



Footprinting and Reconnaissance

Module 02

Unmask the **Invisible Hacker**.



Module Objectives



- 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

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

Reduce Focus Area

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

Identify Vulnerabilities

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

Draw Network Map

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

Objectives of Footprinting



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
- IDSes 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)



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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. lumiakonversationsuk.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. familysafety.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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

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 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	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. o15.officeidv.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.smcarta.com	unknown	July 1995	Microsoft-IIS/7.5	Windows Server 2008
358	msn.microsoft.com	unknown	September 1998	Microsoft-IIS/8.0	Citrix Netscaler
241	technet.microsoft.com	unknown	August 1999	Microsoft-IIS/8.0	Citrix Netscaler
-	www.microsoft.be	unknown	February 1999	Microsoft-IIS/7.5	unknown
-	adsreport.msn.com	unknown	March 2000	BigIP	FS BIG-IP
-	www.safelomon.com	unknown	October 1995	Microsoft-IIS/7.5	Windows Server 2008
185106	www.ian.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
-	www.microsoft.com	unknown	July 2008	Microsoft-IIS/7.6	Windows Server 2008
138898	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.mistbergpodcast.com	unknown	May 2000	Microsoft-IIS/7.5	Windows Server 2008
-	mobile.msn.com	unknown	March 2000	Microsoft-IIS/6.0	unknown

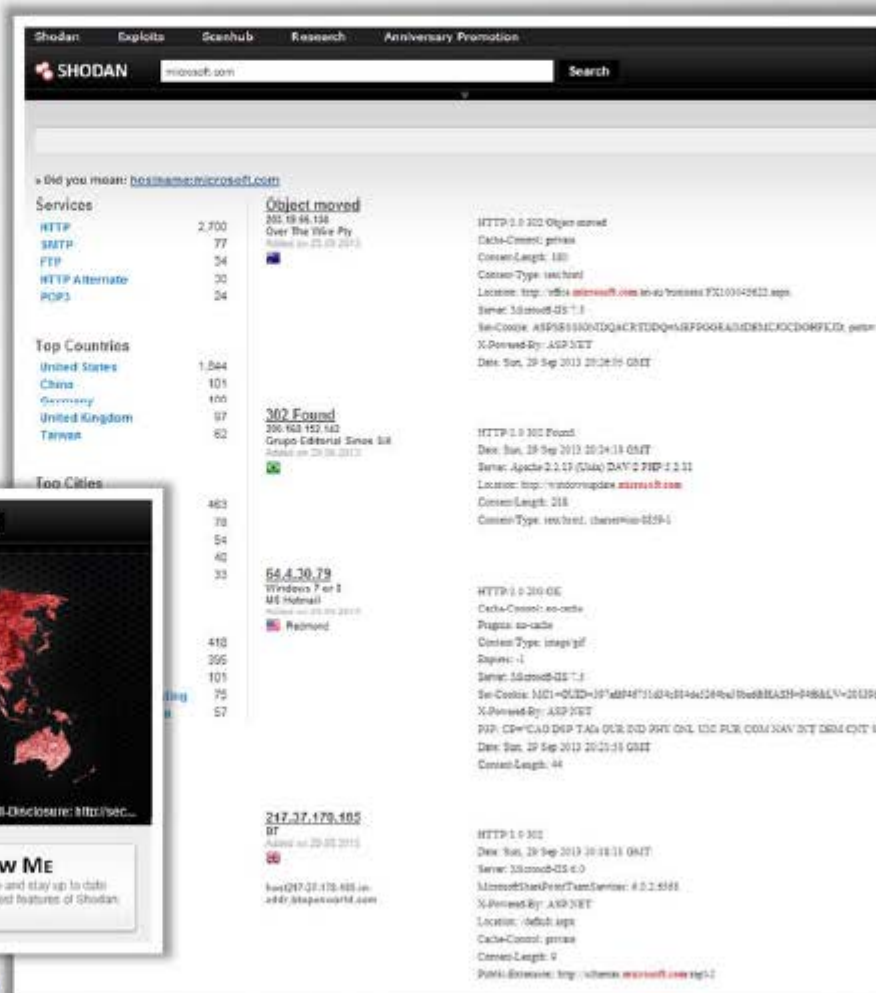
<http://www.netcraft.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction Is Strictly Prohibited.

Determining the Operating System (Cont'd)



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



<http://www.shodanhq.com>

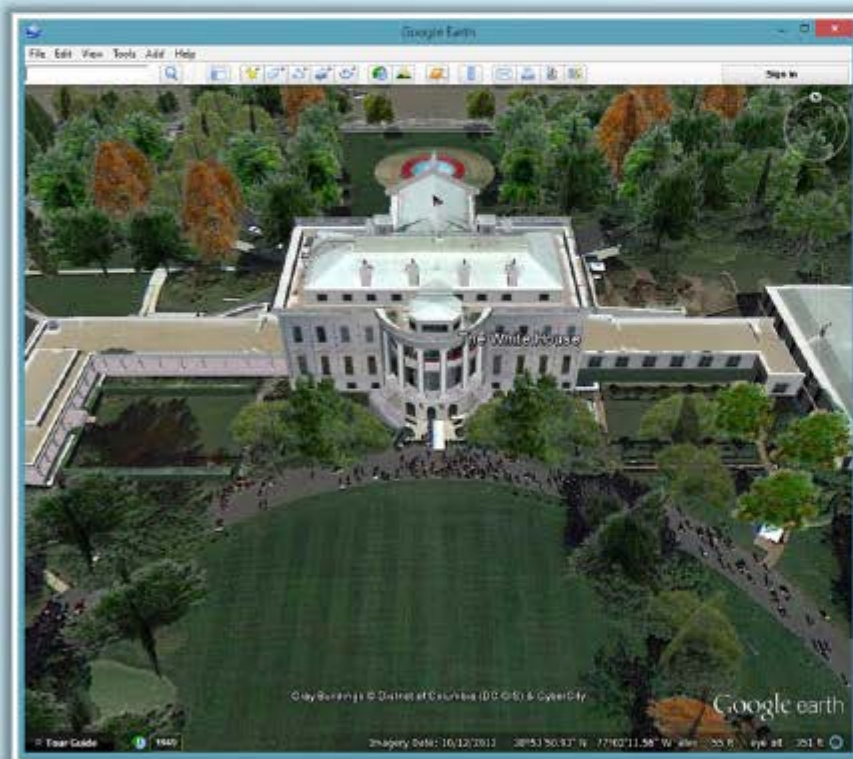
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

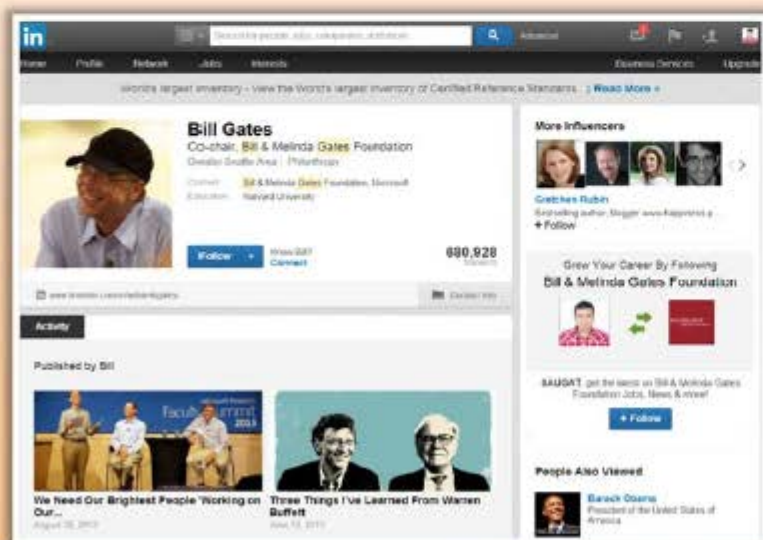


- Social networking sites are the great source of personal and organizational information
- Information about an individual can be found at various **people search websites**
- The people search returns the following **information about a person or organization**:



- Residential addresses and email addresses
- Contact numbers and date of birth
- Photos and social networking profiles

- Blog URLs
- Satellite pictures of private residences
- Upcoming projects and operating environment



