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**

C|EH Certified Ethical Hacker

1 Footprinting Concepts

2 Footprinting Methodology

3 Footprinting Tools

4 Footprinting Countermeasures

5 Footprinting Penetration Testing

What is Footprinting?

C|EH Certified Ethical Hacker

- 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

C|EH
Certified Ethical Hacker

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

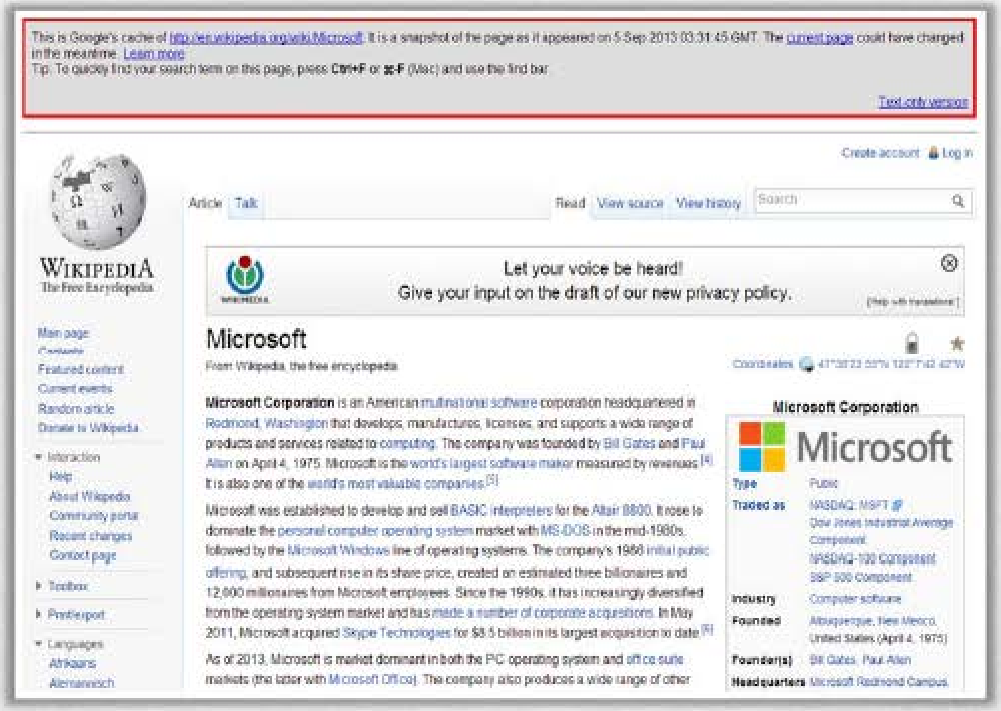
8 DNS Footprinting

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

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

Microsoft

From Wikipedia, the free encyclopedia

Coordinates: 47°38′23.55″N 122°7′42.42″W

Microsoft Corporation is an American multinational software corporation headquartered in Redmond, Washington that develops, manufactures, licenses, and supports a wide range of products and services related to computing. The company was founded by Bill Gates and Paul Allen on April 4, 1975. Microsoft is the world's largest software maker measured by revenues.[4] It is also one of the world's most valuable companies.[5]

Microsoft was established to develop and sell BASIC interpreters for the Altair 8800. It rose to dominate the personal computer operating system market with MS-DOS in the mid-1980s, followed by the Microsoft Windows line of operating systems. The company's 1986 initial public offering, and subsequent rise in its share price, created an estimated three billionaires and 12,000 millionaires from Microsoft employees. Since the 1990s, it has increasingly diversified from the operating system market and has made a number of corporate acquisitions. In May 2011, Microsoft acquired Skype Technologies for $8.5 billion in its largest acquisition to date.[6]

As of 2013, Microsoft is market dominant in both the PC operating system and office suite markets (the latter with Microsoft Office). The company also produces a wide range of other

Microsoft Corporation

Microsoft

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)
Founder(s)	Bill Gates, Paul Allen
Headquarters	Microsoft Redmond Campus

