN | MX | preference: 1 exchange: mta6.am0.yahoodns.net | 1800s (00:30:00) |
| yahoo.com | IN | MX | preference: 1 exchange: mta7.am0.yahoodns.net | 1800s (00:30:00) |
| yahoo.com | IN | NS | ns4.yahoo.com | 172800s (2:00:00:00) |
| yahoo.com | IN | NS | ns6.yahoo.com | 172800s (2:00:00:00) |
| yahoo.com | IN | NS | ns5.yahoo.com | 172800s (2:00:00:00) |
| yahoo.com | IN | NS | ns3.yahoo.com | 172800s (2:00:00:00) |
| yahoo.com | IN | NS | ns2.yahoo.com | 172800s (2:00:00:00) |
| yahoo.com | IN | NS | ns1.yahoo.com | 172800s (2:00:00:00) |
| yahoo.com | IN | TXT | v=spf1 redirect=_spf.mail.yahoo.com | 1800s (00:30:00) |
| 109.253.138.98.in-addr.arpa | IN | PTR | ir1.fp.vip.us1.yahoo.com | 1800s (00:30:00) |
| 253.138.98.in-addr.arpa | IN | NS | ns4.yahoo.com | 172800s (2:00:00:00) |
| 253.138.98.in-addr.arpa | IN | NS | ns1.yahoo.com | 172800s (2:00:00:00) |
| 253.138.98.in-addr.arpa | IN | NS | ns3.yahoo.com | 172800s (2:00:00:00) |
| 253.138.98.in-addr.arpa | IN | NS | ns5.yahoo.com | 172800s (2:00:00:00) |
| 253.138.98.in-addr.arpa | IN | NS | ns2.yahoo.com | 172800s (2:00:00:00) |
| 253.138.98.in-addr.arpa | IN | TXT | Contact for this domain is Yahoo! NOC, +1 408 349 5555 | 1800s (00:30:00) |
| 253.138.98.in-addr.arpa | IN | SOA | server: hidden-master.yahoo.com email: hostmaster@yahoo-inc.com serial: 2014101602 refresh: 3600 retry: 600 expire: 5184000 minimum ttl: 1800 | 600s (00:10:00) |

<http://centralops.net>

DNS Lookup

DNS Lookup for microsoft.com

Searcing for microsoft.com ANY Record at c.root-servers.net [192.33.4.12] referred to f.gld-servers.net
Searcing for microsoft.com ANY Record at f.gld-servers.net [192.35.51.30] referred to ns1.msft.net
Searcing for microsoft.com ANY Record at ns1.msft.net [208.84.0.53]

Results from ns1.msft.net [IP: 208.84.0.53] for microsoft.com ANY Record

| Domain | Type | Time to Live | Answer |
|---------------|------|-----------------|---|
| Answer | | | |
| microsoft.com | A | 3600 [1 Hour] | 134.170.188.221 |
| microsoft.com | A | 3600 [1 Hour] | 134.170.185.46 |
| microsoft.com | NS | 172800 [2 Days] | ns4.msft.net |
| microsoft.com | NS | 172800 [2 Days] | ns1.msft.net |
| microsoft.com | NS | 172800 [2 Days] | ns2.msft.net |
| microsoft.com | NS | 172800 [2 Days] | ns3.msft.net |
| microsoft.com | SOA | 3600 [1 Hour] | Primary Name Server: ns1.msft.net Responsible: ns1list@microsoft.com Serial Number: 2015040301 Refresh: 7200 [2 Hours] Retry: 600 [10 Minutes] Expire: 2419200 [28 Days] Minimum Time to Live: 3600 [1 Hour] |
| microsoft.com | MX | 3600 [1 Hour] | microsoft-com.mail.protection.outlook.com [Preference: 10] |
| microsoft.com | TXT | 3600 [1 Hour] | FbUF6DbkE+Aw1/wi9xgDi8KVrlIZus5v8L8tbIQZkGrQ/rVQKJ |

<https://network-tools.webwiz.co.uk>

DNS Interrogation Tools



DIG

<http://www.kloth.net>



myDNSTools

<http://www.mydnstools.info>



Professional Toolset

<http://www.dnsstuff.com>



DNS Records

<http://network-tools.com>



DNSData View

<http://www.nirsoft.net>



DNSWatch

<http://www.dnswatch.info>



DomainTools

<http://www.domaintools.com>



DNS Query Utility

<http://www.dnsqueries.com>



DNS Lookup

<https://www.ultratools.com>



DNS Query Utility

<http://www.webmaster-toolkit.com>

Locate the Network Range

- Network range information assists attackers to create 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