<http://www.linkedin.com>



<https://pipl.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

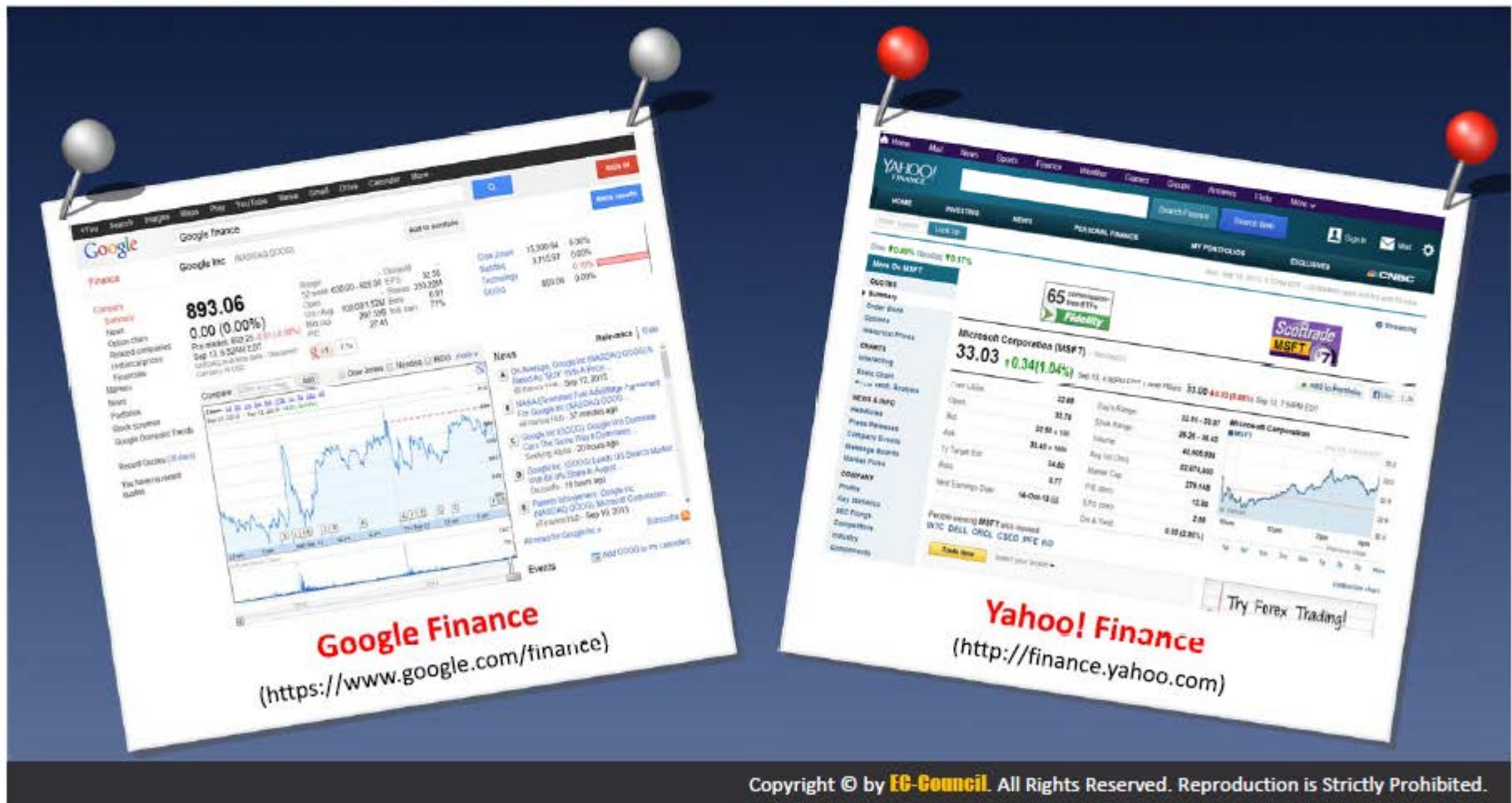
People Search **Online Services**

**AnyWho**<http://www.anywho.com>**PeopleSmart**<http://www.peoplesmart.com>**US Search**<http://www.ussearch.com>**Veromi**<http://www.veromi.net>**Intelius**<http://www.intelius.com>**PrivateEye**<http://www.privateeye.com>**411**<http://www.411.com>**People Search Now**<http://www.peoplesearchnow.com>**PeopleFinders**<http://www.peoplefinders.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.



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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 92668

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>

Google Alerts interface showing search query: Security News, Result type: Everything, How often: Once a day, How many: Only the best results, Deliver to: [redacted]@gmail.com. Buttons: CREATE ALERT, Manage your alerts.



Google Alert - Security News. 10 new results for Security News. News. Defenders forward deploy to secure Air Force assets. DIVOC: Airman 1st Class Christian Mejia, 378th Expeditionary Security Forces Squadron Fly Away Security Team member, Transit Center at Manas, Kyrgyzstan, ... See all stories on this topic. Homeland Security launches smartphone app to catch predators. Blast near security forces vehicle maims one in NWVA. Joliet eyes lighter security at new transportation center.

Information Gathering Using Groups, Forums, and Blogs



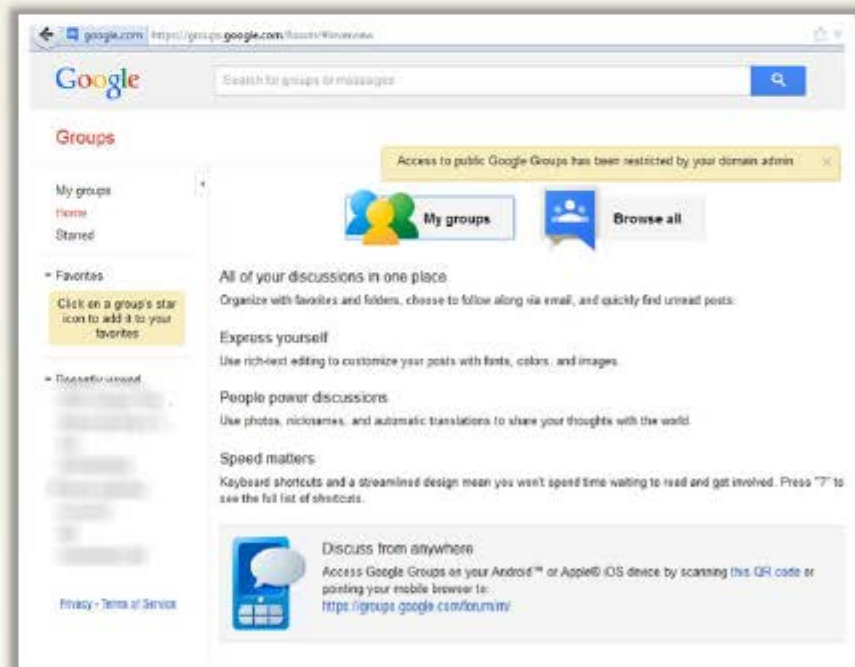
Groups, forums, and blogs provide sensitive information about a target such as **public network information**, **system information**, **personal information**, etc.



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



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**

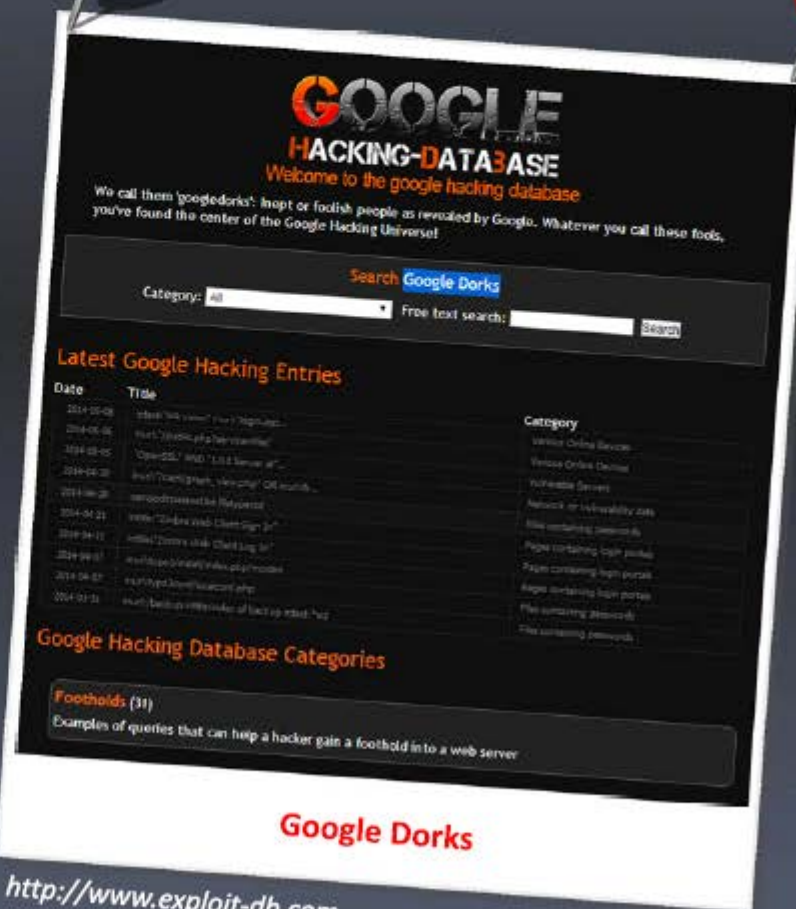
- [cache:]** > Displays **the web pages** stored in the Google cache
- [link:]** > Lists web pages that have **links to the specified web page**
- [related:]** > Lists web pages that are **similar** to a specified web page
- [info:]** > Presents some **information** that Google has about a particular 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



Google Hacking Database (GHDB)

<http://www.hackersforcharity.org>



Google Dorks

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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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 page in a web browser. The address bar displays the URL: https://www.google.com/advanced_search?hl=en&lg=1. The page title is "Advanced Search".

Find pages with...

- 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:

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

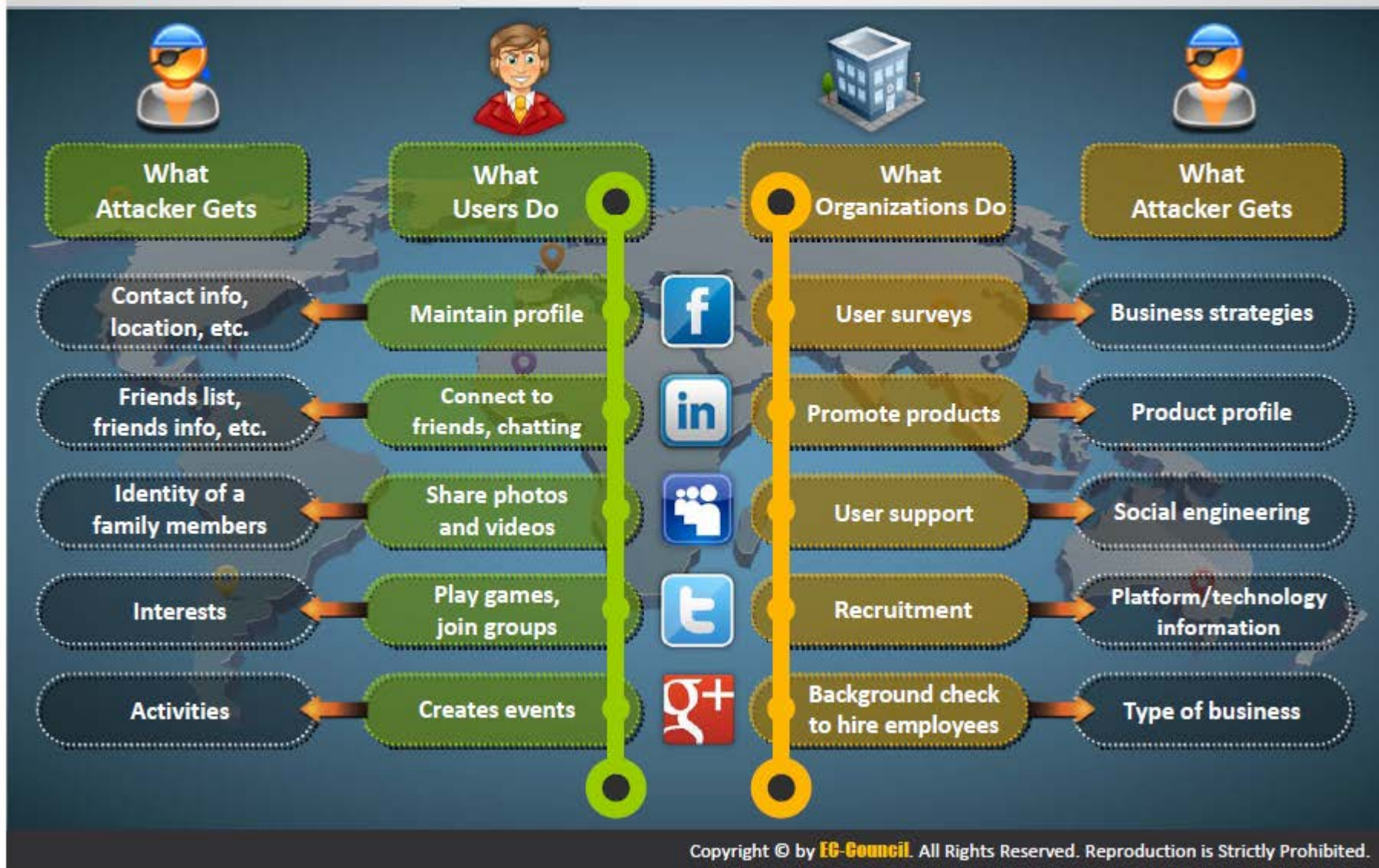


Employees may **post personal information** such as date of birth, educational and employment backgrounds, spouses names, etc. and information about their company such as potential clients and business partners, trade secrets of business, websites, company's upcoming news, mergers, acquisitions, etc.



