

Footprinting and Reconnaissance

Module 02

Unmask the Invisible Hacker.



Module Objectives

C|EH
Certified Ethical Hacker

- 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



Module Flow



1

Footprinting
Concepts

2

Footprinting
Methodology

3

Footprinting
Tools

4

Footprinting
Countermeasures

5

Footprinting
Penetration
Testing

What is Footprinting?

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

Objectives of Footprinting

C|EH
Certified Ethical Hacker

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
- IDSe 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



1

Footprinting
Concepts

2

Footprinting
Methodology

3

Footprinting
Tools

4

Footprinting
Countermeasures

5

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](#) [Help](#)

Microsoft

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

Microsoft Corporation

From Wikipedia, the free encyclopedia

Microsoft Corporation

Type: **Public**
Traded as: **NASDAQ: MSFT** [\[?\]](#)
Dow Jones Industrial Average Component
NASDAQ-100 Component
S&P 500 Component
Industry: **Computer software**
Founded: **Albuquerque, New Mexico, United States (April 4, 1975)**
Founders: **Bill Gates, Paul Allen**
Headquarters: **Microsoft Redmond Campus**

Main page [Content](#) [Featured content](#) [Current events](#) [Random article](#) [Donate to Wikipedia](#)

Interaction: [Help](#) [About Wikipedia](#) [Community portal](#) [Recent changes](#) [Contact page](#)

Toolbox: [Print/export](#)

Languages: [Afrikaans](#) [Alemannisch](#)

Finding Company's Public and Restricted Websites



- Search for the target company's external URL in a search engine such as **Google**, **Bing**, etc.

- Restricted URLs **provide an insight** into different departments and business units in an organization

- You may find a company's restricted URLs **by trial and error method or using a service such as**
<http://www.netcraft.com>



Results for microsoft.com

Found 255 sites

Site	Site Report	First seen
81. emails.microsoft.com		june 2015
82. privacy.microsoft.com		march 2006
83. images2.store.microsoft.com		april 2009
84. mvp.microsoft.com		may 2012
85. i.s-microsoft.com		december 2012
86. schemas.microsoft.com		june 2002
87. pinpoint.microsoft.com		september 2008
88. windowshelp.microsoft.com		january 2010
89. expertzone.microsoft.com		september 2005
90. lumiaconversationsuk.microsoft.com		march 2015
91. shopformusic.microsoft.com		may 2006
92. licensing.microsoft.com		june 2002
93. account.webapps.microsoft.com		august 2015
94. smallbusiness.support.microsoft.com		july 2012
95. familiesafety.microsoft.com		july 2012
96. powerbi.microsoft.com		june 2015
97. advertising.microsoft.com		december 2006
98. wer.microsoft.com		october 2005
99. curah.microsoft.com		december 2013
100. oem.microsoft.com		december 1996

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 2012
5. windows.microsoft.com		june 1998	microsoft corporation	unknown
6. msn.microsoft.com		september 1998	microsoft corporation	windows server 2012
7. social.technet.microsoft.com		august 2008	microsoft corporation	citrix netscaler
8. answers.microsoft.com		august 2009	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	akamai 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	akamai technologies	linux
15. www.update.microsoft.com		may 2007	microsoft corporation	windows server 2008
16. s15.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	65.55.58.201	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 1996	Microsoft-IIS/7.5	Windows Server 2008
358	msdn.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
-	adspocit.msn.com	unknown	March 2000	BigIP	F5 BIG-IP
-	www.solomon.com	unknown	October 1995	Microsoft-IIS/7.5	Windows Server 2008
185106	www.rtm.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.de	unknown	January 2002	Microsoft-IIS/7.5	unknown
-	ads.msn.com	unknown	January 1997	Microsoft-IIS/7.5	unknown
-	www.1hotmail.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 2009	Microsoft-IIS/7.5	Windows Server 2008
-	mobile.msn.com	unknown	March 2000	Microsoft-IIS/6.0	unknown

<http://www.netcraft.com>

Determining the Operating System

(Cont'd)



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



EXPOSE ONLINE DEVICES.

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

[TAKE A TOUR](#) [FREE SIGN UP](#)

Possible Search Queries: RissoedCom exposed via Telnet - Wired: <http://www.wired.com/threatlevel/2012/04/rissoedcom-backdoor/> Full Disclosure: <http://sec...>

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

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

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

<http://www.shodanhq.com>

Did you mean: [hostnames:microsoft.com](#)

Services	Count
HTTP	2,700
SRTP	77
FTP	24
HTTP Alternate	30
POP3	24

Top Countries

Country	Count
United States	1,544
China	101
Germany	100
United Kingdom	97
Taiwan	82

Top Cities

City	Count
463	463
78	78
54	54
40	40
33	33
64.4.30.79	64.4.30.79
Windows 7 or I	Windows 7 or I
MS Hotmail	MS Hotmail
410	410
395	395
101	101
75	75
57	57

Object moved

HTTP/1.1 302 Object moved
Cache-Control: private
Content-Length: 180
Content-Type: text/html
Location: <http://www.microsoft.com/en-us/windows/FX101042622.aspx>
Server: Microsoft-IIS/7.0
X-AspNet-Version: 4.0.30319.1
X-Powered-By: ASP.NET
Date: Sun, 29 Sep 2013 20:36:59 GMT

302 Found

HTTP/1.1 302 Found
Date: Sun, 29 Sep 2013 20:34:13 GMT
Server: Apache/2.2.17 (Ubuntu) DAV/2 PHP/5.2.11
Location: <http://windowsupdate.microsoft.com>
Content-Length: 218
Content-Type: text/html; charset=UTF-8

64.4.30.79

HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: image/gif
Expires: -1
Server: Microsoft-IIS/7.0
Set-Cookie: NC1=Q3D=197a8f4f711d34c3144e5284e1bed&HASH=448&LV=20130914
X-Powered-By: ASP.NET
P3P: CP="CAO DSP PSA OUR IND PNT ONL UIC FOR COM NAV INT DEM CNT ET
Date: Sun, 29 Sep 2013 20:31:51 GMT
Content-Length: 44

217.27.179.405

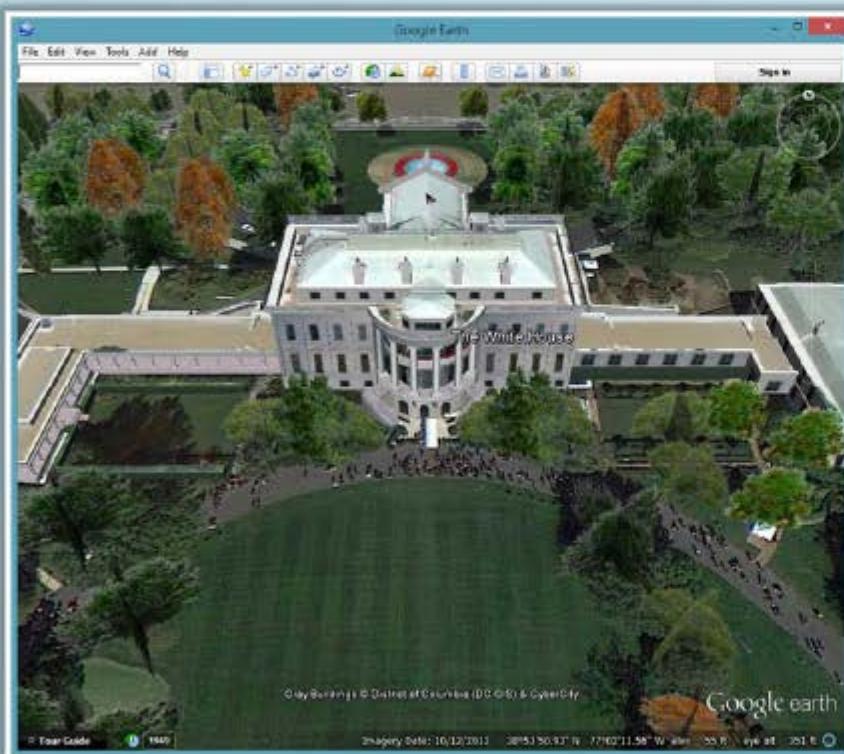
HTTP/1.1 302
Date: Sun, 29 Sep 2013 20:38:31 GMT
Server: Microsoft-IIS/6.0
MicrosoftSharePointTeamService: #0.2.5168
X-Powered-By: ASP.NET
Location: /default.aspx
Cache-Control: private
Content-Length: 9
P3P: CP="CAO DSP PSA OUR IND PNT ONL UIC FOR COM NAV INT DEM CNT ET

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**:



Bill Gates
Co-chair, Bill & Melinda Gates Foundation
Greater Seattle Area | Microsoft
Contact: Bill & Melinda Gates Foundation, Microsoft
Education: Harvard University

Follow | View 690,928 Connections

Published by Bill

We Need Our Brightest People Working on Our... (August 10, 2010)
Three Things I've Learned From Warren Buffett (June 10, 2010)

<http://www.linkedin.com>

Nicolas Cage | United States

Suggested Searches for Nicolas Cage, United States

- Nicolas Cage, Los Angeles, CA, US, 49 years old
- Nicolas Cage, Santa Barbara, CA, US, publisher, 42 years old
- Nicolas Cage, Coyote Beach, FL, US, 27 years old
- Nicolas Cage, Jeffersonville, IN, US, 40 years old
- Nicolas Cage, 11 Hollywood, CA, US, Los Angeles, CA, US

Results for Nicolas Cage, United States

Profile: 88,000+ | Joined: 2007 | Background: 100+ | Friends: 100+ | Public: 500+

Nicolas Cage, Long Beach, CA, US, 49 years old, Actor, Adaptation, The Art of..., Actor, Director, Producer, Writer, Film, 2000+

Nicolas Cage, Santa Barbara, CA, US, publisher, 42 years old, Parent, Entrepreneur, Social Entrepreneur, Personal Profile - 100+

Nicolas Cage, Jeffersonville, IN, US, 42 years old, Personal Profile - 100+

<https://pipl.com>

People Search Online Services

CEH
Certified Ethical Hacker



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

C|EH
Certified Ethical Hacker

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.