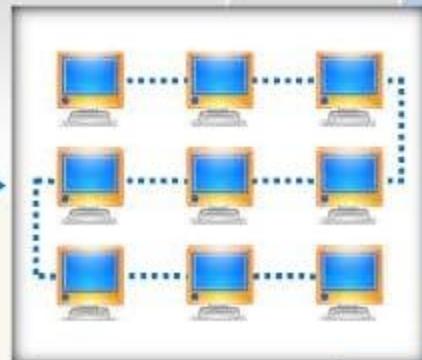
| Network | |
|-------------------|---|
| NetRange | 207.46.0.0 - 207.46.255.255 |
| CIDR | 207.46.0.0/16 |
| Name | MICROSOFT-GLOBAL-NET |
| Handle | NET207-46-0-1 |
| Parent | NET207 (NET-207-0-0-0) |
| Net Type | Direct Assignment |
| Origin AS | |
| Organization | Microsoft Corporation (MSFT) |
| Registration Date | 1997-03-31 |
| Last Updated | 2013-08-20 |
| Comments | |
| ABSTRL Link | http://whois.arin.net/rest/net/NET-207-46-0-1 |
| 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 Date | 1998-07-10 |
| Last Updated | 2013-08-21 |
| 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: https://oam.microsoft.com . For SPAM and other abuse issues, such as Microsoft Accounts, please contact: abuse@microsoft.com . To report security vulnerabilities in Microsoft products and services, please contact: secure@microsoft.com . For legal and law enforcement-related requests, please contact: microsoft@microsoft.com . For routing, peering or DNS issues, please contact: Contact: |

Queried
whois.arin.net with
"207.46.232.182"