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

CEH
Certified Ethical Hacker

1

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



2

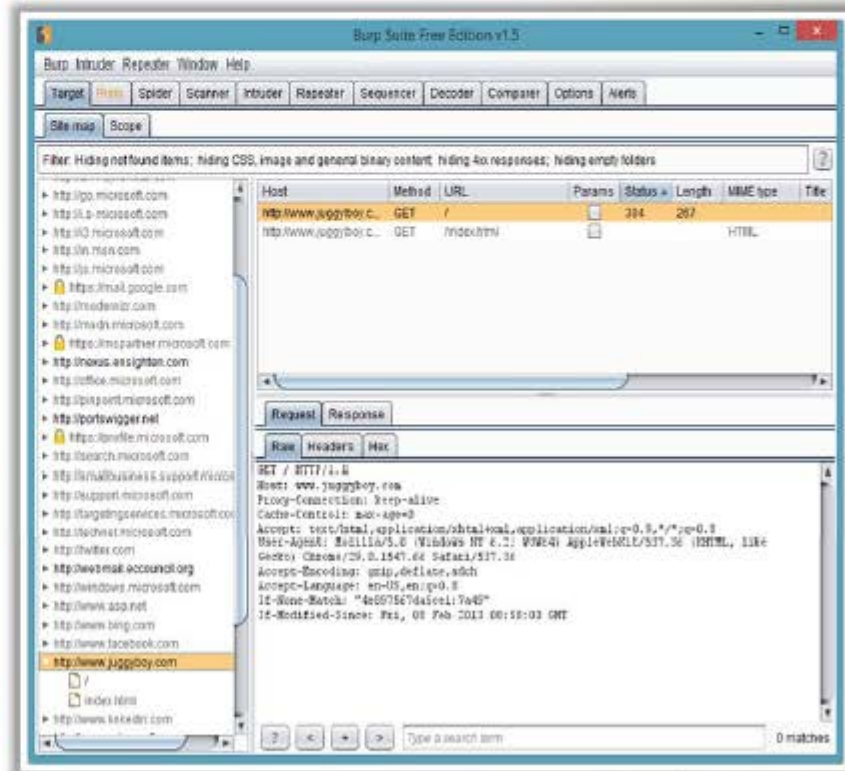
Browsing the target website may provide:

- 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



<http://portswigger.net>

Copyright © by **EG-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Website Footprinting

(Cont'd)



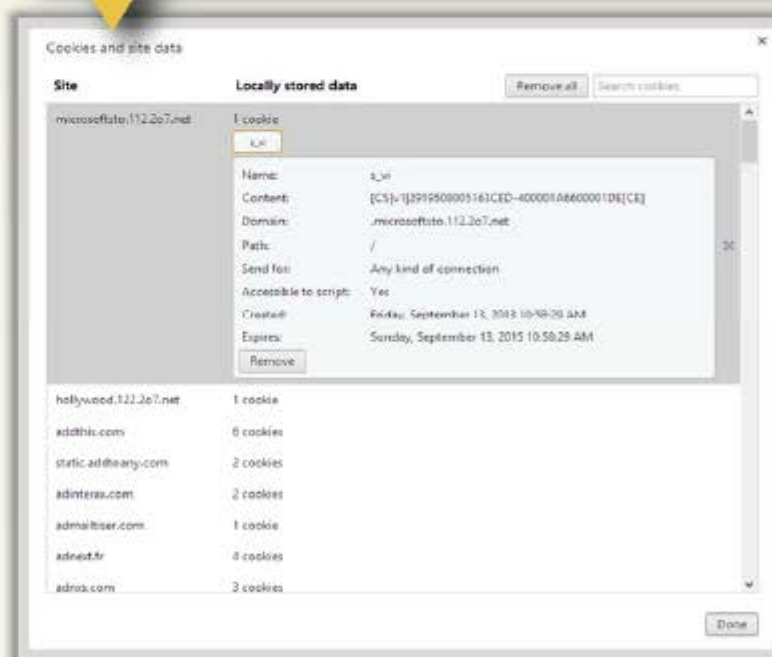
Examining HTML source provide:

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

```
<!--Third party scripts and code linked to or referenced from this website are licensed to you by the parties that own such code, not by Microsoft. See ASP.NET Ajax CDN Terms of Use - http://www.asp.net/ajaxlibrary/CDN.aspx.-->
<script type="text/javascript" src="http://i.s-microsoft.com/en-
```

Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used

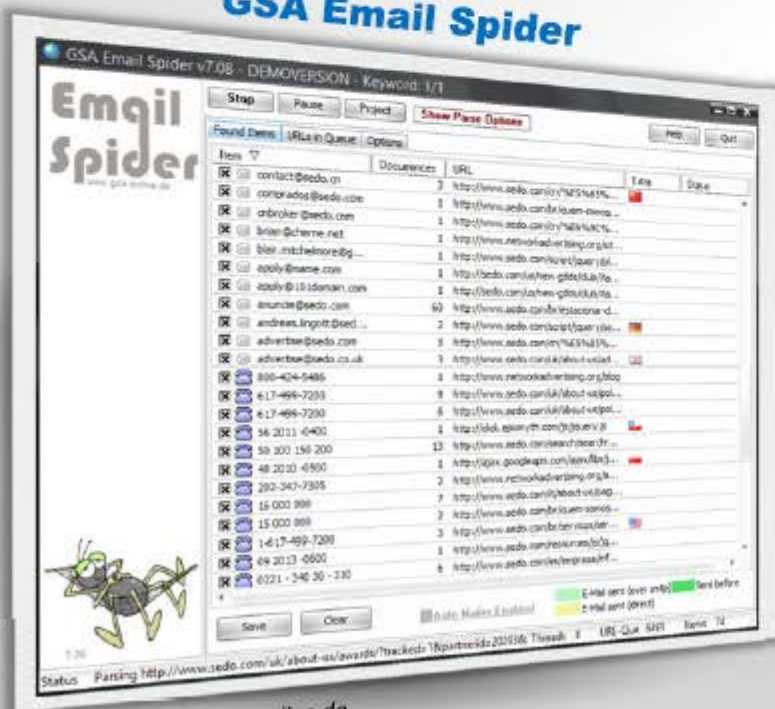


Website Footprinting using Web Spiders



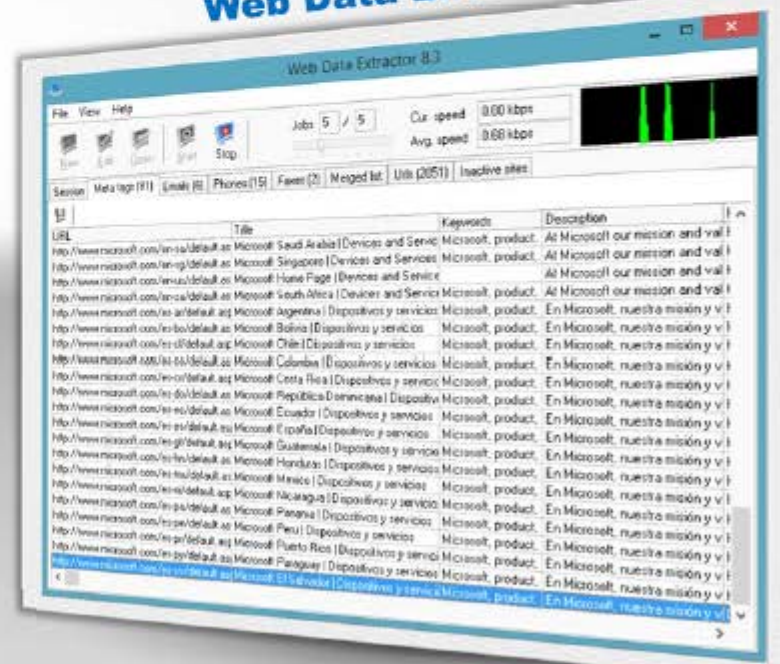
- Web spiders perform automated searches on the target website and collect specified information such as **employee names**, **email addresses**, etc.
- Attackers use the collected information to perform further **footprinting** and **social engineering attacks**

GSA Email Spider



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

Web Data Extractor



<http://www.webextractor.com>

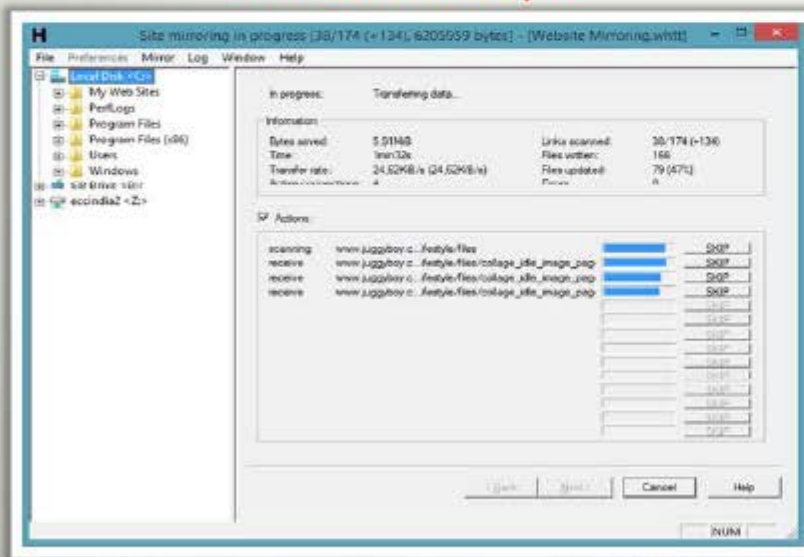
Mirroring Entire Website

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>)