The image shows two screenshots of financial websites pinned to a dark blue background. On the left, a white pin holds a screenshot of Google Finance for Google Inc. (Nasdaq: GOOG). It displays the stock price at \$893.06, a 0.00% change, and a chart showing price movements from 2011 to 2012. On the right, a red pin holds a screenshot of Yahoo Finance for Microsoft Corporation (MSFT). It shows the stock price at \$33.03, a +0.34 (+1.04%) change, and a chart showing price movements from 2010 to 2012. Both pages include navigation menus and news tickers.

Google Finance
(<https://www.google.com/finance>)

Yahoo! Finance
(<http://finance.yahoo.com>)

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>



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

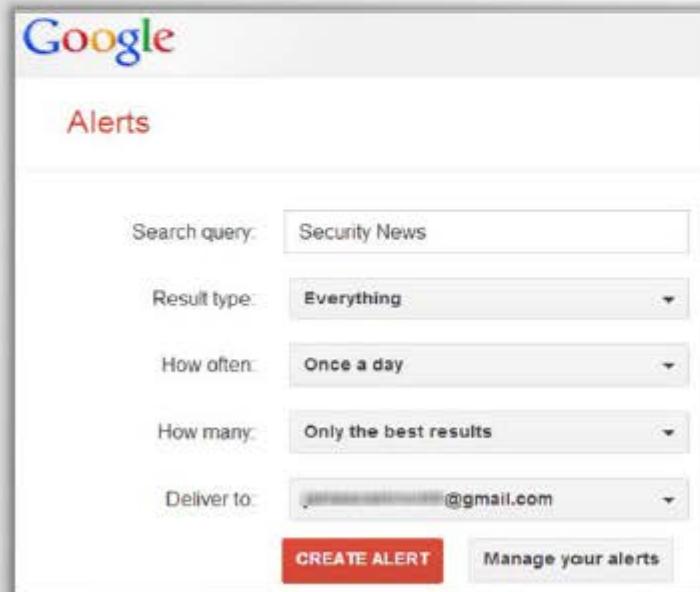
Examples of Alert Services

1 Google Alerts - <http://www.google.com/alerts>

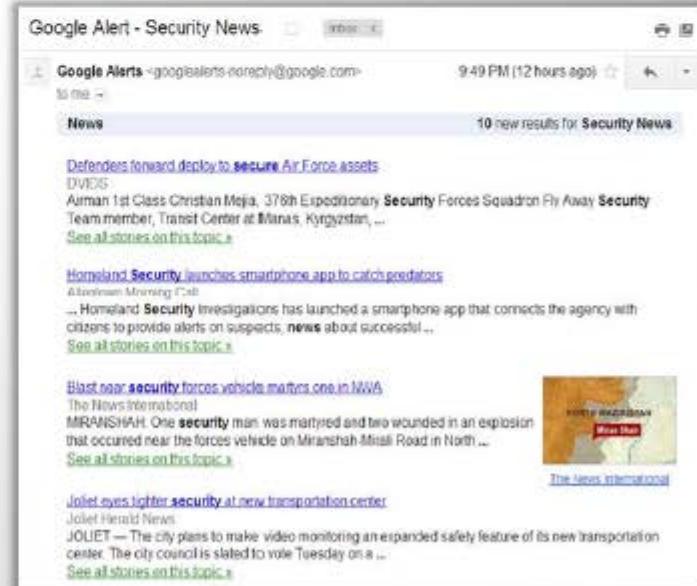
2 Yahoo! Alerts - <http://alerts.yahoo.com>

3 Twitter Alerts - <https://twitter.com/alerts>

4 Giga Alert - <http://www.gigaalert.com>



The screenshot shows the Google Alerts interface. It has a search bar labeled "Search query:" containing "Security News". Below it are dropdown menus for "Result type:" set to "Everything", "How often:" set to "Once a day", and "How many:" set to "Only the best results". At the bottom, there's a "Deliver to:" field with an obscured email address followed by "@gmail.com", a "CREATE ALERT" button in red, and a "Manage your alerts" link.



The screenshot shows a "Google Alert - Security News" page. At the top, it says "10 new results for Security News". Below are three news items:

- Defenders forward deploy to secure Air Force assets**
DVIDS
Airman 1st Class Christian Mejia, 378th Expeditionary Security Forces Squadron Fly Away Security Team member, Transit Center at Minas, Kyrgyzstan, ...
[See all stories on this topic](#)
- Homeland Security launches smartphone app to catch predators**
Associated Press
... Homeland Security Investigations has launched a smartphone app that connects the agency with citizens to provide alerts on suspects, **news** about successful ...
[See all stories on this topic](#)
- Blast near security forces vehicle maims one in NWA**
The News International
MIRANSHAH: One **security** man was martyred and two wounded in an explosion that occurred near the forces vehicle on Miranshah-Mirali Road in North ...
[See all stories on this topic](#)

Information Gathering Using Groups, Forums, and Blogs

C|EH
Certified Ethical Hacker



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



Access to public Google Groups has been restricted by your domain admin

My groups

Home

Stared

Favorites

Click on a group's star icon to add it to your favorites

Express yourself

People power discussions

Speed matters

Discuss from anywhere

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 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

CEH
Certified Ethical Hacker

Date	Title	Summary
2004-03-04	EarlyImpact Productant	The EarlyImpact Productant contains multiple vulnerabilities, which could exploited to allow an attacker to steal user credentials or mount other attacks.
2004-03-04	misSearch vulnerability	Aspiring http://www.securityfocus.com/bid/9667 certain versions of misSearch contains a buffer overflow vulnerability which allow an attacker to ...
2004-05-12	initial questbook "advanced questbook 2.2 now..."	Advanced Questbook v2.2 has an SQL injection problem which allows unauthorized access. Attackers 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 dynamic web application. VP-ASP is a customizable, dynamic solution for

Google Hacking Database (GHDB)

<http://www.hackersforcharity.org>

Category

- Virus Online Service
- Virus Online Device
- Vulnerable Servers
- Network or Vulnerability sites
- File containing password
- Page containing login pages
- Page containing login ports
- Page containing login forms
- File containing passwords

Google Hacking Database Categories

Footholds (31)

Examples of queries that can help a hacker gain a foothold in to a web server

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

Google

The screenshot shows the Google Advanced Search interface. At the top, it displays the URL https://www.google.com/advanced_search?hl=en&lg=1. Below the URL, the word "Google" is visible. The main area is titled "Advanced Search". It contains several input fields and dropdown menus:

- "Find pages with..." section:
 - "all these words":
 - "this exact word or phrase":
 - "any of these words":
 - "none of these words":
 - "numbers ranging from": to
- "Then narrow your results by...":
 - language:
 - region:
 - last update:
 - site or domain:
 - terms appearing:
 - SafeSearch:
 - reading level:
 - file type:
 - usage rights:
- A blue "Advanced Search" button at the bottom right.