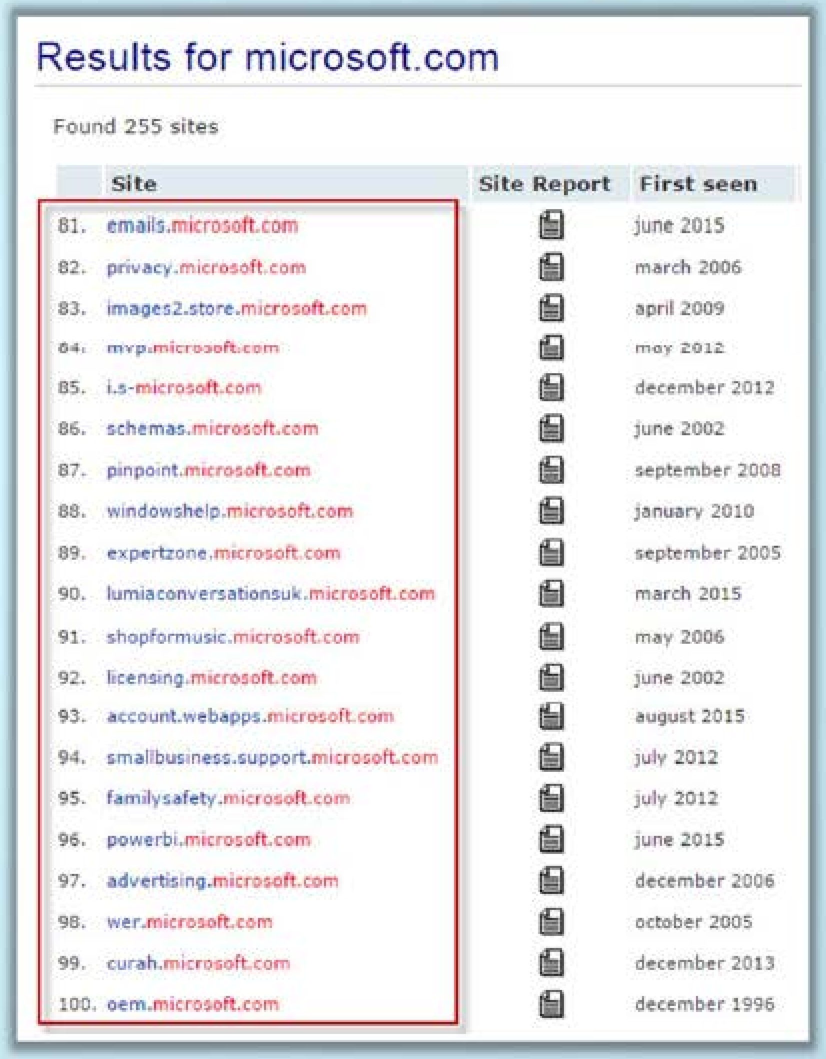
Finding Company's Public and Restricted Websites

CEH Certified Ethical Hacker

- 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`



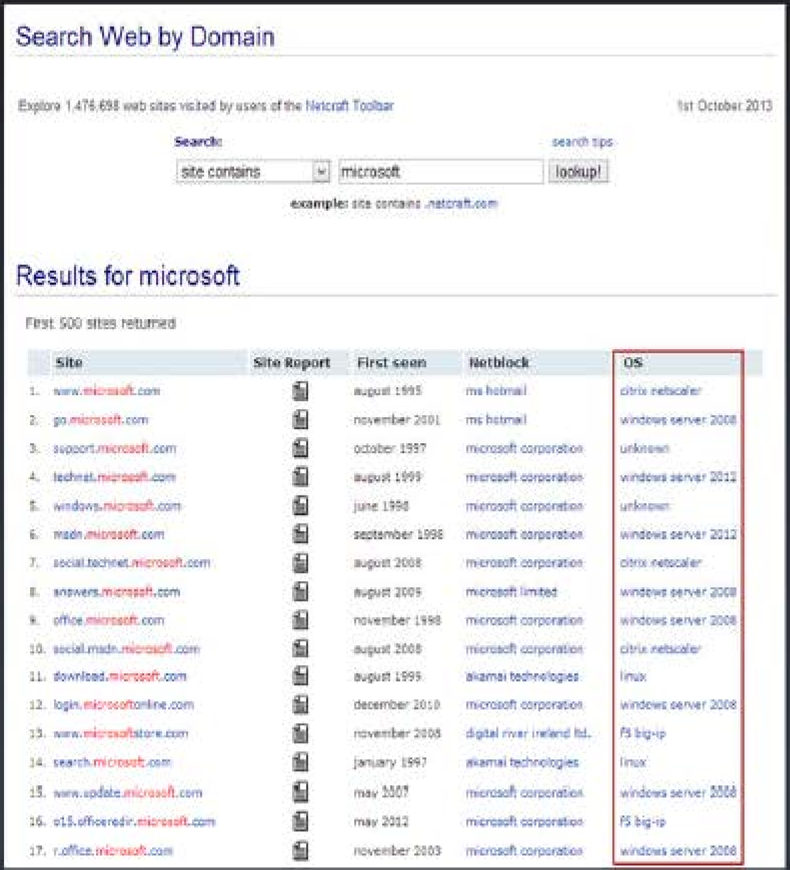
Results for microsoft.com

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.	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