Attacker



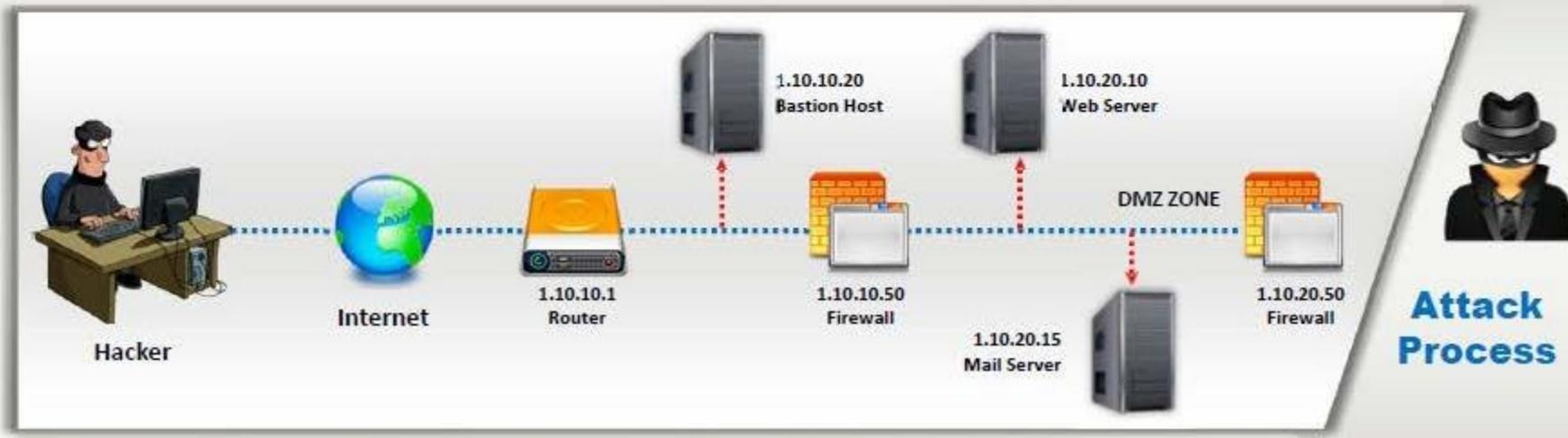
Traceroute

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



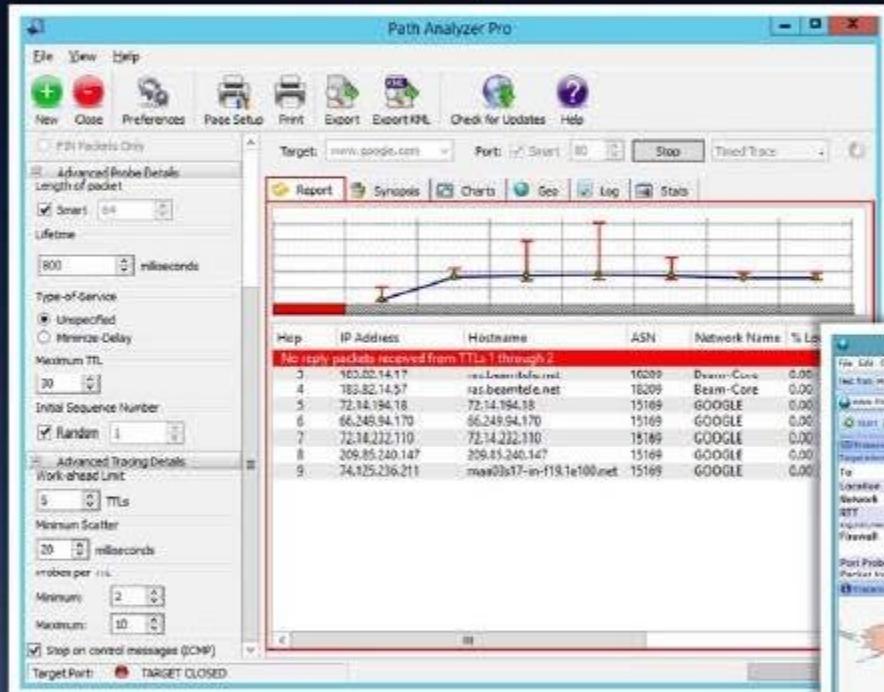
Traceroute Analysis

- 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

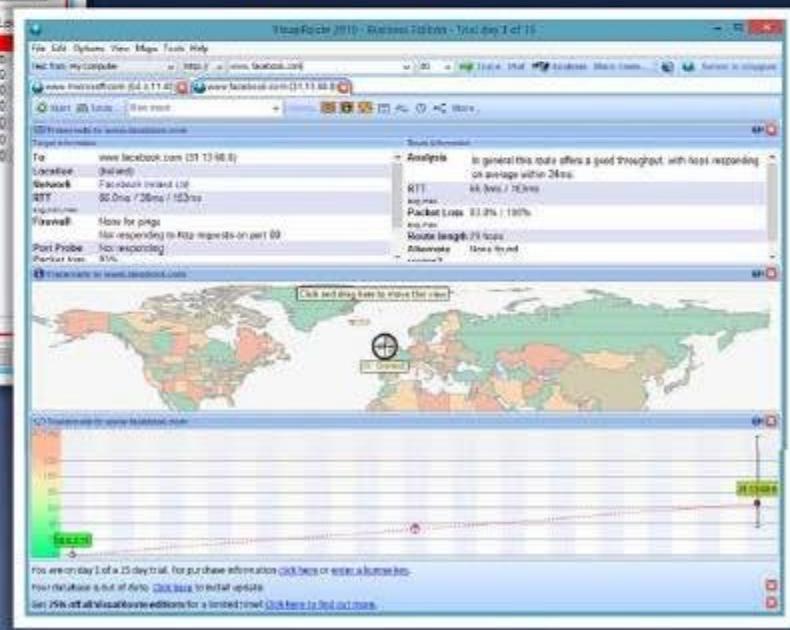
Path Analyzer Pro



<http://www.pathanalyzer.com>



VisualRoute



<http://www.visualroute.com>

Traceroute Tools

(Cont'd)



Network Pinger

<http://www.networkpinger.com>



GEOSpider

<http://www.oreware.com>



vTrace

<http://vtrace.pl>



Trout

<http://www.mcafee.com>



Roadkil's Trace Route

<http://www.roadkil.net>



Magic NetTrace

<http://www.tialsoft.com>



3D Traceroute

<http://www.d3tr.de>



AnalogX HyperTrace

<http://www.analogx.com>



Network Systems Traceroute

<http://www.net.princeton.edu>



Ping Plotter

<http://www.pingplotter.com>

Footprinting Methodology

1

Footprinting through Search Engines

2

Footprinting Using Advanced Google Hacking Techniques

3

Footprinting through Social Networking Sites

4

Website Footprinting

5

Email Footprinting

6

Competitive Intelligence

7

WHOIS Footprinting

8

DNS Footprinting

9

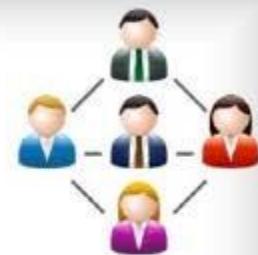
Network Footprinting

10

Footprinting through Social Engineering

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



Social engineering techniques:

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



Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Eavesdropping

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



Shoulder Surfing

- Shoulder surfing is a technique, where attackers secretly observes 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 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



**Footprinting
Concepts**



**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



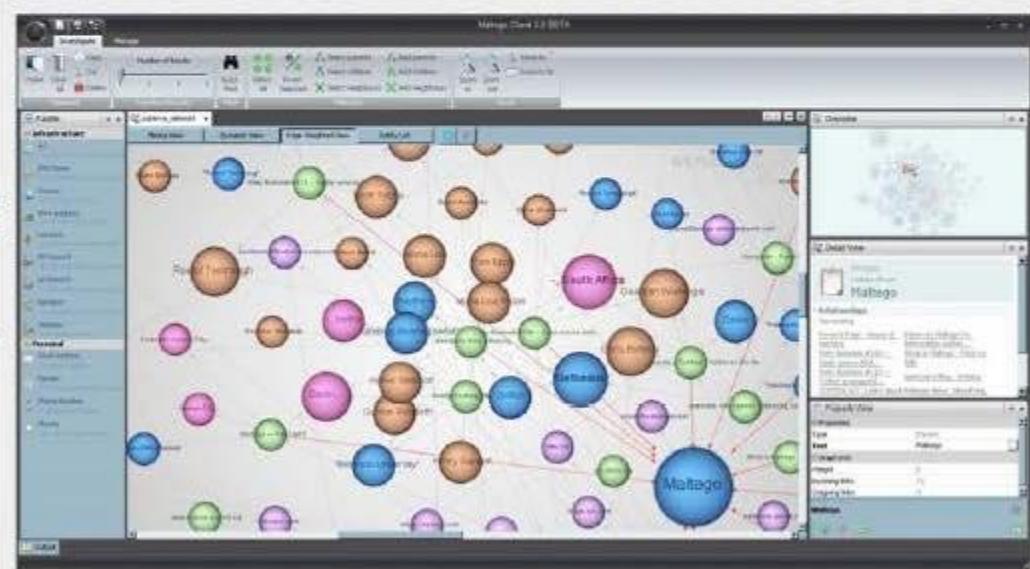
**Footprinting
Penetration
Testing**

Footprinting Tool: Maltego



Internet Domain

<http://www.paterva.com>



Personal Information

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

Footprinting Tool: 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

The image shows two terminal windows on a Kali Linux desktop. The left window displays the Recon-**ng** interface with a target website for 'Black Hills Information Security'. The right window shows the results of a netcraft search for 'ECCOUNCIL.ORG'.