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

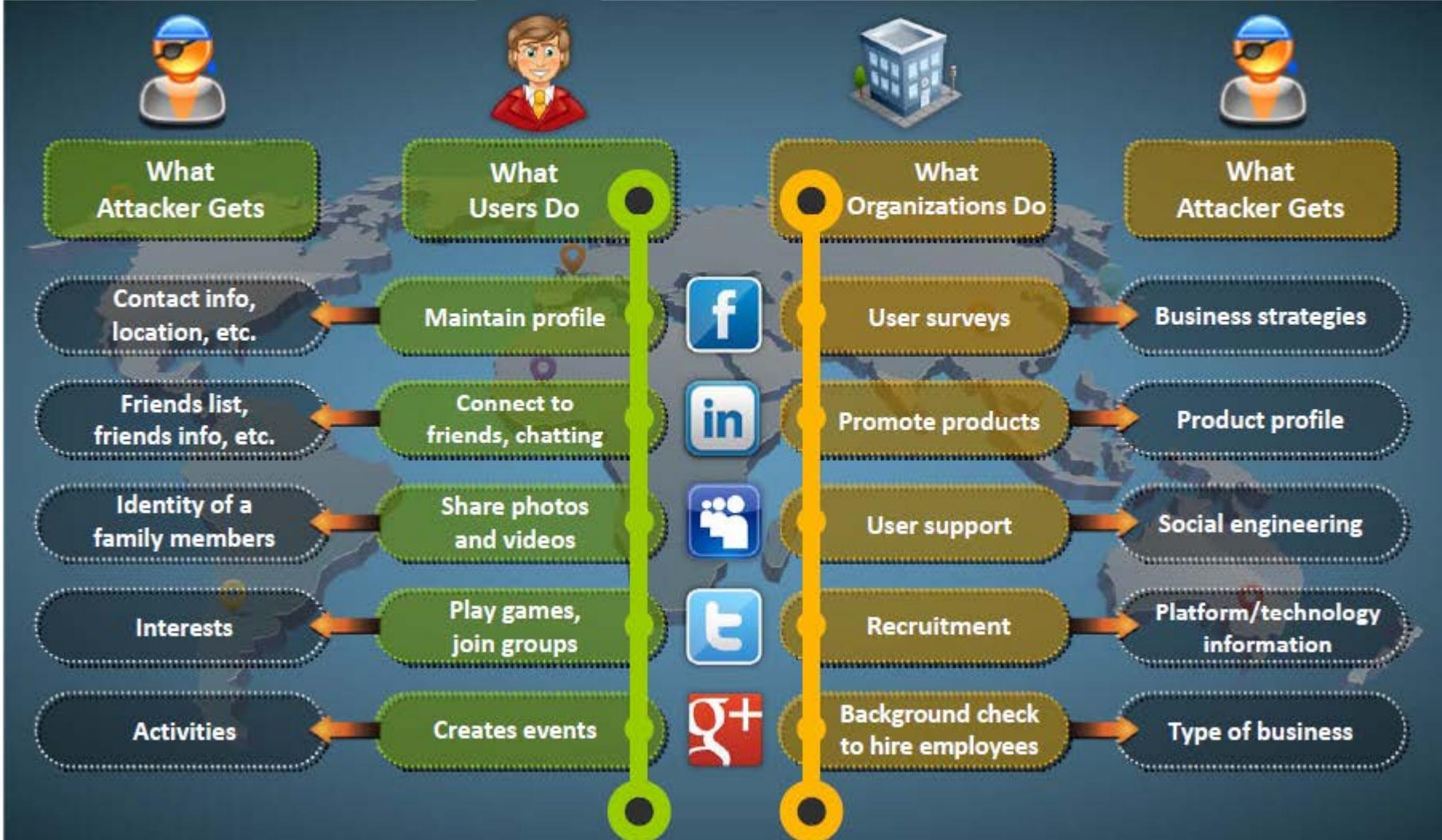


Employees may **post personal information** such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.



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

The screenshot shows the Burp Suite Free Edition v1.5 interface. The main window displays a list of host entries on the left, including various Microsoft domains like http://iis0.microsoft.com, http://iis1.microsoft.com, and http://iis2.microsoft.com. On the right, there is a table with columns: Host, Method, URL, Params, Status, Length, MIME type, and Title. Two rows are visible: one for http://www.juggboy.com with a GET method and an empty URL, and another for http://www.juggboy.com with a GET method and a URL of index.html. Below the table, there are tabs for Request, Response, Raw, Headers, and Mix. The Headers tab is active, showing detailed HTTP headers for the selected entry. The User-Agent header is listed as Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/29.0.1547.62 Safari/537.36. Other headers shown include Accept, Accept-Encoding, Accept-Language, and Date.

<http://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
- Script type

```
<html class="en-us no-js" lang="en" dir="ltr" xmlns:hl="urn:schemas-microsoft-com:icon:1.0">
```

The screenshot shows the raw HTML source code of the Microsoft homepage. It includes meta tags for character encoding and viewport settings, a title referring to Microsoft Home Page | Devices and Services, and numerous links to shared CSS and JavaScript files located at <http://i.microsoft.com>. The source code also contains comments about third-party scripts and code linked to or referenced from the website.

Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used



The screenshot shows a 'Cookies and site data' window from a browser. It lists cookies for several sites, with detailed information for each cookie such as name, content, domain, path, and creation date. The table includes columns for Site, Locally stored data, Remove, and Search cookies.

Site	Locally stored data
microsoftto.112.267.net	1 cookie
hollywood.112.267.net	1 cookie
idthis.com	6 cookies
static.adthearty.com	2 cookies
hdinteras.com	2 cookies
adminuser.com	1 cookie
adnext.fr	8 cookies
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**

The image displays two software interfaces side-by-side. On the left is the 'GSA Email Spider v7.08 - DEMOVERSION' interface, showing a list of URLs and their status (e.g., 200 OK, 301 Moved Permanently). A cartoon spider icon is visible in the bottom left corner. The URL list includes various domains like pedo.com, pedo.ca, and microsoft.com. On the right is the 'Web Data Extractor 8.3' interface, showing a list of extracted data items such as titles, keywords, and descriptions for Microsoft's website. Both interfaces have a toolbar at the top with various buttons and a progress bar at the bottom.