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

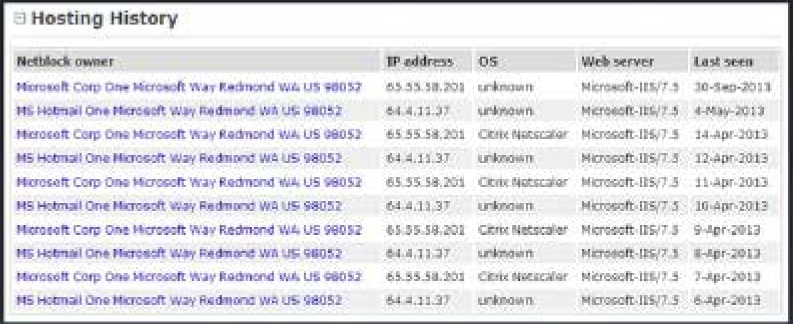
Search: site contains microsoft lookup! search tips

example: site contains .netcraft.com

Results for microsoft

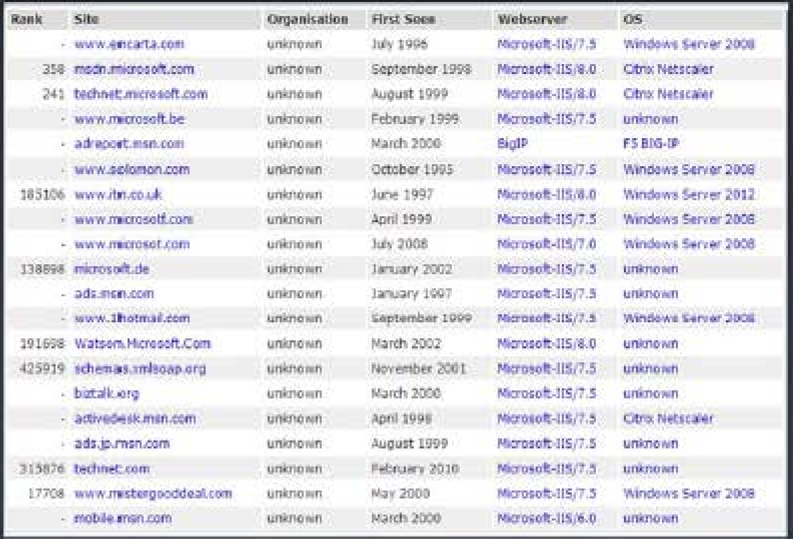
First 500 sites returned

	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.	msdn.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.msdn.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.	f5 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.officeredir.microsoft.com	🗎	may 2012	microsoft corporation	f5 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.encarta.com	unknown	July 1996	Microsoft-IIS/7.5	Windows Server 2008
358	msdn.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
-	adreport.msn.com	unknown	March 2000	BigIP	F5 BIG-IP
-	www.solomon.com	unknown	October 1995	Microsoft-IIS/7.5	Windows Server 2008
185106	www.itn.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.microsot.com	unknown	July 2008	Microsoft-IIS/7.0	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
-	biztalk.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.mistergooddeal.com	unknown	May 2000	Microsoft-IIS/7.5	Windows Server 2008
-	mobile.msn.com	unknown	March 2000	Microsoft-IIS/6.0	unknown