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Website Mirroring Tools



BlackWidow

<http://softbytelabs.com>



PageNest

<http://www.pagenest.com>



NCollector Studio

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



Backstreet Browser

<http://www.spadixbd.com>



Website Ripper Copier

<http://www.tensons.com>



Offline Explorer Enterprise

<http://www.metaproducts.com>



Teleport Pro

<http://www.tenmax.com>



GNU Wget

<http://www.gnu.org>



Portable Offline Browser

<http://www.metaproducts.com>



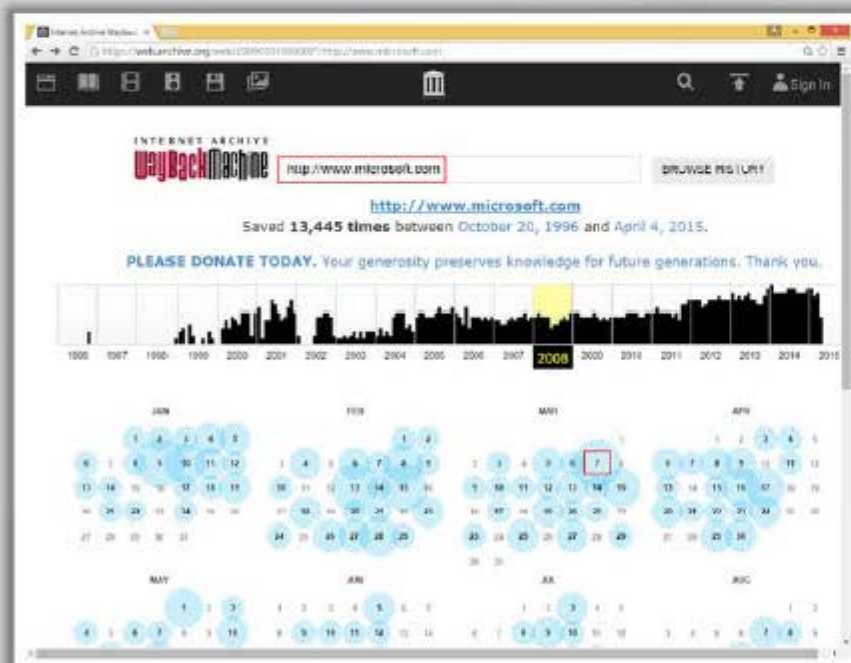
Hooey Webprint

<http://www.hooeywebprint.com>

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



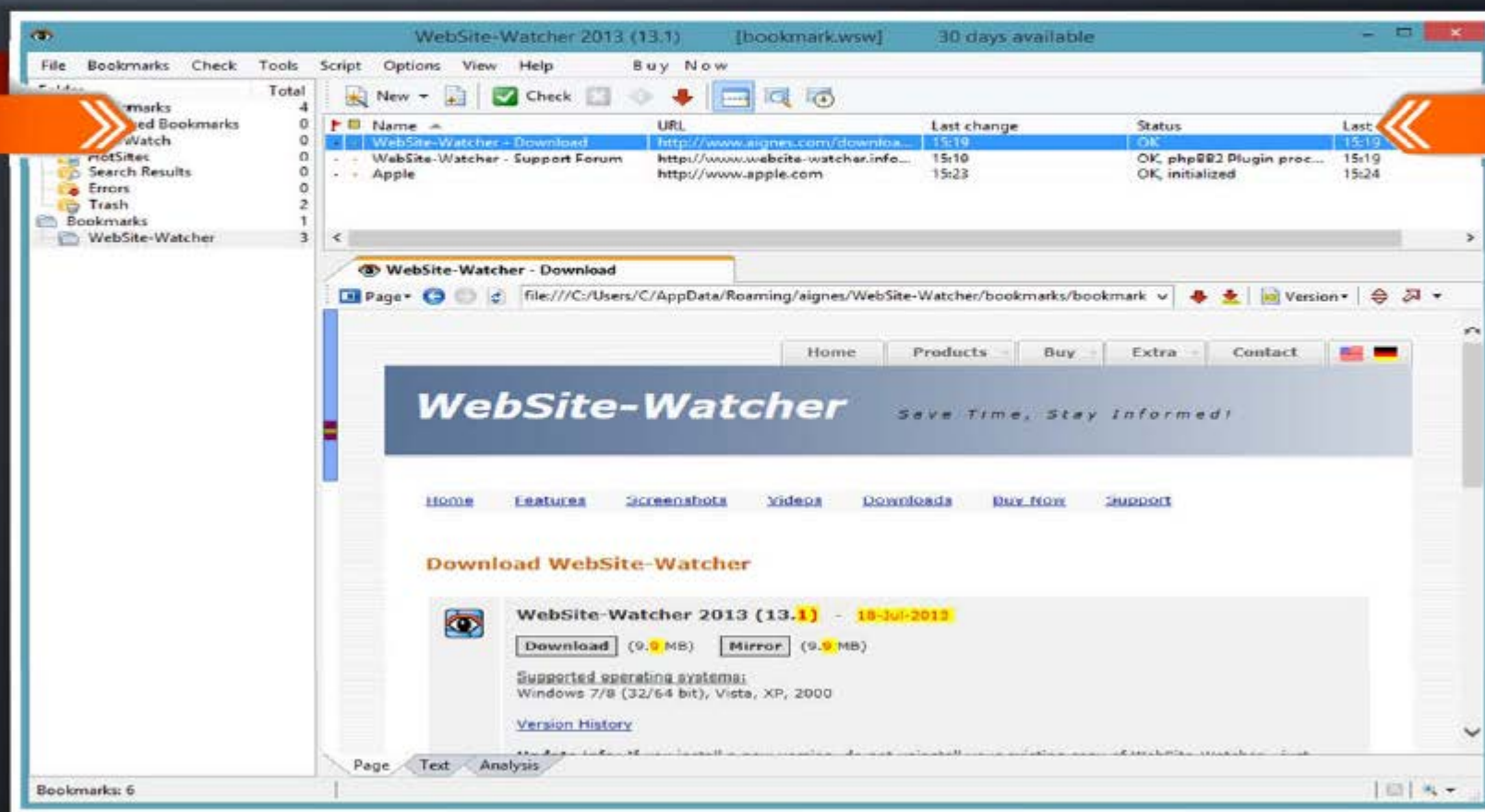
Internet Archive's Wayback Machine allows you to visit **archived versions of websites**



Monitoring Web Updates Using Website-Watcher



Website-Watcher **automatically checks web pages** for updates and changes



<http://aignes.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Web Updates Monitoring Tools



Change Detection

<http://www.changedetection.com>



OnWebChange

<http://onwebchange.com>



Follow That Page

<http://www.followthatpage.com>



Infominder

<http://www.infominder.com>



Page2RSS

<http://page2rss.com>



TrackedContent

<http://trackedcontent.com>



Watch That Page

<http://www.watchthatpage.com>



Websnitcher

<http://websnitcher.com>



Check4Change

<https://addons.mozilla.org>



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] designates 10.224.205.137 as permitted sender) client-ip=10.224.205.137;
Authentication-Results: mr.google.com; spf=pass (mail from [redacted]erma@gmail.com designates 10.224.205.137 as permitted sender) smtp.mail=[redacted]erma@gmail.com; dkim=pass header.i=[redacted]erma@gmail.com
Received: from mr.google.com ([10.224.205.137])
by 10.224.205.137 with SMTP id fq9mr8578570qab.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+QZXzZKexlNnvRcnD/+P4+Nk5NKSPtG7uHXDsFv/hGH46e2P+75MxDR8
blPK3eJ3Uf/CsaBZWDIT0XLAK0AGrP3Bot92MCZFxeUUQ9uwl/xHALSnkeUIEEeKGqOC
oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqt1fP
ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNgs1KxcO7xQjeZuw+HWK/vR6xChDjap24
K5ZafYZmkIKFX+VdLZqu7YGFzy6oHcuP16yS/C2fXHVdsuYamMT/yecvhCVo8Oq7FKt6
/Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9mr8578570qab.39.11040318;
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: <CAOYWATT1zdDXE3o8D2rhiE4Ber2ev@mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4Ber2MtV0uhro6r+7Mu7c8ubp8Eg@mail.gmail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAMSvoXT0qEjnfW8WJdSzhNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ... SOLUTIONS :::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]in@gmail.com,
[redacted] SOLUTIONS <[redacted]olutions@gmail.com>, [redacted]_er@yahoo.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>)

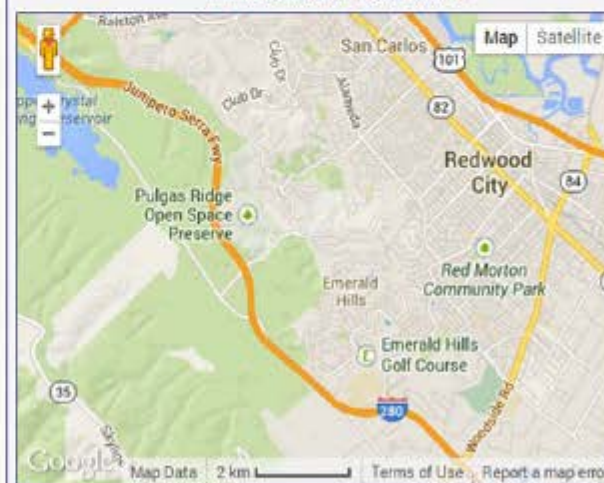
Email Lookup - Free Email Tracker

Trace Email - Track Email

Email Header Analysis

IP Address: 199.15.215.15 (em-sjsm01-15.mktroute.com)
 IP Address Country: United States
 IP Continent: North America
 IP Address City Location: San Mateo
 IP Address Region: California
 IP Address Latitude: 37.555
 IP Address Longitude: -122.2687
 Organization: Marketo - Marketo

Email Lookup Map (show/hide)



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

Email Tracking Tools

(Cont'd)

**Yesware**<http://www.yesware.com>**Zendio**<http://www.zendio.com>**ContactMonkey**<https://contactmonkey.com>**Pointofmail**<http://www.pointofmail.com>**Read Notify**<http://www.readnotify.com>**WhoReadMe**<http://whoreadme.com>**DidTheyReadIt**<http://www.didtheyreadit.com>**GetNotifly**<http://www.getnotifly.com>**Trace Email**<http://whatismyipaddress.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