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

<http://www.webextractor.com>

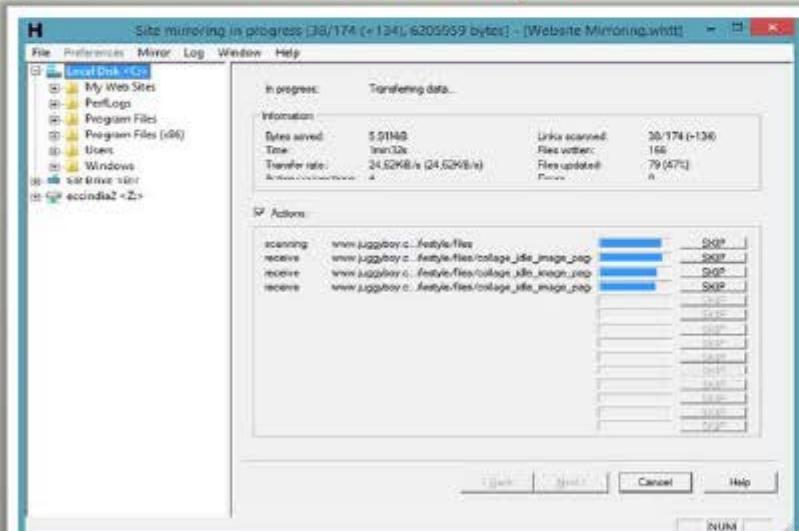
Mirroring Entire Website

CEH
Certified Ethical Hacker

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

CEH
Certified Ethical Hacker



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>



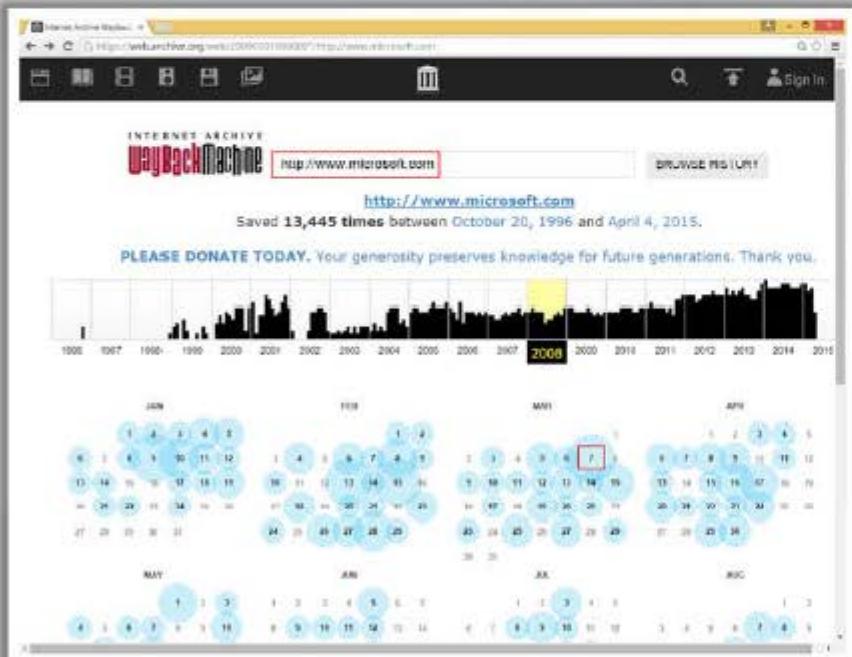
Hooeey Webprint

<http://www.hooeeywebprint.com>

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



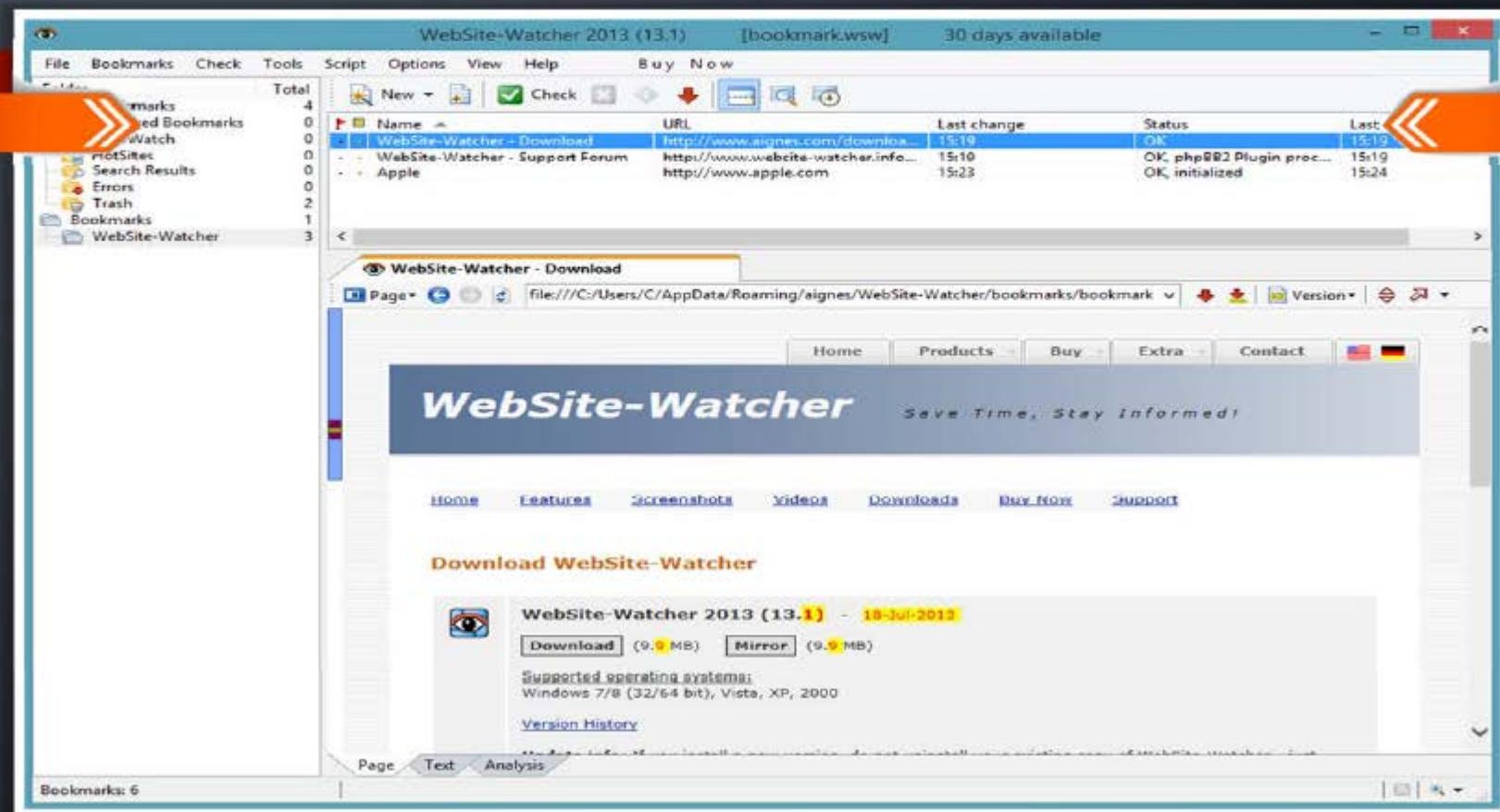
Internet Archive's Wayback Machine allows you to visit **archived versions** of websites



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 q7cs
          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 (mr.google.com: 10.224.205.137 as permitted sender) smtp.mailheader.i=[REDACTED]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
          by 10.224.205.137 with SMTP id fa9mr8578570qab.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+ghh7OkPjkx+Tt/iAC1
                b=KguZLTLfg2+QZXzKex1NnvRcnD/+P4+Nk5NKSPTG7uHXDs9fv/hGH46e2P+75MxDR8
                  b1PK3ej3UF/CsaBZWDT0XLaK0AGrP3BoT92MCZFxeUUQ9uwL/xHALSnceUIEEEeKGqOC
                  oa9hd59D3oXI8KAC7zmkb1GzXmV4D1WffCL894RaMBOUoMzRwOWWIib95aII38cqtlfP
                  ZhrWFKh5xSn2XsE73xZPEYzp7yecCeQuYZNGs1KxcO7xQjeZuw+HWK/vR6xChDJaP24
                  K5ZAfYZmkIKFx+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 Jun 2013 21:24:00 -0700 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhIE4Ber2cv>
References: <CAOYWATT1zdDXE3o8D2rhIE4Ber2MtV0uhro6r+7Mu7c8ubp8Eq@mail.gmail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAMSwvoXT0qEjnFw8WJdSzQhNnO=EMJcgfjX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ... SOLUTIONS ::
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

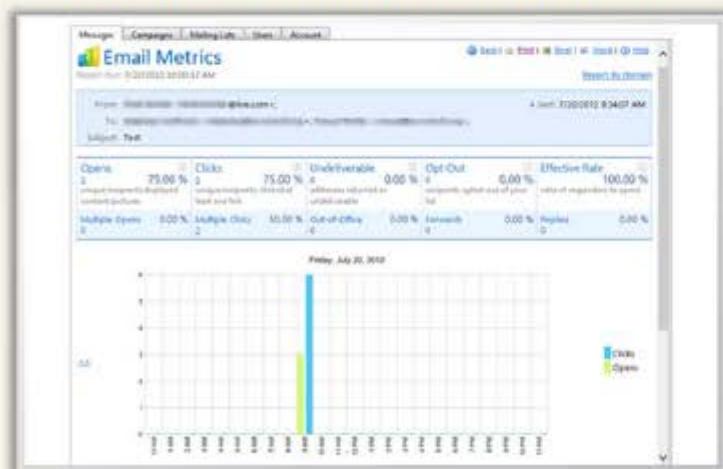
Sender's full name

Email Tracking Tools

C|EH
Certified Ethical Hacker



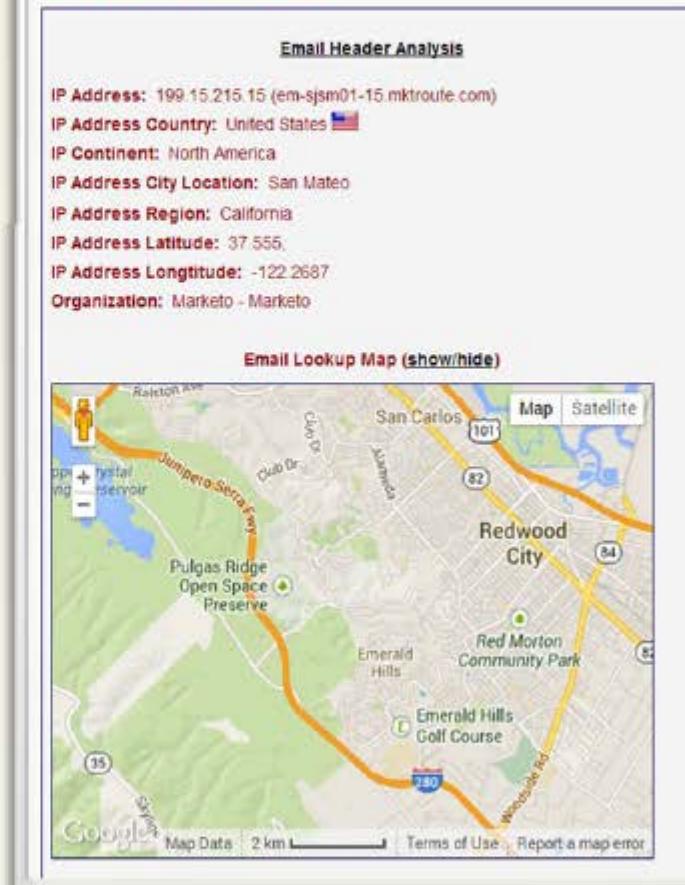
eMailTrackerPro (<http://www.emailtrackerpro.com>)



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?

CEH
Certified Ethical Hacker



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

CEH
Certified Ethical Hacker

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>



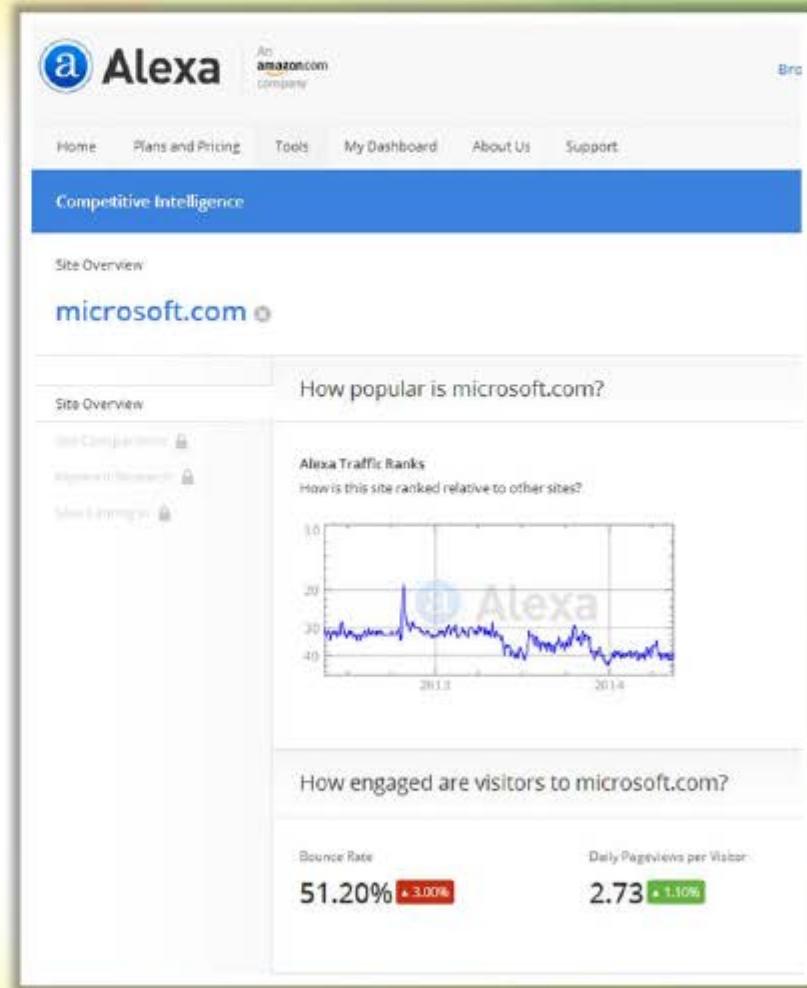
Monitoring Website Traffic of Target Company