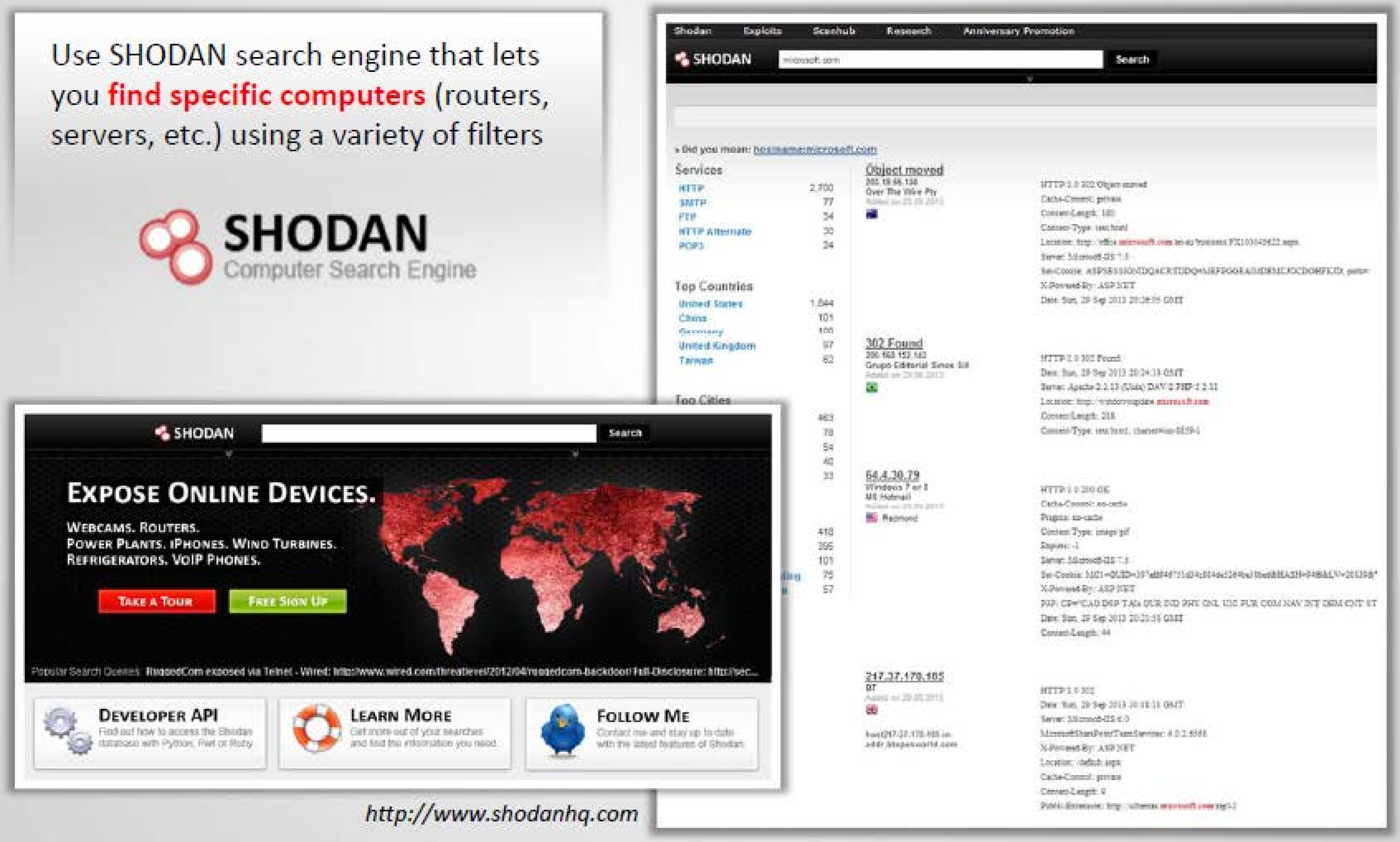
http://www.netcraft.com

Determining the Operating System (Cont'd)

Certified Ethical Hacker

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

SHODAN
Computer Search Engine



Shodan Exploits Scanhub Research Anniversary Promotion

SHODAN microsoft.com Search

» Did you mean: hostname:microsoft.com

Services

HTTP	2,700
SMTP	77
FTP	34
HTTP Alternate	30
POP3	24

Top Countries

United States	1,844
China	101
Germany	100
United Kingdom	97
Taiwan	62

Top Cities

[illegible]	463
[illegible]	78
[illegible]	54
[illegible]	40
[illegible]	33

[illegible]	418
[illegible]	395
[illegible]	101
[illegible]	75
[illegible]	57

Object moved
[illegible]
Over The Wire Pty
Added on 29.09.2013

```
HTTP/1.0 302 Object moved
Cache-Control: private
Content-Length: 180
Content-Type: text/html
Location: http://office.microsoft.com/en-au/business/FX[illegible].aspx
Server: Microsoft-IIS/7.5
Set-Cookie: ASPSESSIONID[illegible]; path=
X-Powered-By: ASP.NET
Date: Sun, 29 Sep 2013 20:26:[illegible] GMT
```