Social engineering employees

06

02 Search engines, Internet, and online DB

Product catalogues and retail outlets

07

03 Press releases and annual reports

Analyst and regulatory reports

08

04 Trade journals, conferences, and newspaper

Customer and vendor interviews

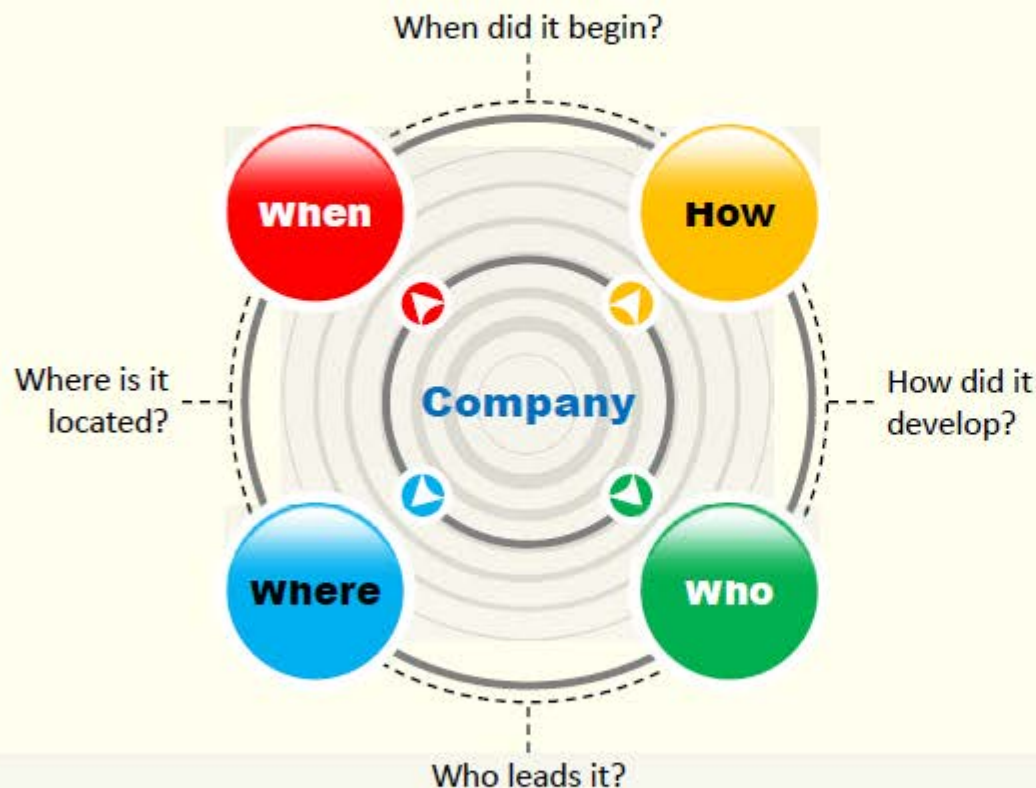
09

05 Patent and trademarks

Agents, distributors, and suppliers

10

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



Visit These Sites

01. EDGAR Database



<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>**Compete PRO™**<http://www.compete.com>**AttentionMeter**<http://www.attentionmeter.com>**AttentionMeter****Copernic Tracker**<http://www.copernic.com>**copernic****Jobitorial**<http://www.jobitorial.com>**SEMRush**<http://www.semrush.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

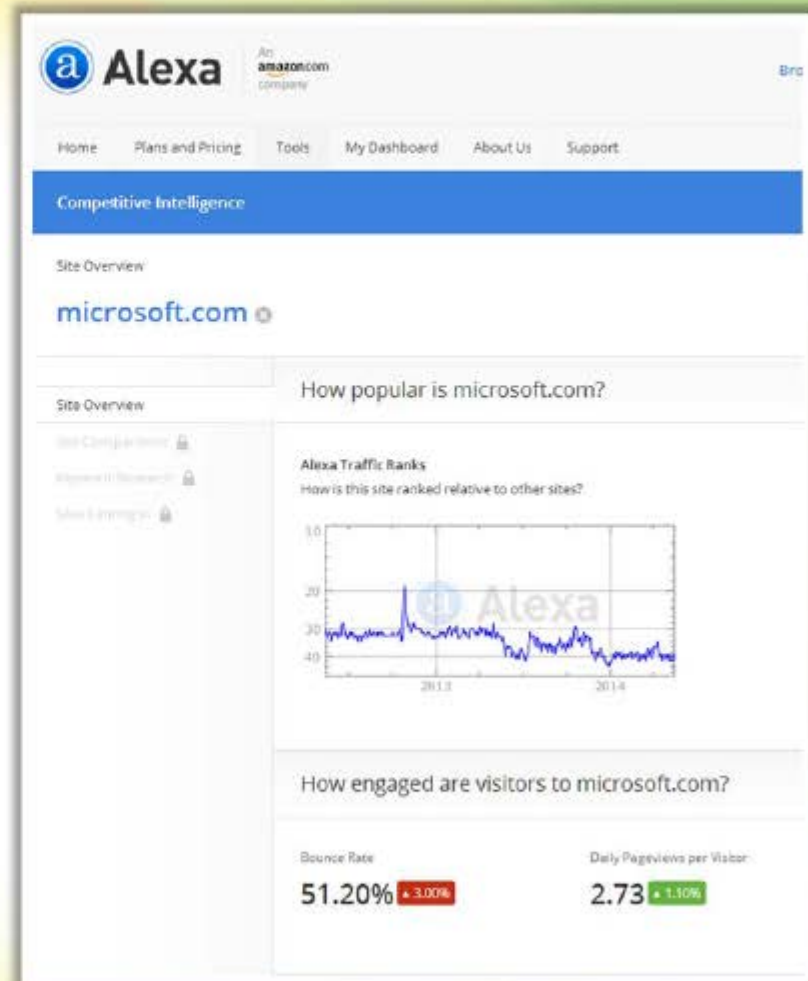
Page views

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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

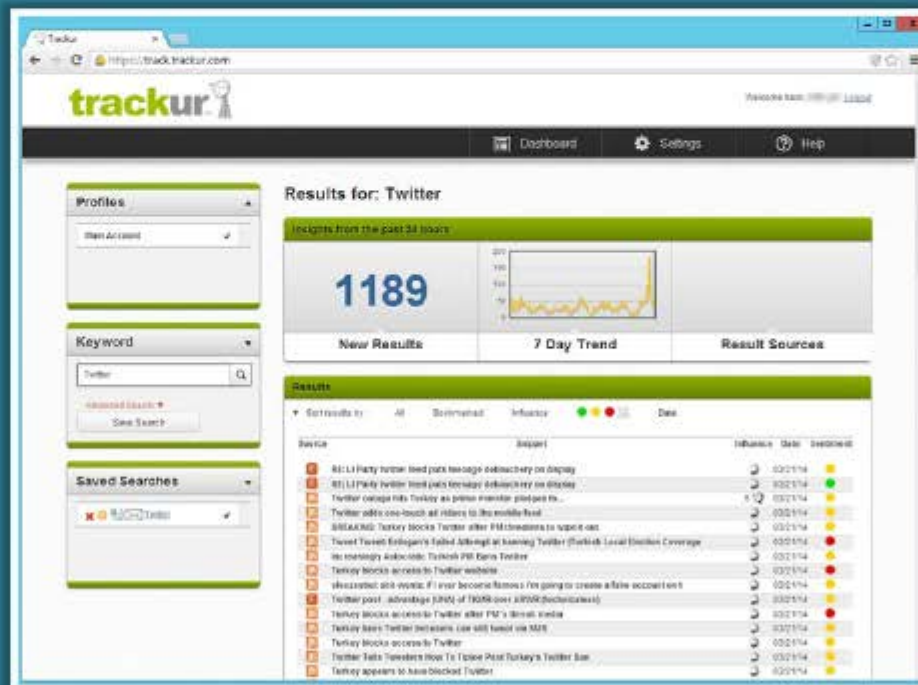
Tracking Online Reputation of the Target



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

An attacker makes use of ORM tracking tools to:

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



<http://www.trackur.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Tools for Tracking Online Reputation of the Target

**Rankur**<http://rankur.com>**Google Alerts**<http://www.google.com>**Social Mention**<http://www.socialmention.com>**WhosTalkin**<http://www.whostalkin.com>**ReputationDefender**<https://www.reputation.com>**PR Software**<http://www.cision.com>**Naymz**<http://www.naymz.com>**BrandsEye**<http://www.brandseye.com>**Brandyourself**<https://brandyourself.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	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	4 registrars
History	

<http://whois.domaintools.com>

SmartWhois - Evaluation Version

File Query Edit View Settings Help

IP, host or domain: Query

Results

microsoft.com

64.4.11.37

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
United States
domains@microsoft.com + 1.425020090 Fax: + 1.4250247220

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
United States
domains@microsoft.com + 1.4258828080 Fax: + 1.4258967329

MSN Hostmaster
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
United States
msnhst@microsoft.com + 1.4258828080 Fax: + 1.4258967329

ns2.msft.net
ns1.msft.net
ns3.msft.net
ns4.msft.net

Google Page Rank: 8
Alexa Traffic Rank: 25

Created: 1991-05-01
Updated: 2013-08-11
Expires: 2021-05-02
Source: whois.markmonitor.com

Completed at 8/30/2013 6:53:25 PM
Processing time: 10.17 seconds
[View source](#)

<http://www.tamos.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

WHOIS Lookup Tools

**LanWhols**<http://lantricks.com>**HotWhois**<http://www.tialsoft.com>**Batch IP Converter**<http://www.networkmost.com>**ActiveWhois**<http://www.johnru.com>**CallerIP**<http://www.callerippro.com>**WhoisThisDomain**<http://www.nirsoft.net>**Whols Lookup Multiple
Addresses**<http://www.sobolsoft.com>**SoftFuse Whois**<http://www.softfuse.com>**Whols Analyzer Pro**<http://www.whoisanalyzer.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/tn561381-whois-lookup.aspx>



Network-Tools.com

<http://network-tools.com>



UltraTools

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

WHOIS Lookup Tools for Mobile



DNS Tools



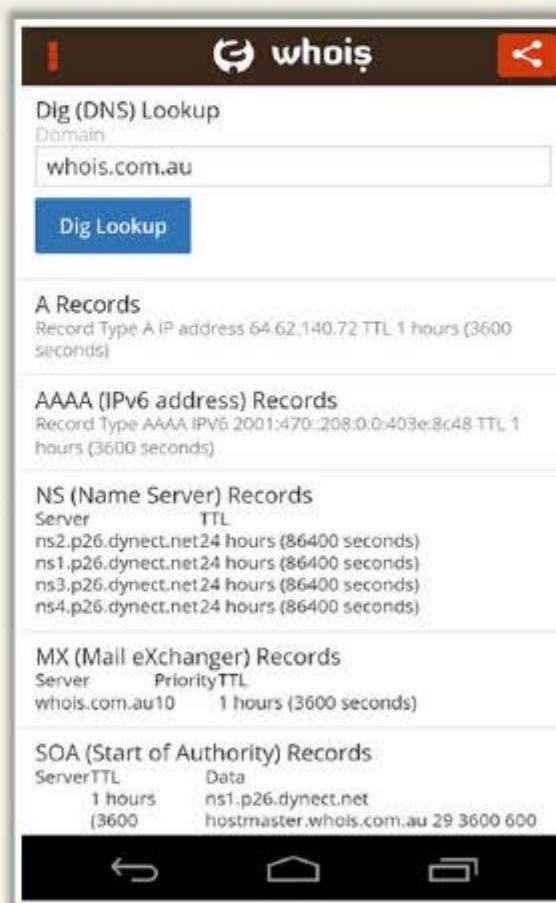
<https://www.dnssniffer.com>

UltraTools Mobile



<https://www.ultratools.com>

Whois® Lookup Tool



<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.ne1.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