- Attacker uses website traffic monitoring tools such as **web-stat**, **Alexa**, **Monitis**, etc. to collect the information about target company



- 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

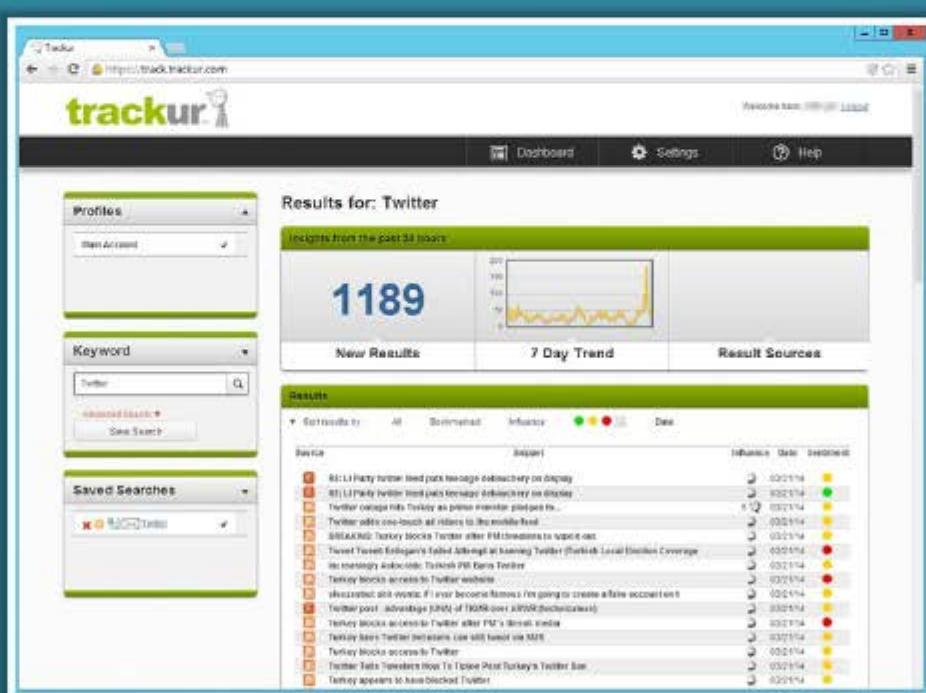
CEH



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

An attacker makes use of ORM tracking tools to:

- Track company's online reputation
 - Collect company's search engine ranking information
 - Obtain email notifications when a company is mentioned online
 - Track conversations
 - Obtain social news about the target organization



<http://www.trackur.com>

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

CEH
Certified Ethical Hacker

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)

ARIN
American Registry for Internet Numbers

AFRINIC
The African Network Information Centre

RIPE NCC

LAC

APNIC



WHOIS Lookup Result Analysis

C|EH
Certified Ethical Hacker

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: Washington - Seattle - Akamai Technologies Inc.

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

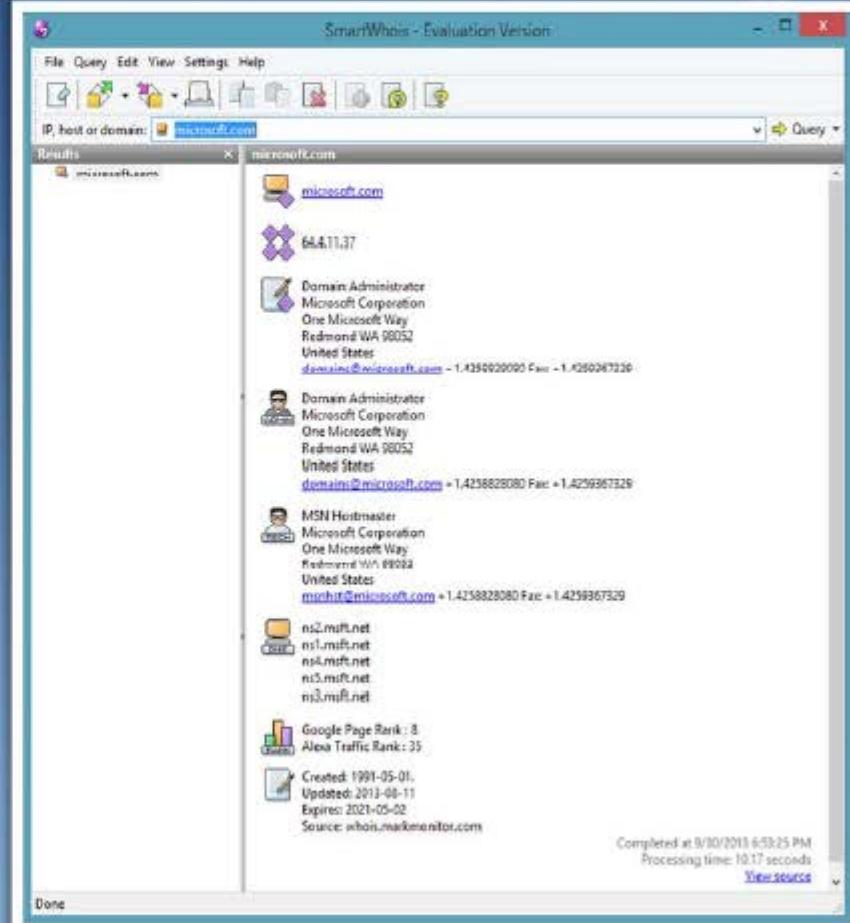
Domain Status: Registered And Active Website

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

<http://whois.domaintools.com>



<http://www.tamos.com>

WHOIS Lookup Tools

CEH
Certified Ethical Hacker



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.whoisalyzer.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>



BetterWhois

<http://www.betterwhois.com>



Whois Online

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



Web Wiz

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



Network-Tools.com

<http://network-tools.com>



Whois

<http://tools.whois.net>



DNSstuff

<http://www.dnsstuff.com>



Network Solutions Whois

<http://www.networksolutions.com>



WebToolHub

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



UltraTools

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

WHOIS Lookup Tools for Mobile



DNS Tools

DNS Report

Domain

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.gtid-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.

<https://www.dnssniffer.com>

UltraTools Mobile

UltraTools™ neuscar DASHBOARD

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** **GeoIP Lookup**

<https://www.ultratools.com>

Whois® Lookup Tool

whois

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

<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

C|EH
Certified Ethical Hacker

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	96.138.253.109	1800s (00:30:00)
yahoo.com	IN	A	206.190.36.45	1800s (00:30:00)
yahoo.com	IN	A	96.139.183.24	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.vipne1.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] refered to f.gld-servers.net
Searcing for microsoft.com ANY Record at f.gld-servers.net [192.35.61.30] refered 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: nsinhist.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