Terminal 1 (Left):

```
root@kali:~# recon-ng
[recon-ng][default] >
```

Terminal 2 (Right):

```
Sat Apr 4, 3:20 AM
root@kali:~#
[ECCOUNCIL.ORG]
URL: http://searchdns.netcraft.com/restrictionelite%2Bands%2Bwithnestcouncil.org
store.eccouncil.org
ciso.eccouncil.org
aspen.eccouncil.org
academia.eccouncil.org
www.eccouncil.org
portals.eccouncil.org
vesta.eccouncil.org
ilabs.eccouncil.org
foundation.eccouncil.org
ictass.eccouncil.org
cert.eccouncil.org
frank.eccouncil.org

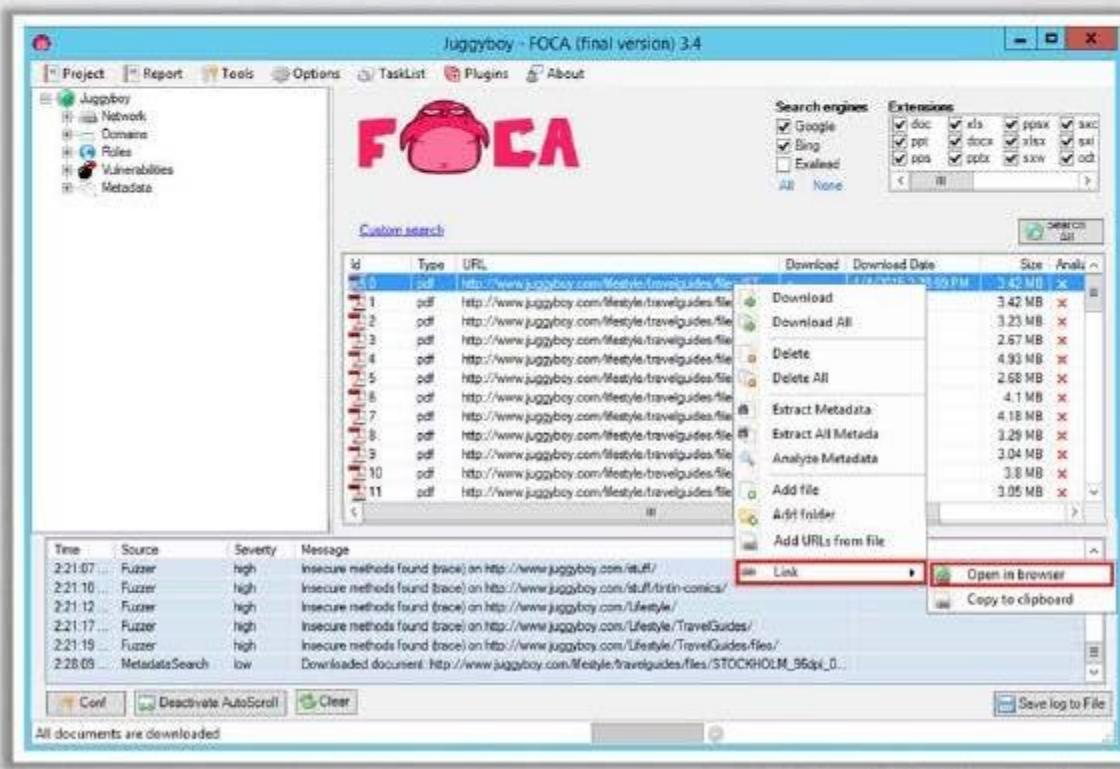
SUMMARY
--> 12 total (12 new) hosts found.
[recon-ng][eccouncil.org][netcraft] > show hosts
```

| rowid | host | ip_address | region | country | latitude | longitude | module |
|-------|--------------------------|------------|--------|---------|----------|-----------|----------|
| 1 | store.eccouncil.org | | | | | | netcraft |
| 2 | ciso.eccouncil.org | | | | | | netcraft |
| 3 | aspen.eccouncil.org | | | | | | netcraft |
| 4 | academia.eccouncil.org | | | | | | netcraft |
| 5 | www.eccouncil.org | | | | | | netcraft |
| 6 | portals.eccouncil.org | | | | | | netcraft |
| 7 | vesta.eccouncil.org | | | | | | netcraft |
| 8 | ilabs.eccouncil.org | | | | | | netcraft |
| 9 | foundation.eccouncil.org | | | | | | netcraft |
| 10 | ictass.eccouncil.org | | | | | | netcraft |
| 11 | cert.eccouncil.org | | | | | | netcraft |
| 12 | frank.eccouncil.org | | | | | | netcraft |

https://bitbucket.org

Footprinting Tool: FOCA

- FOCA (Fingerprinting Organizations with Collected Archives) is a tool used mainly to find metadata and hidden information in the documents its scans
- Using FOCA, it is possible to undertake multiple attacks and analysis techniques such as **metadata extraction**, **network analysis**, DNS snooping, proxies search, **fingerprinting**, open directories search, etc.



<https://www.elevenpaths.com>

Additional Footprinting Tools



Prefix Whois

<http://pwhois.org>



NetScanTools Pro

<http://www.netscantools.com>



Tctrace

<http://www.phenoelit.org>



**Autonomous System
Scanner (ASS)**

<http://www.phenoelit.org>



DNS-Digger

<http://www.dnsdigger.com>



Netmask

<http://www.phenoelit.org>



Binging

<http://www.blueinfy.com>



SearchBug

<http://www.searchbug.com>



TinEye

<http://www.tineye.com>



Robtex

<http://www.robtex.com>

Additional Footprinting Tools

(Cont'd)