Searching for microsoft.com ANY Record at c.root-servers.net [192.33.4.12] referred to f.gtld-servers.net
Searching for microsoft.com ANY Record at f.gtld-servers.net [192.35.51.30] referred to ns1.msft.net
Searching 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: msntst.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/wi9xgDi8KVrllZus5v8L6tbiQZkGrQ/rVQKJ

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

DNS Interrogation Tools

**DIG**<http://www.kloth.net>**DNSWatch**<http://www.dnswatch.info>**myDNSTools**<http://www.mydnstools.info>**DomainTools**<http://www.domaintools.com>**Professional Toolset**<http://www.dnsstuff.com>**DNS Query Utility**<http://www.dnsqueries.com>**DNS Records**<http://network-tools.com>**DNS Lookup**<https://www.ultratools.com>**DNSData View**<http://www.nirsoft.net>**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

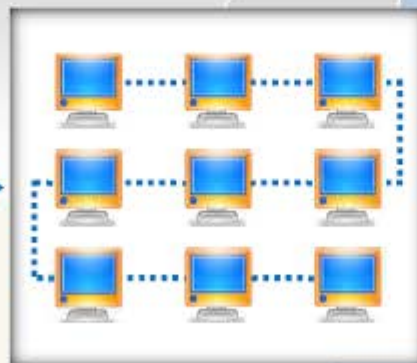
Network	
NetRange	207.46.0.0 - 207.46.255.255
CIDR	207.46.0.0/16
Name	MICROSOFT-GLOBAL-NET
Handle	NET-207-46-0-0-1
Parent	NET207 (NET-207-0-0-0-0)
Net Type	Direct Assignment
Origin AS	
Organization	Microsoft Corporation (MSFT)
Registration Date	1997-03-31
Last Updated	2013-08-20
Comments	
RESTful Link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

Queried
whois.arin.net with
"207.46.232.182"

Organization	
Name	Microsoft Corporation
Handle	MSFT
Street	One Microsoft Way
City	Redmond
State/Province	WA
Postal Code	98052
Country	US
Registration Date	1999-07-10
Last Updated	2013-08-21
Comments	<p>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</p> <p>For SPAM and other abuse issues, such as Microsoft Accounts, please contact: * abuse@microsoft.com</p> <p>To report security vulnerabilities in Microsoft products and services, please contact: * secure@microsoft.com</p> <p>For legal and law enforcement-related requests, please contact: * msnldo@microsoft.com</p> <p>For routing, peering or DNS issues, please contact:</p>



Attacker

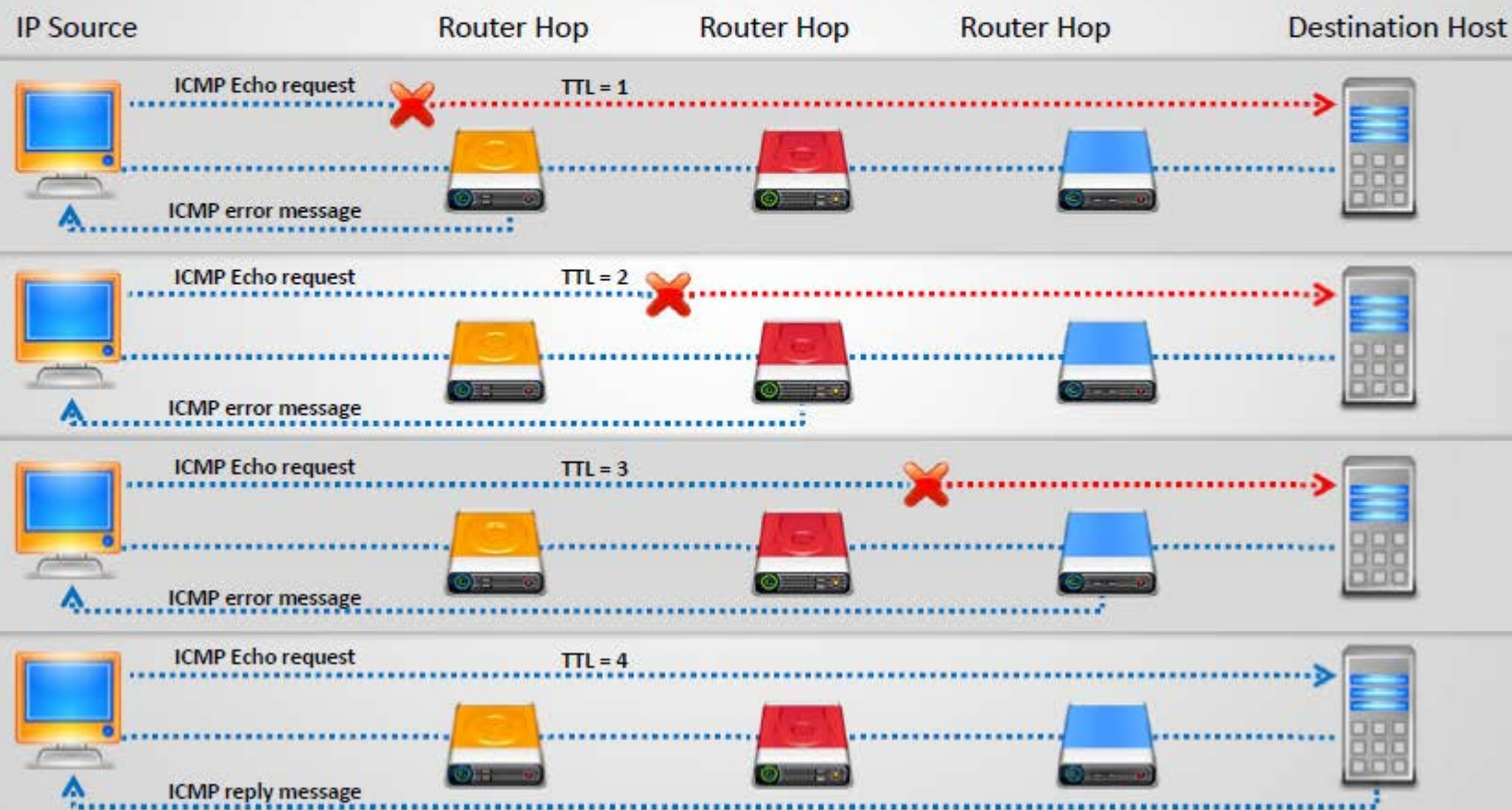


Network

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

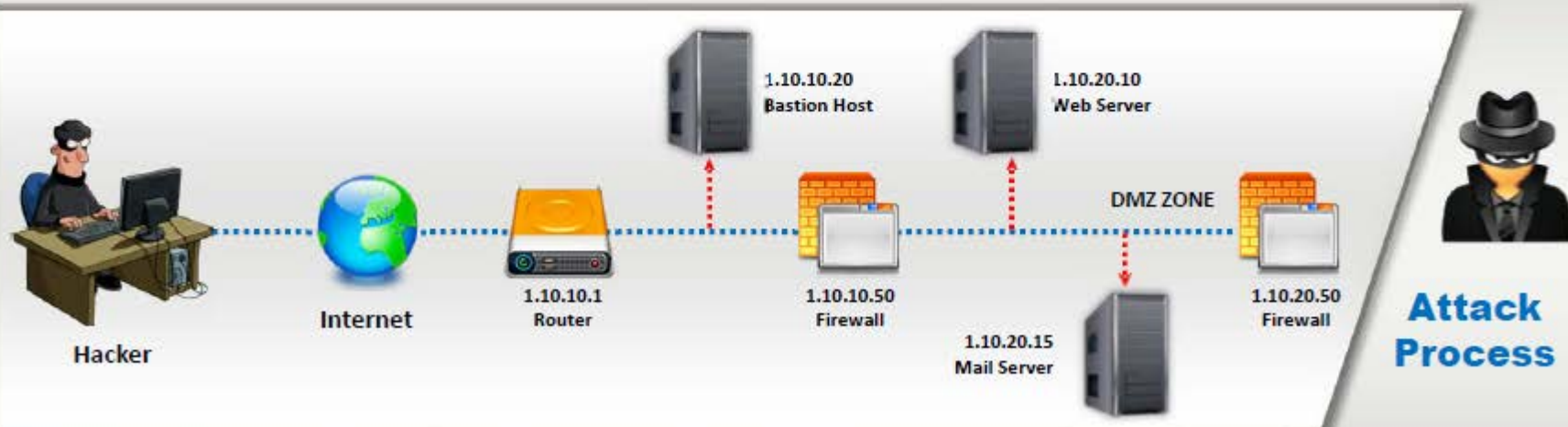


Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Traceroute Analysis



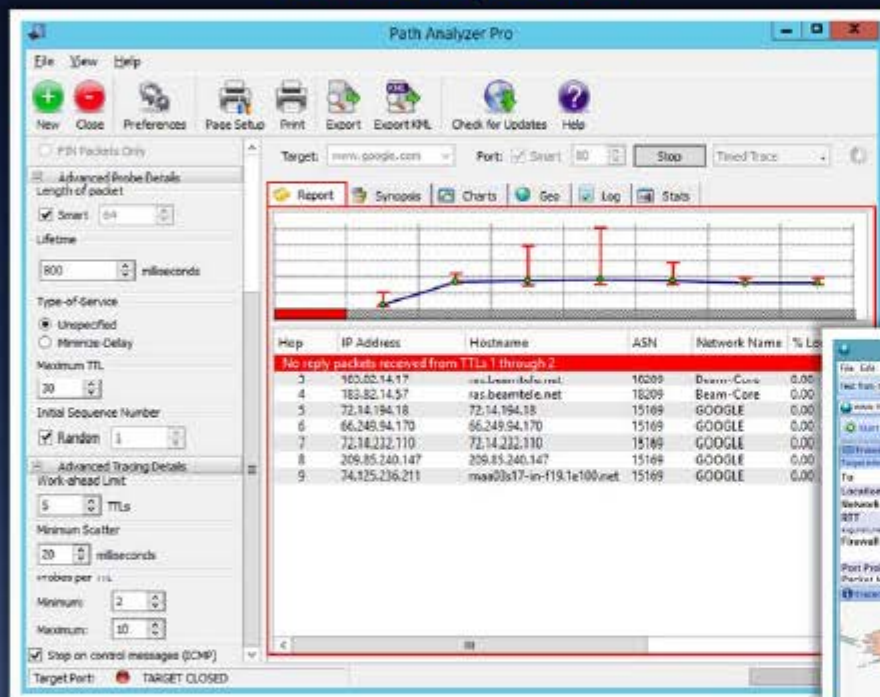
- Attackers conduct traceroute to extract information about: **network topology**, **trusted routers**, and **firewall locations**
- For example: after running several **traceroutes**, an attacker might obtain the following information:
 - traceroute 1.10.10.20, second to last hop is 1.10.10.1
 - traceroute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