CEH
Certified Ethical Hacker



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>

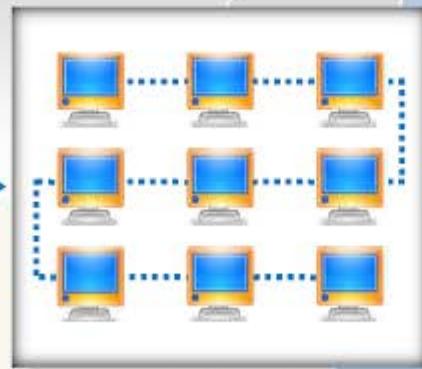
Locate the Network Range

CEH
Certified Ethical Hacker

- 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)**



Attacker



Network

Network Whois Record

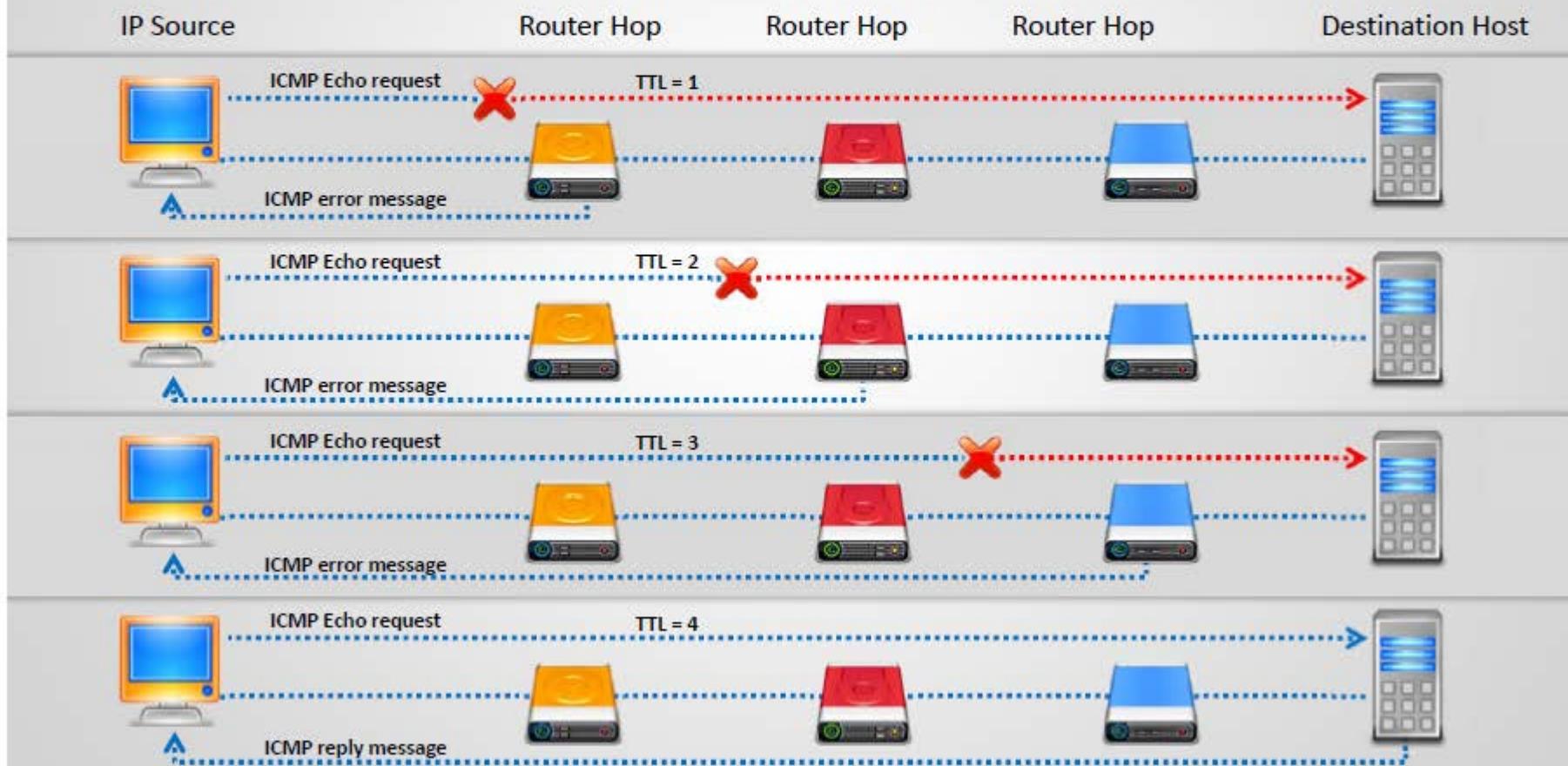
Network	
NetRange	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET207-46-0-1
Parenet	NET207 (NET-207-0-0-0)
Net Type	Direct Assignment
Origin AS	
Organization	Microsoft Corporation (MSFT)
Registration Date	1997-03-31
Last Updated	2013-08-20
Comments	
RESTful Link	http://whois.arin.net/restnet/NET-207-46-0-1
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://icam.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: milcc@microsoft.com
	For routing, peering or DNS issues, please contact: contact@microsoft.com

Queried
whois.arin.net with
"207.46.232.182"

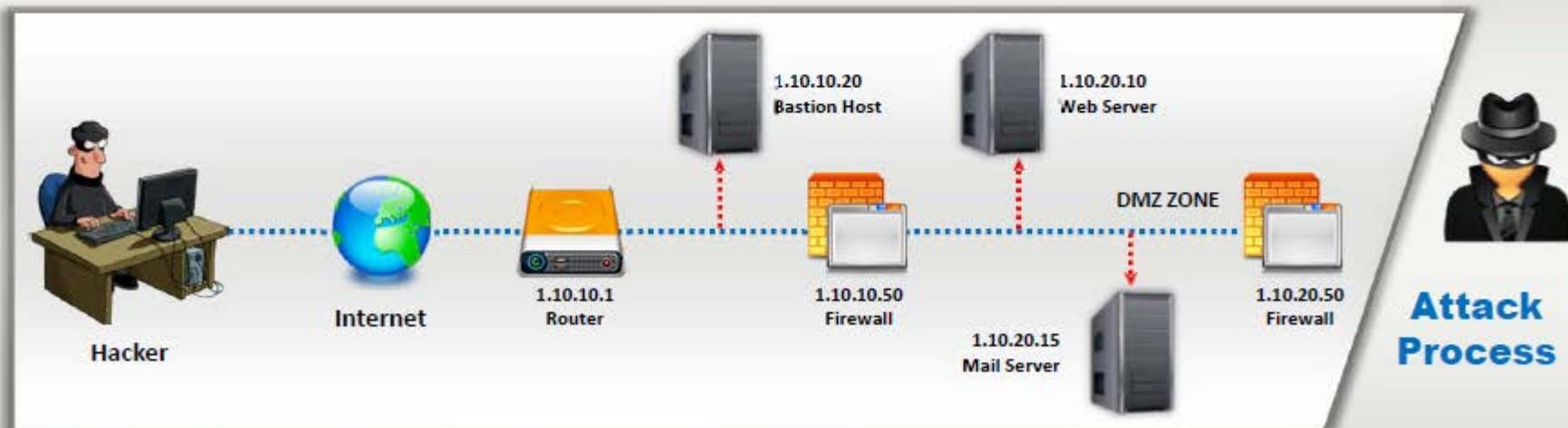
Traceroute

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



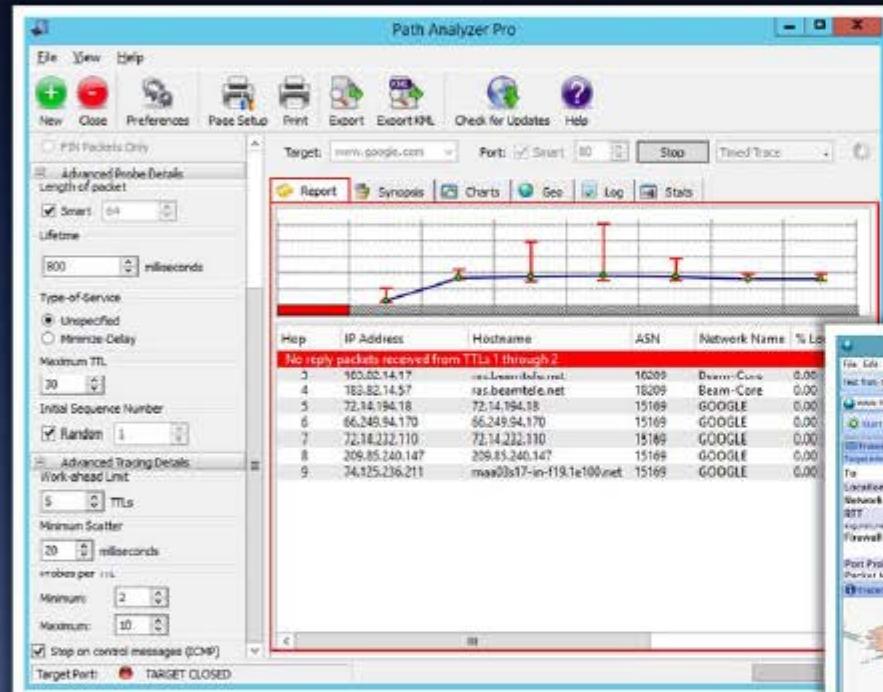
Traceroute Analysis

- 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

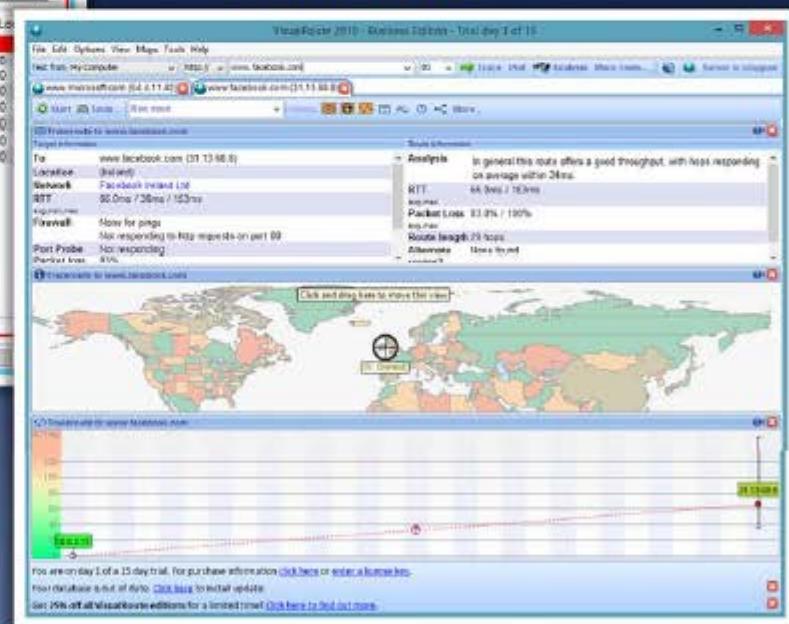
Path Analyzer Pro



<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

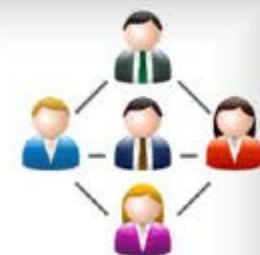


- 1 Footprinting through Search Engines
- 2 Footprinting Using Advanced Google Hacking Techniques
- 3 Footprinting through Social Networking Sites
- 4 Website Footprinting
- 5 Email Footprinting
- 6 Competitive Intelligence
- 7 WHOIS Footprinting
- 8 DNS Footprinting
- 9 Network Footprinting
- 10 Footprinting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