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



White Pages
<http://www.whitepages.com>



Email Tracking Tool
<http://www.filley.com>



yoName
<http://yoname.com>



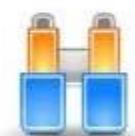
Ping-Probe
<http://www.ping-probe.com>



SpiderFoot
<http://www.spiderfoot.net>



NSlookup
<http://www.kloth.net>



Zaba Search
<http://www.zabasearch.com>



GeoTrace
<http://www.nabber.org>



DomainHostingView
<http://www.nirsoft.net>

Additional Footprinting Tools

(Cont'd)



MetaGoofil

<http://www.edge-security.com>



Wikto

<http://research.sensepost.com>



SiteDigger

<http://www.mcafee.com>



Google Hacks

<http://code.google.com>



BiLE Suite

<http://www.sensepost.com>



GMapCatcher

<http://code.google.com>



SearchDiggity

<http://www.bishopfox.com>



Google HACK DB

<http://www.secpoint.com>



Gooscan

<http://www.darknet.org.uk>



Trellian

<http://ci.trellian.com>

Module Flow



**Footprinting
Concepts**



**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



**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)

 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

 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



**Footprinting
Concepts**



**Footprinting
Methodology**



**Footprinting
Tools**



**Footprinting
Countermeasures**



**Footprinting
Penetration
Testing**

Footprinting Pen Testing

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



Prevent **DNS record retrieval** from publicly available servers



Footprinting pen testing helps organization to:



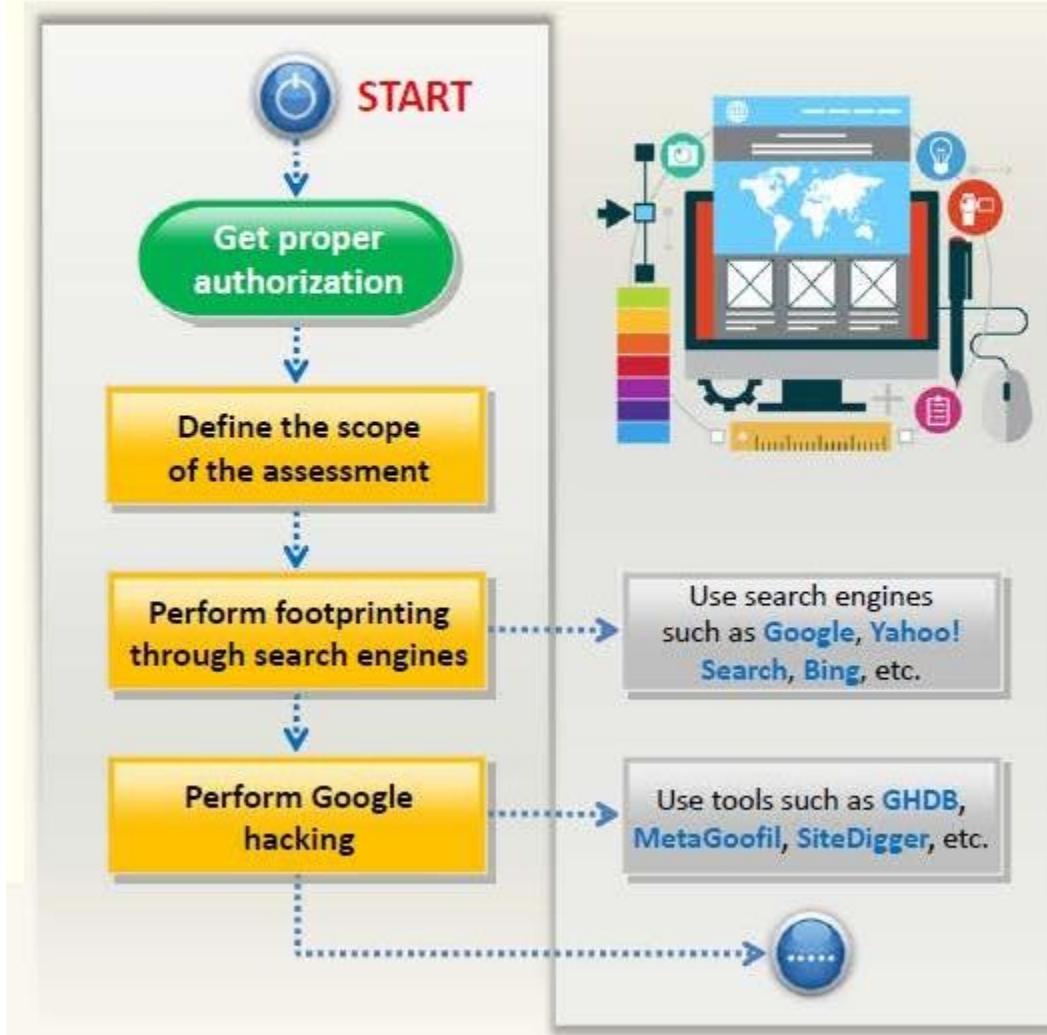
Prevent **information leakage**



Prevent **social engineering attempts**

Footprinting Pen Testing

(Cont'd)