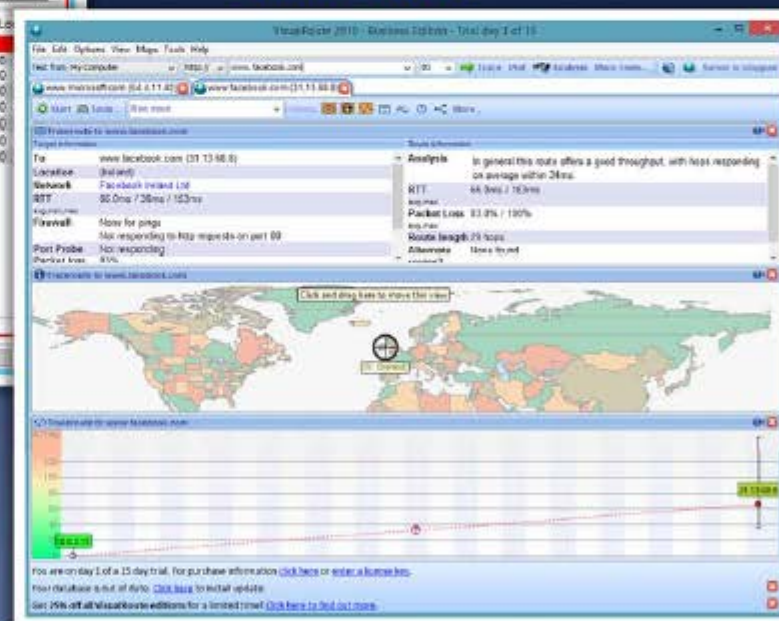
Path Analyzer Pro



<http://www.pathanalyzer.com>



VisualRoute



<http://www.visualroute.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Traceroute Tools

(Cont'd)



Network Pinger

<http://www.networkpinger.com>



Magic NetTrace

<http://www.tialsoft.com>



GEOSpider

<http://www.oreware.com>



3D Traceroute

<http://www.d3tr.de>



vTrace

<http://vtrace.pl>



AnalogX HyperTrace

<http://www.analogx.com>



Trout

<http://www.mcafee.com>



Network Systems Traceroute

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



Roadkil's Trace Route

<http://www.roadkil.net>



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

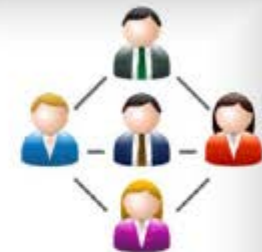
10

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 observe the target** to gain critical information
- Attackers gather information such as **passwords, personal identification number**, account numbers, credit card information, etc.



Dumpster Diving

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



Module Flow



1

**Footprinting
Concepts**

2

**Footprinting
Methodology**

3

**Footprinting
Tools**

4

**Footprinting
Countermeasures**

5

**Footprinting
Penetration
Testing**

Footprinting Tool: Maltego

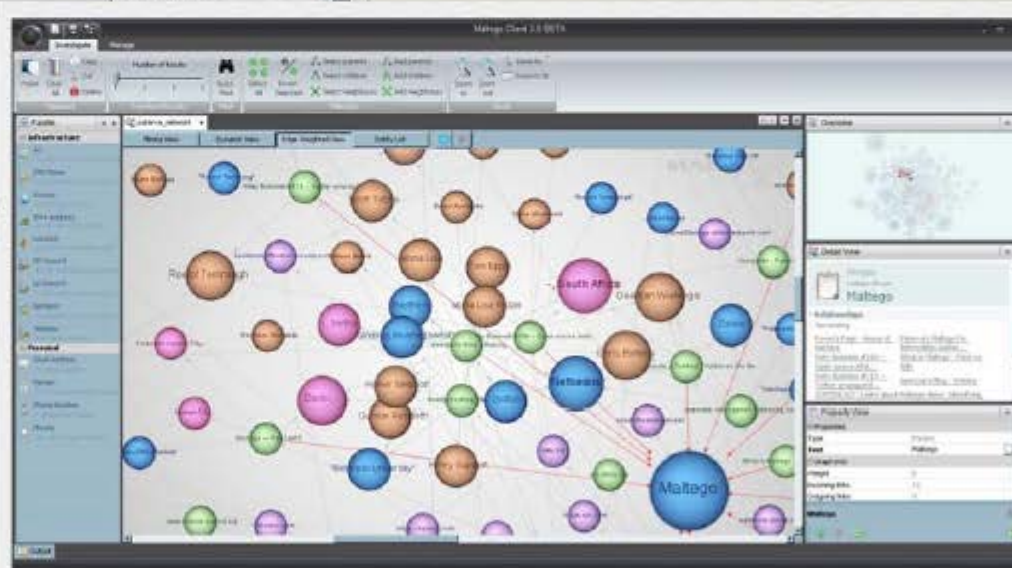


Internet Domain

<http://www.paterva.com>



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



Personal Information

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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

```

root@kali:~# recon-ng
[recon-ng v4.5.1, Tan Tanee (KaliMad4B3)]

Recon modules
Reporting modules
Query modules
Exploitation modules
Discovery modules

[recon-ng][default] >
  
```

```

root@kali:~# recon-ng
ECCOUNCIL.ORG

URL: http://searchdns.netcraft.com/?restriction=site%28ends%28with%28eccouncil.org
store.eccouncil.org
ciso.eccouncil.org
aspen.eccouncil.org
academia.eccouncil.org
www.eccouncil.org
portal.eccouncil.org
vesta.eccouncil.org
ilabs.eccouncil.org
foundation.eccouncil.org
iclass.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 | portal.eccouncil.org |  |  |  |  |  | netcraft
7 | vesta.eccouncil.org |  |  |  |  |  | netcraft
8 | ilabs.eccouncil.org |  |  |  |  |  | netcraft
9 | foundation.eccouncil.org |  |  |  |  |  | netcraft
10 | iclass.eccouncil.org |  |  |  |  |  | netcraft
11 | cert.eccouncil.org |  |  |  |  |  | netcraft
12 | frank.eccouncil.org |  |  |  |  |  | netcraft

12 rows returned
[recon-ng][eccouncil.org][netcraft] >
  
```

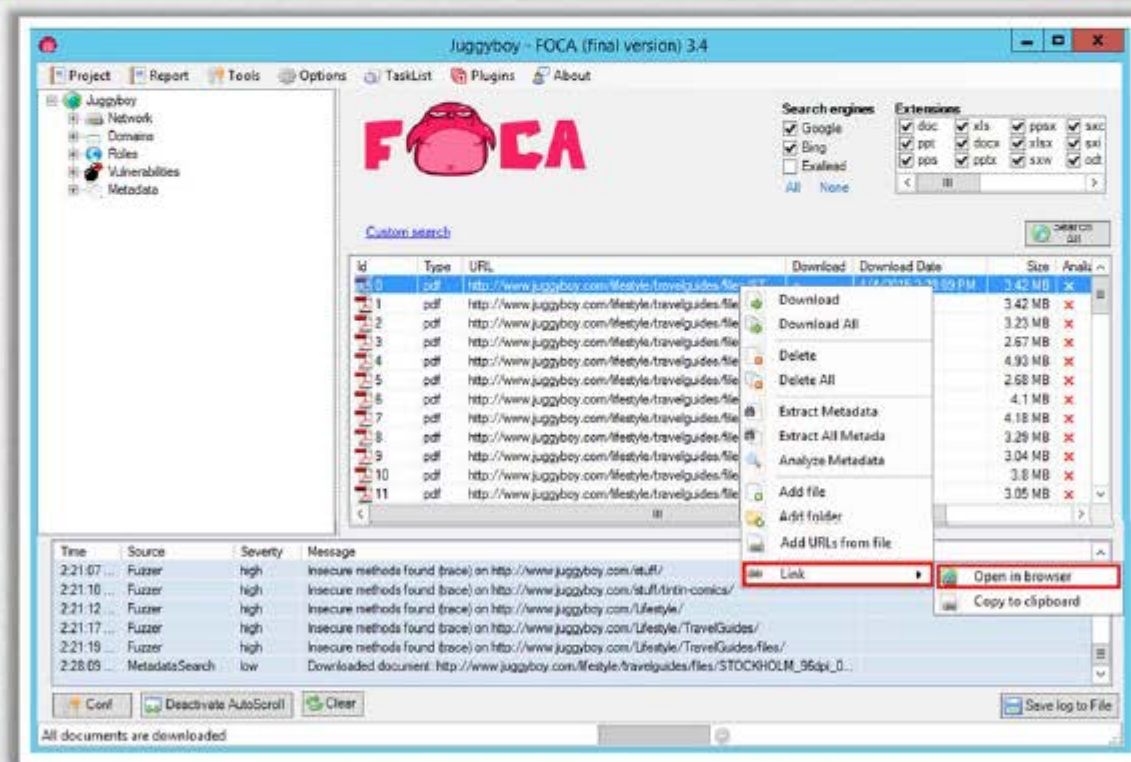
<https://bitbucket.org>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

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>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Additional Footprinting Tools



Prefix Whois

<http://pwhois.org>



Netmask

<http://www.phenoelit.org>



NetScanTools Pro

<http://www.netscantools.com>



Binging

<http://www.blueinfy.com>



Tctrace

<http://www.phenoelit.org>



SearchBug

<http://www.searchbug.com>



Autonomous System Scanner (ASS)

<http://www.phenoelit.org>



TinEye

<http://www.tineye.com>



DNS-Digger

<http://www.dnsdigger.com>



Robtex

<http://www.robtex.com>

Additional Footprinting Tools

(Cont'd)



Dig Web Interface

<http://www.digwebinterface.com>



SpiderFoot

<http://www.spiderfoot.net>



White Pages

<http://www.whitepages.com>



NSlookup

<http://www.kloth.net>



Email Tracking Tool

<http://www.filley.com>



Zaba Search

<http://www.zabasearch.com>



yoName

<http://yiname.com>



GeoTrace

<http://www.nabber.org>



Ping-Probe

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



DomainHostingView

<http://www.nirsoft.net>

Additional Footprinting Tools

(Cont'd)