Footprinting through Social Engineering

CEH
Certified Ethical Hacker

- 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

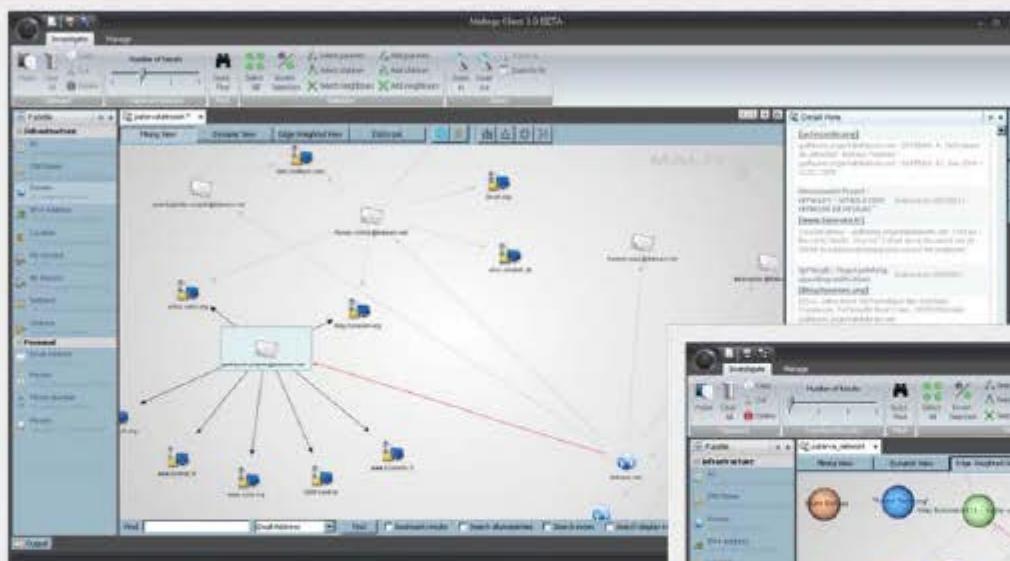
- Dumpster diving is **looking for treasure in someone else's trash**
- It involves collection of **phone bills, contact information, financial information**, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.



Module Flow

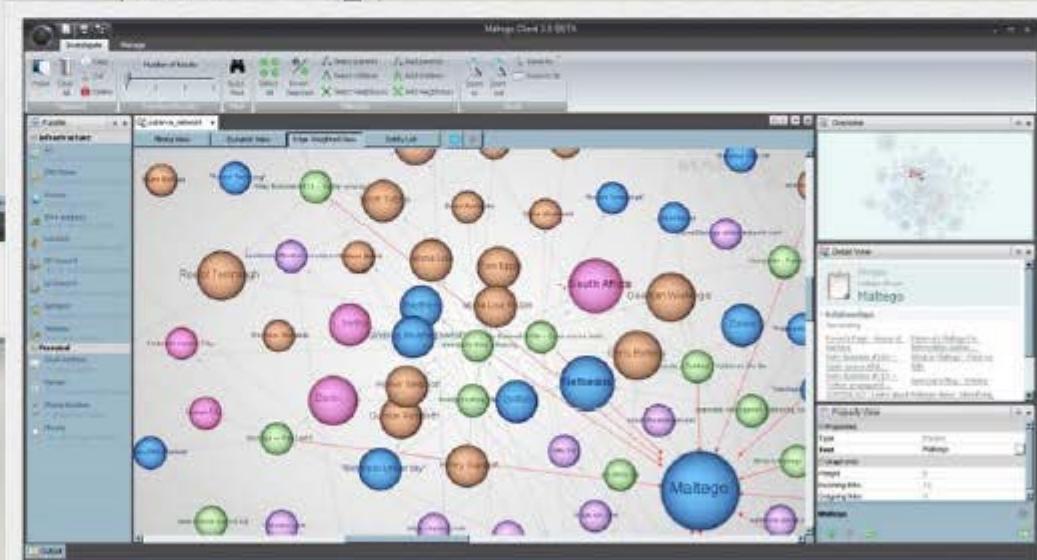


Maltego is a program that can be used to determine the **relationships and real world links** between people, groups of people (social networks), companies, organizations, websites, Internet infrastructure, phrases, documents, and files



Internet Domain

<http://www.paterva.com>



Personal Information

Footprinting Tool: 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 screenshot shows two terminal windows on a Kali Linux desktop. The left window displays the Recon-ng interface with a list of modules: User modules, Reporting modules, Sensors modules, Administration modules, and Discovery modules. The right window shows the results of a footprinting operation against the ECOUNCIL.ORG domain.

Left Terminal (Recon-ng Interface):

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

Right Terminal (Footprint Results):

```
root@kali:~# Set Apr 4, 3:16 AM
root@kali:~# Applications Places
root@kali:~# ECOUNCIL.ORG
root@kali:~# URL: http://searchdns.netcraft.com/?restriction=site%28ends%2Bwith%29account.org
store.account.org
ciso.account.org
aspen.account.org
academia.account.org
www.account.org
portal.account.org
vesta.account.org
ilabs.account.org
foundation.account.org
iclass.account.org
cert.account.org
frank.account.org
root@kali:~# SUMMARY
root@kali:~# 12 total (12 new) hosts found.
[recon-ng][ecouncil.org][netcraft] > show hosts
root@kali:~#
```

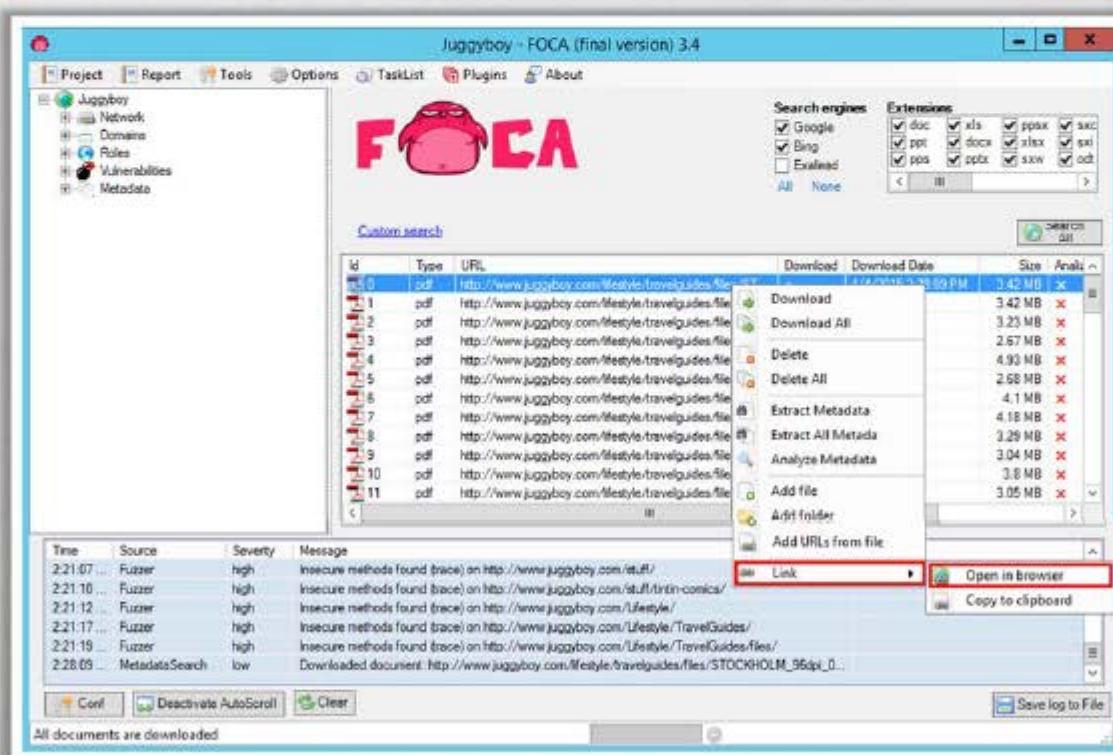
rowid	host	ip_address	region	country	latitude	longitude	module
1	store.account.org						netcraft
2	ciso.account.org						netcraft
3	aspen.account.org						netcraft
4	academia.account.org						netcraft
5	www.account.org						netcraft
6	portal.account.org						netcraft
7	vesta.account.org						netcraft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

```
[recon-ng][ecouncil.org][netcraft] >
root@kali:~#
```