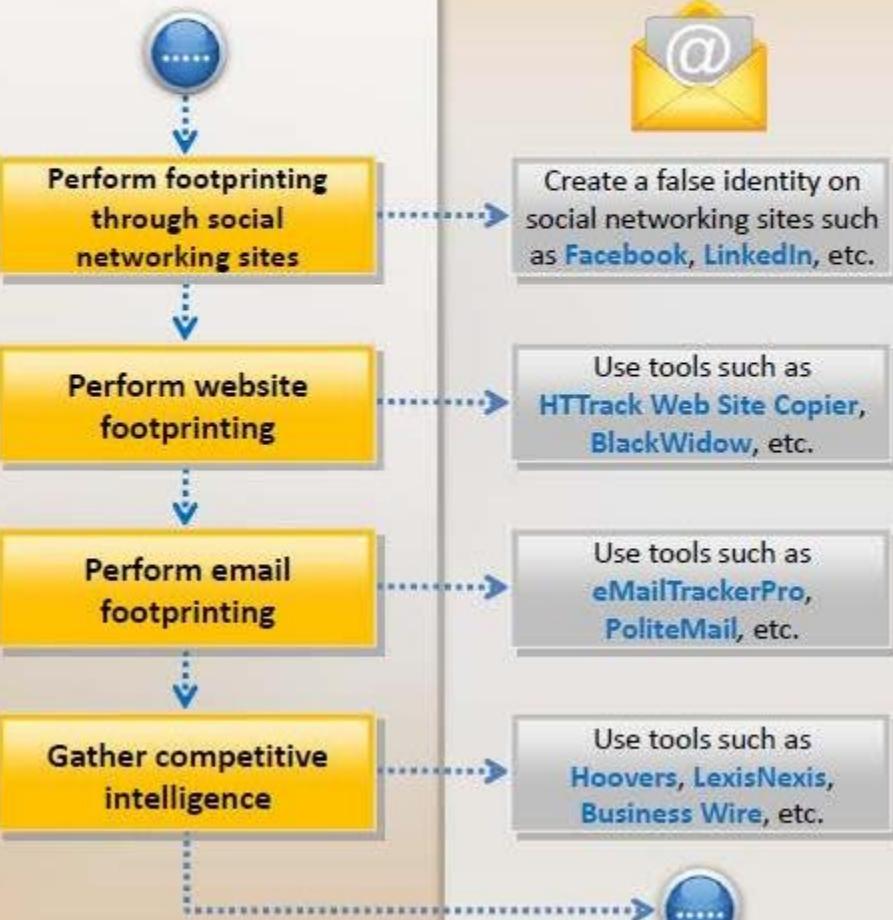


- Get proper authorization and define the scope of the assessment
- Footprint search engines such as **Google**, **Yahoo! Search**, **Ask**, **Bing**, **Dogpile**, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering and other types of advanced system attacks
- Perform Google hacking using tools such as **GHDB**, **MetaGoofil**, **SiteDigger**, etc.