302 Found
[illegible]
Grupo Editorial Sinos SA
Added on 29.09.2013

```
HTTP/1.0 302 Found
Date: Sun, 29 Sep 2013 20:24:18 GMT
Server: Apache/2.2.17 (Unix) DAV/2 PHP/5.2.[illegible]
Location: http://windowsupdate.microsoft.com
Content-Length: 218
Content-Type: text/html; charset=iso-8859-1
```

64.4.30.79
Windows 7 or 8
MS Hotmail
Added on 29.09.2013
Redmond

```
HTTP/1.0 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: image/gif
Expires: -1
Server: Microsoft-IIS/7.5
Set-Cookie: MC1=GUID=[illegible]
X-Powered-By: ASP.NET
P3P: CP="CAO DSP TAIa OUR IND PHY ONL UNI PUR COM NAV INT DEM CNT ST
Date: Sun, 29 Sep 2013 20:23:[illegible] GMT
Content-Length: 44
```

217.37.170.105
BT
Added on 29.09.2013

host217-37-170-105.in-addr.btopenworld.com

```
HTTP/1.0 302
Date: Sun, 29 Sep 2013 20:18:[illegible] GMT
Server: Microsoft-IIS/6.0
MicrosoftSharePointTeamServices: 6.0.2.[illegible]
X-Powered-By: ASP.NET
Location: /default.aspx
Cache-Control: private
Content-Length: 0
Public-Extension: http://schemas.microsoft.com/repl-2
```

SHODAN Search

EXPOSE ONLINE DEVICES.

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

TAKE A TOUR FREE SIGN UP

Popular Search Queries: RuggedCom exposed via Telnet - Wired: http://www.wired.com/threatlevel/2012/04/ruggedcom-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

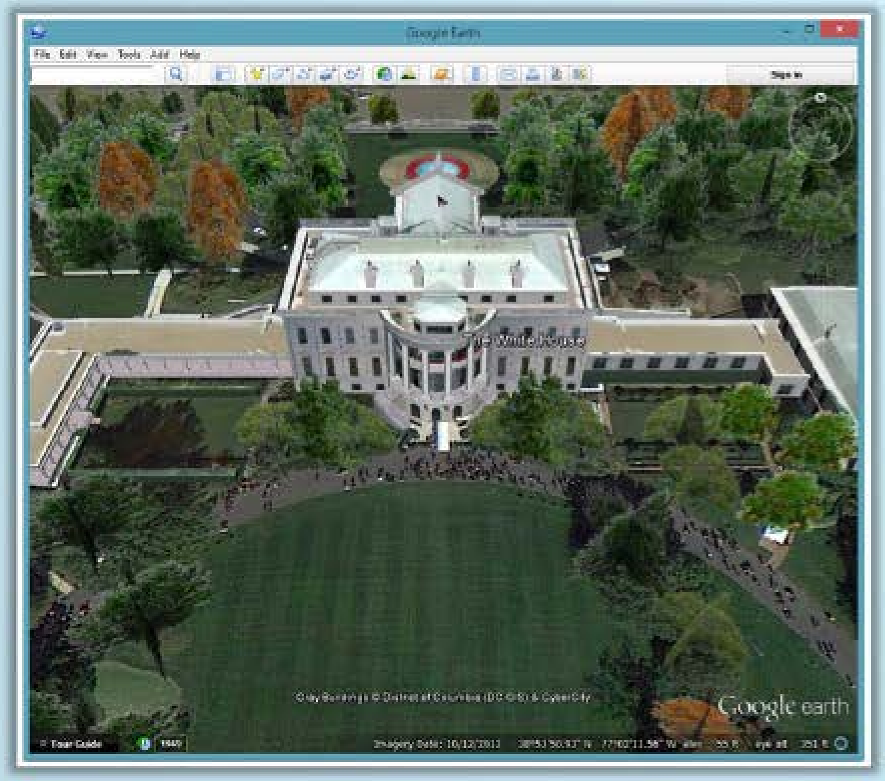
FOLLOW ME
Contact me and stay up to date with the latest features of Shodan