**MetaGoofil**<http://www.edge-security.com>**GMapCatcher**<http://code.google.com>**Wikto**<http://research.sensepost.com>**SearchDiggity**<http://www.bishopfox.com>**SiteDigger**<http://www.mcafee.com>**Google HACK DB**<http://www.secpoint.com>**Google Hacks**<http://code.google.com>**Gooscan**<http://www.darknet.org.uk>**BiLE Suite**<http://www.sensepost.com>**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



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**



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



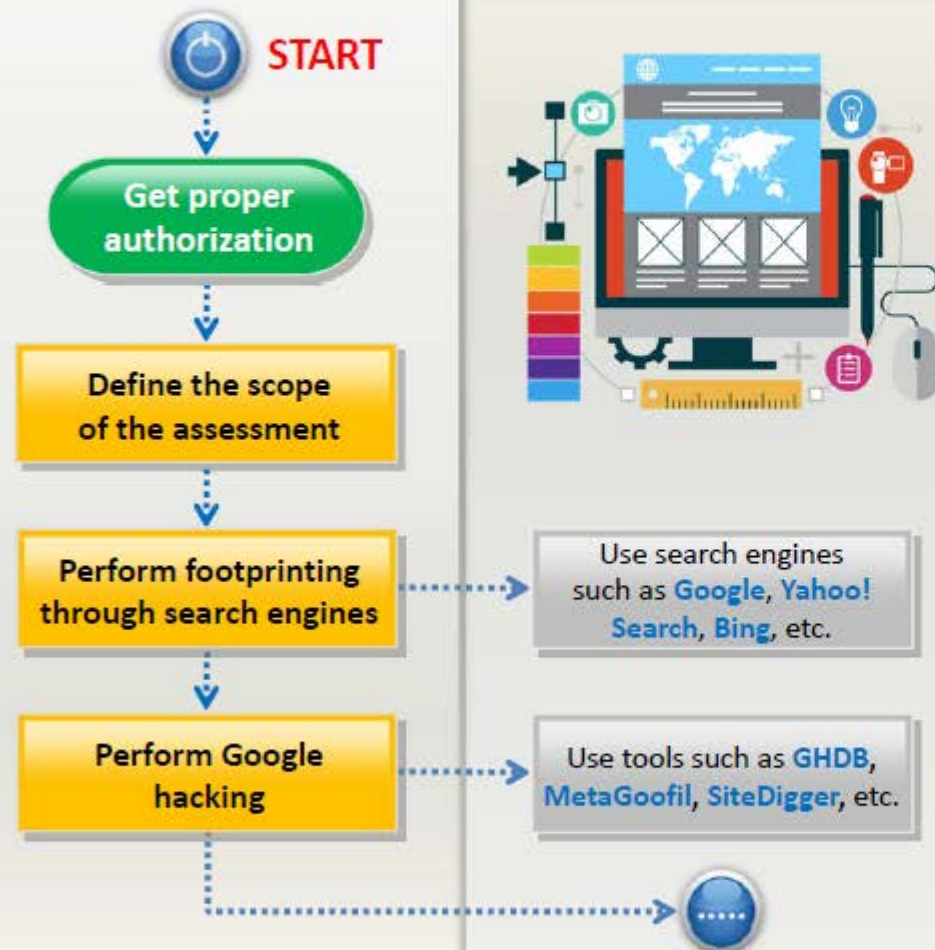
Prevent **information leakage**



Prevent **social engineering attempts**

Footprinting Pen Testing

(Cont'd)

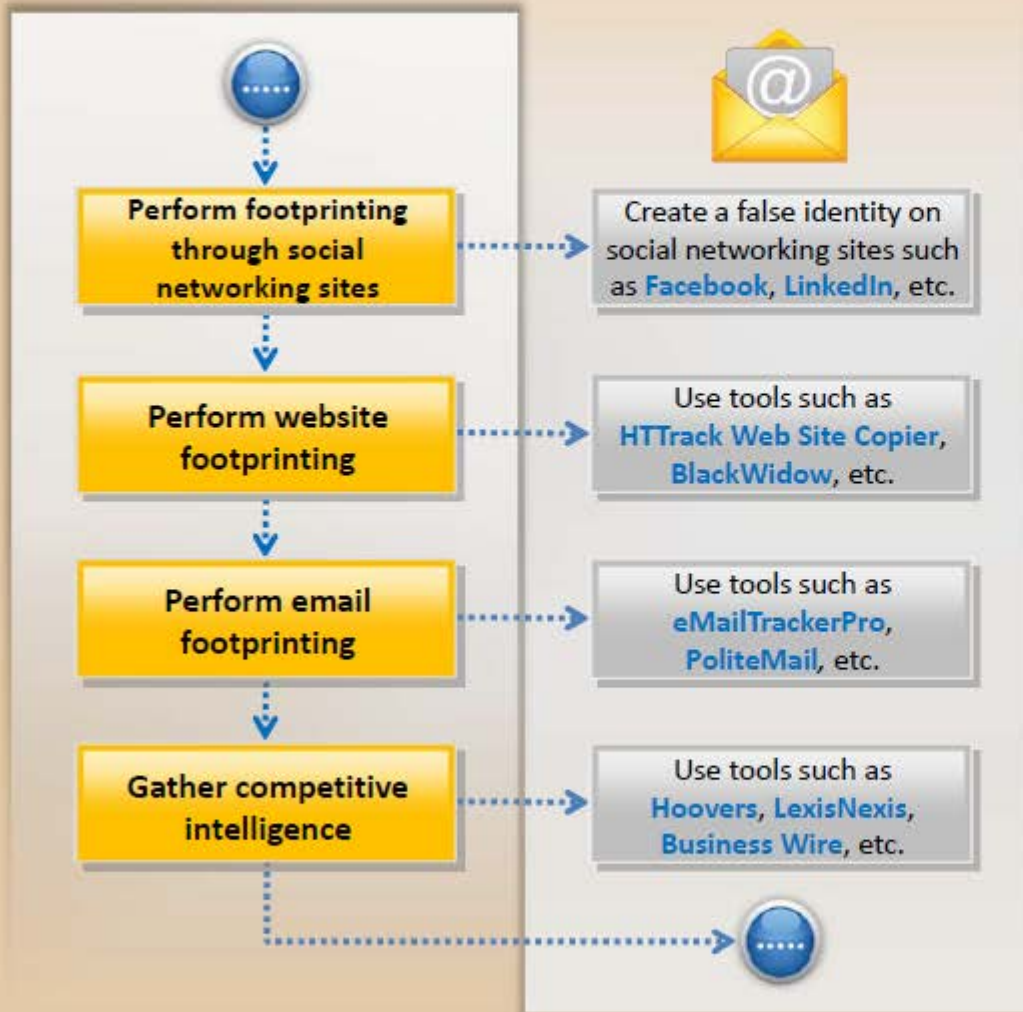


- Get proper authorization and define the scope of the assessment
- Footprint search engines such as **Google, Yahoo! Search, Ask, Bing, Dogpile**, etc. to gather target organization's information such as employee details, login pages, intranet portals, etc. that helps in performing social engineering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



Footprinting Pen Testing

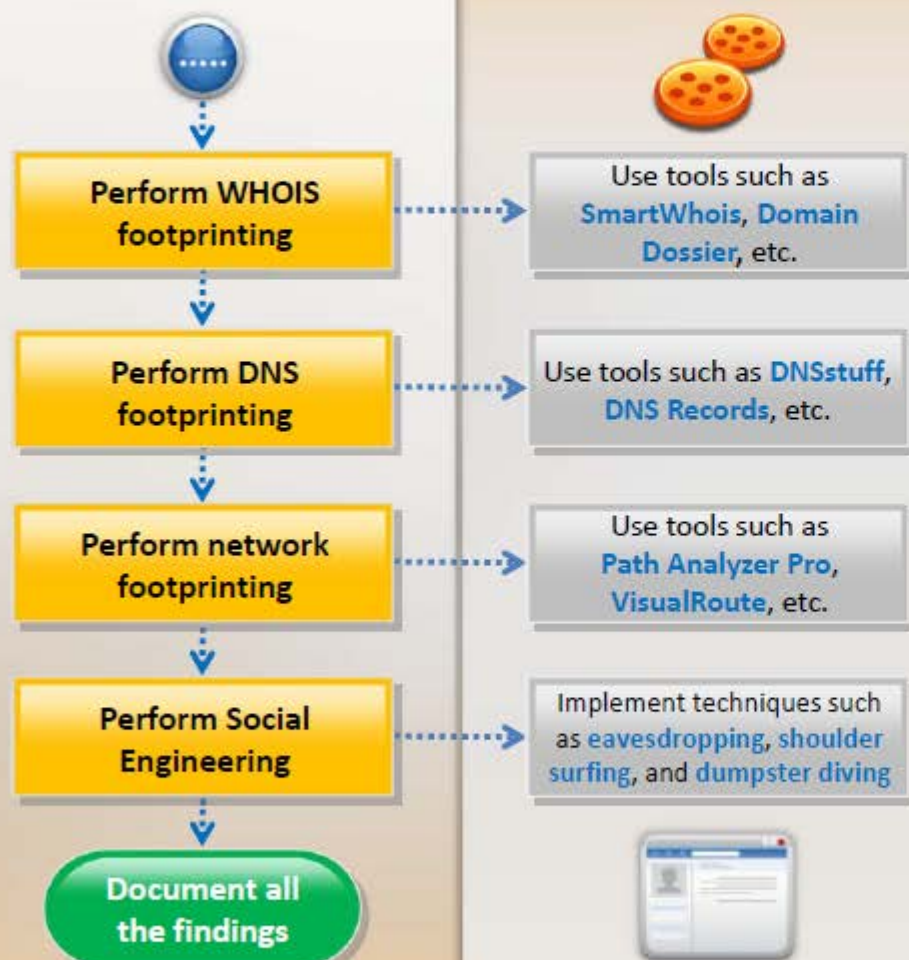
(Cont'd)



- 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**, **Webripper**, 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:

 Project plans:

 Others:


Information obtained through WHOIS footprinting


 Domain name details:

 Contact details of domain owner:


 Domain name servers:


 Netrange:


 When a domain has been created:

 Others:

Information obtained through DNS footprinting

 Location of DNS servers:


 Type of servers:

 Others:


Information obtained through network footprinting

 Range of IP addresses:

 Subnet mask used by the target organization:

 OS's in use:

 Firewall locations:

 Others:


Information obtained through social engineering


 Personal information:


 Financial information:

 Operating environment:

 User names and passwords:

 Network layout information:

 IP addresses and names of servers:

 Others:



Module Summary



- ☐ Footprinting is the 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

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.