Footprinting Pen Testing

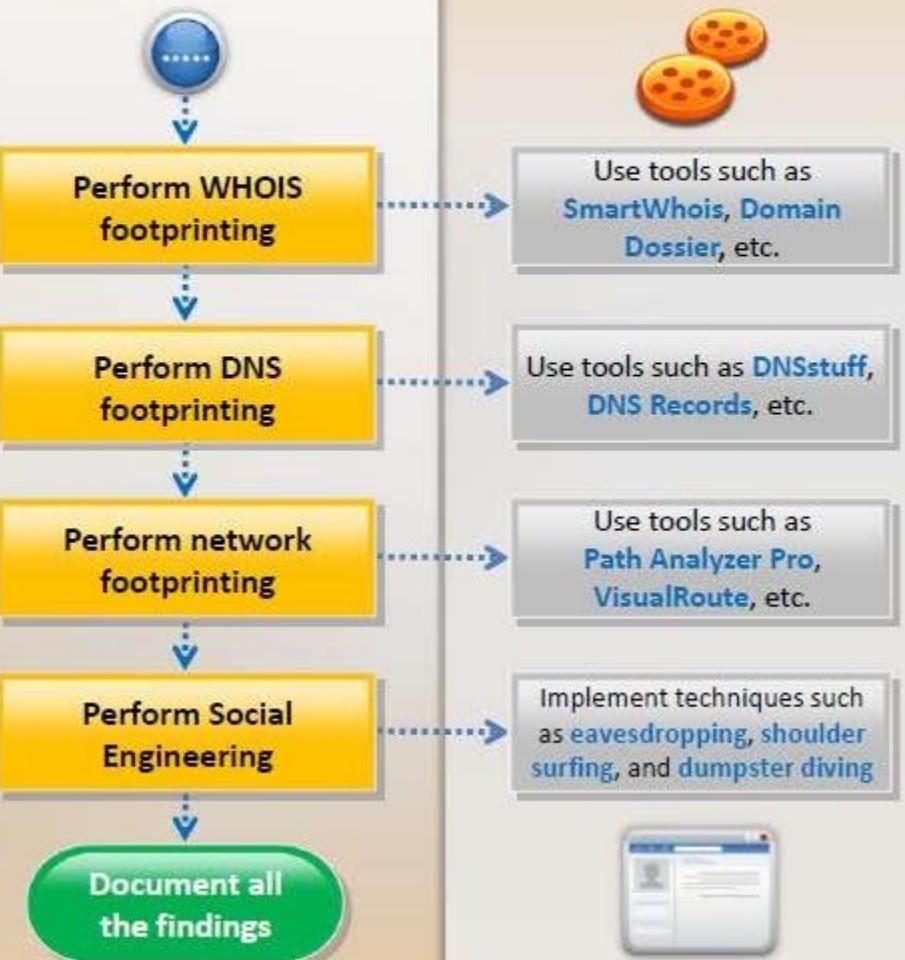
(Cont'd)



- Gather target organization employees information from their personal profiles on social networking sites such as **Facebook**, **LinkedIn**, **Twitter**, **Google+**, **Pinterest**, etc. that assist to perform social engineering
- Perform website footprinting using tools such as **HTTrack Web Site Copier**, **BlackWidow**, **Webscraper**, etc. to build a detailed map of website's structure and architecture
- Perform email footprinting using tools such as **eMailTrackerPro**, **PoliteMail**, **Email Lookup – Free Email Tracker**, etc. to gather information about the physical location of an individual to perform social engineering that in turn may help in mapping target organization's network
- Gather competitive intelligence using tools such as **Hoovers**, **LexisNexis**, **Business Wire**, etc.

Footprinting Pen Testing

(Cont'd)



- Perform WHOIS footprinting using tools such as **SmartWhois**, **Domain Dossier**, etc. to create detailed map of organizational network, to gather personal information that assists to perform social engineering, and to gather other internal network details, etc.
- Perform DNS footprinting using tools such as **DNSstuff**, **DNS Records**, etc. to determine key hosts in the network and perform social engineering attacks
- Perform network footprinting using tool such as **Path Analyzer Pro**, **VisualRoute**, **Network Pinger**, etc. to create a map of the target's network
- Implement social engineering techniques such as **eavesdropping**, **shoulder surfing**, and **dumpster diving** that may help to gather more critical information about the target organization
- 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 people search

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

Information obtained through Google

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

Information obtained through 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: | Range of IP addresses: |
| Project plans: | Subnet mask used by the target organization: |
| Others: | OS's in use: |
| Information obtained through WHOIS footprinting | |
| Domain name details: | Firewall locations: |
| Contact details of domain owner: | Others: |
| Domain name servers: | |
| Netrange: | |
| When a domain has been created: | |
| Others: | |
| Information obtained through DNS footprinting | |
| Location of DNS servers: | Personal information: |
| Type of servers: | Financial information: |
| Others: | Operating environment: |
| | User names and passwords: |
| | Network layout information: |
| | IP addresses and names of servers: |
| | Others: |

Module Summary

- ❑ Footprinting is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system
- ❑ It reduces attacker's focus area to specific range of IP address, 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 location and type of servers
- ❑ Attackers conduct traceroute to extract information about: network topology, trusted routers, and firewall locations