<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

CEH
Certified Ethical Hacker



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



1

**Footprinting
Concepts**

2

**Footprinting
Methodology**

3

**Footprinting
Tools**

4

**Footprinting
Countermeasures**

5

**Footprinting
Penetration
Testing**

Footprinting Countermeasures

CEH
Certified Ethical Hacker



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



1

Footprinting
Concepts

2

Footprinting
Methodology

3

Footprinting
Tools

4

Footprinting
Countermeasures

5

Footprinting
Penetration
Testing

Footprinting Pen Testing



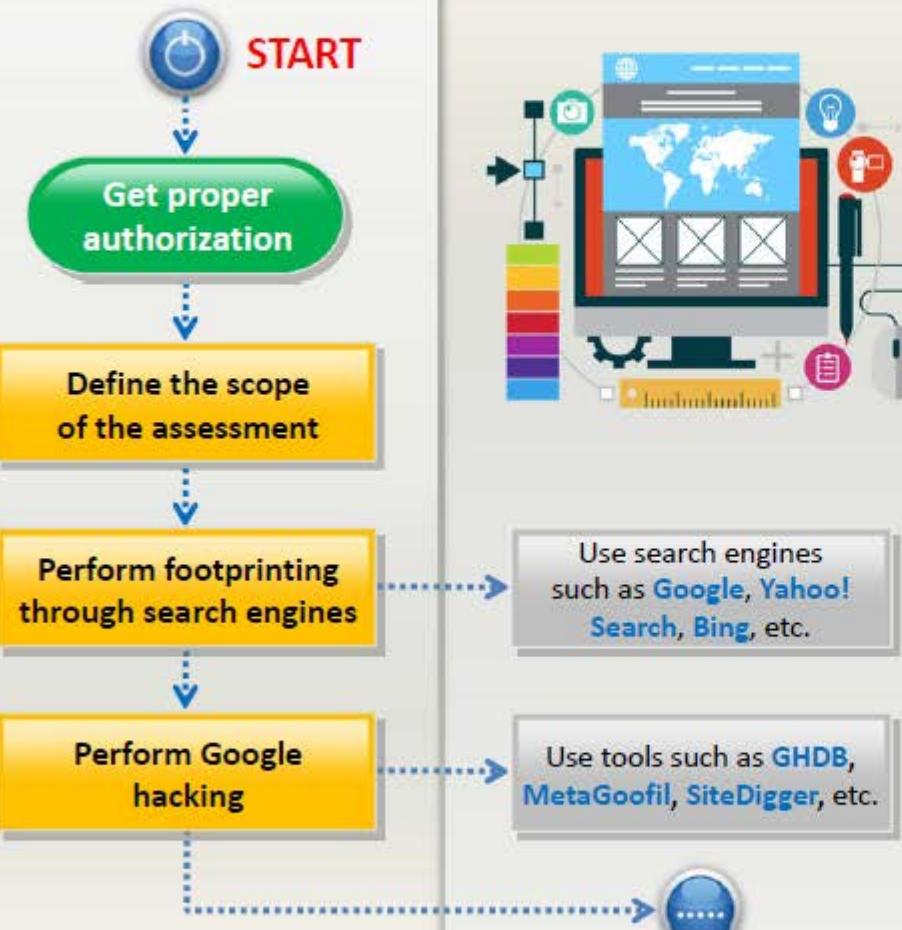
- Footprinting pen testing is used to **determine organization's publicly available information**
- The tester attempts to gather as much information as possible about the target organization from the **Internet and other publicly accessible sources**



Footprinting Pen Testing

(Cont'd)

C|EH
Certified Ethical Hacker



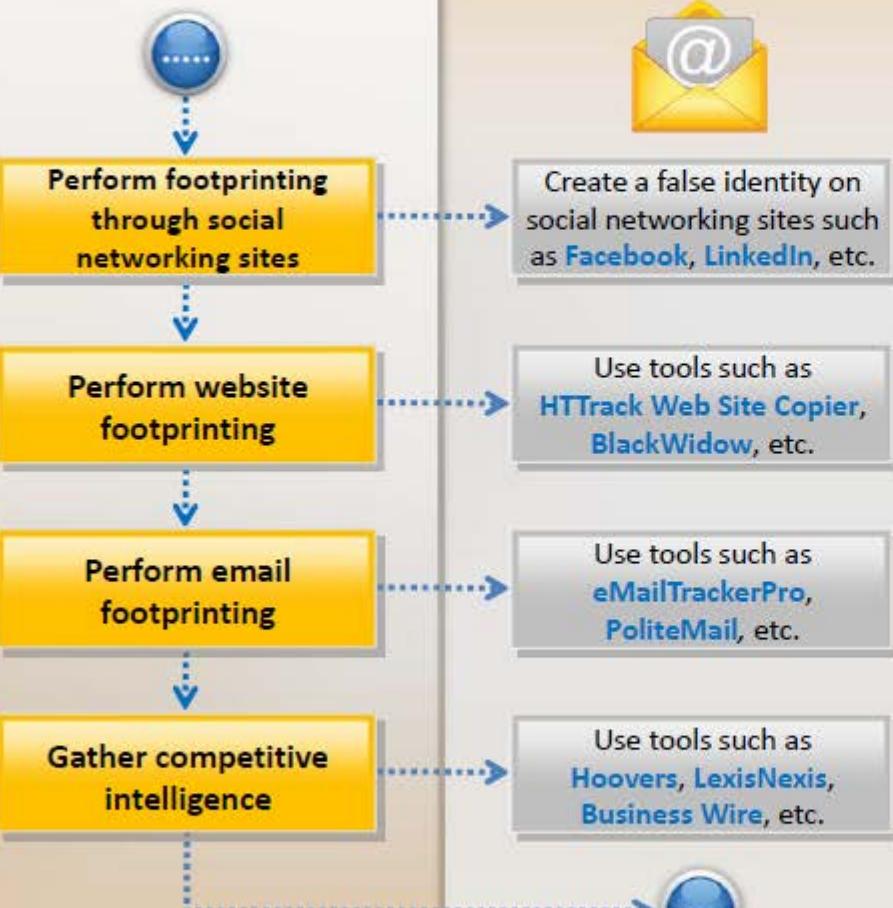
- Get proper authorization and define the scope of the assessment
- Footprint search engines such as **Google**, **Yahoo! Search**, **Ask**, **Bing**, **Dogpile**, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social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



Footprinting Pen Testing

(Cont'd)

C|EH
Certified Ethical Hacker

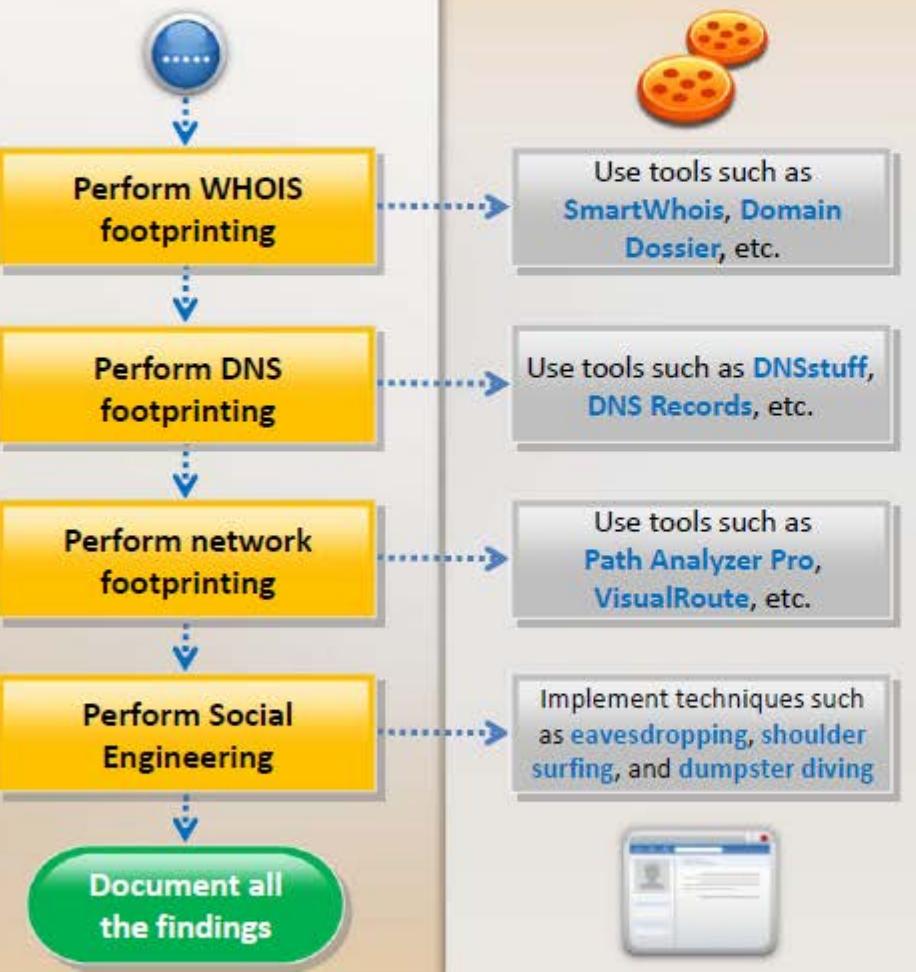


- Gather target organization employees information from their personal profiles on social networking sites such as **Facebook**, **LinkedIn**, **Twitter**, **Google+**, **Pinterest**, etc. that assist to perform social engineering
- Perform website footprinting using tools such as **HTTrack Web Site 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)

C|EH
Certified Ethical Hacker



- 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:
- Project plans:
- Others:

Information obtained through WHOIS footprinting

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



Information obtained through network footprinting

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

Information obtained through DNS footprinting

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

Information obtained through social engineering

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

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