http://www.shodanhq.com

Collect Location Information

Google Earth

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



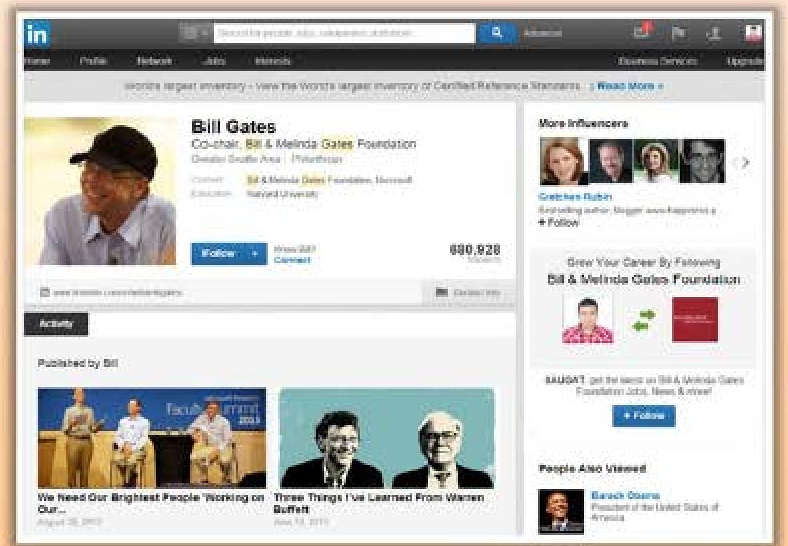
http://www.google.com

Tools for finding the geographical location

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

People Search: Social Networking Sites/People Search Services

- Social networking sites are the great source of personal and organizational information
- Information about an individual can be found at various **people search websites**
- The people search returns the following **information about a person or organization**:
  - Residential addresses and email addresses
  - Contact numbers and date of birth
  - Photos and social networking profiles
  - Blog URLs
  - Satellite pictures of private residencies
  - Upcoming projects and operating environment



Bill Gates
Co-chair, Bill & Melinda Gates Foundation

Current: Bill & Melinda Gates Foundation, Microsoft
Education: Harvard University

680,928

Grow Your Career By Following
Bill & Melinda Gates Foundation

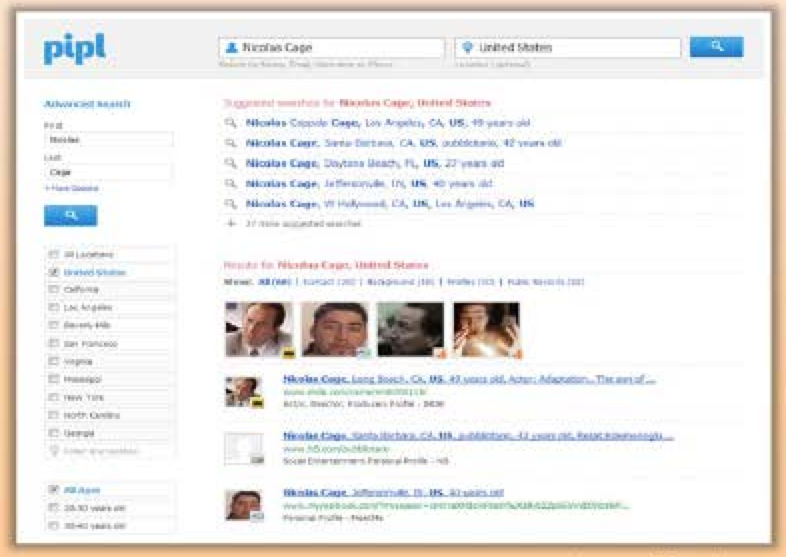
Published by Bill

We Need Our Brightest People Working on Our...

Three Things I've Learned From Warren Buffett

People Also Viewed
Barack Obama
President of the United States of America

http://www.linkedin.com



Nicolas Cage
United States

Suggested searches for Nicolas Cage, United States

Nicolas Coppola Cage, Los Angeles, CA, US, 49 years old
Nicolas Cage, Santa Barbara, CA, US, 42 years old
Nicolas Cage, Daytona Beach, FL, US, 27 years old
Nicolas Cage, Jeffersonville, IN, US, 40 years old
Nicolas Cage, W Hollywood, CA, US, Los Angeles, CA, US

Results for Nicolas Cage, United States

Nicolas Cage, Long Beach, CA, US, 49 years old, Actor: Adaptation... The son of ...
Nicolas Cage, Santa Barbara, CA, US, 42 years old ...
Nicolas Cage, Jeffersonville, IN, US, 40 years old

https://pipl.com

People Search Online Services

AnyWho
http://www.anywho.com

US Search
http://www.ussearch.com

Intelius
http://www.intelius.com

411
http://www.411.com

PeopleFinders
http://www.peoplefinders.com

PeopleSmart
http://www.peoplesmart.com

Veromi
http://www.veromi.net

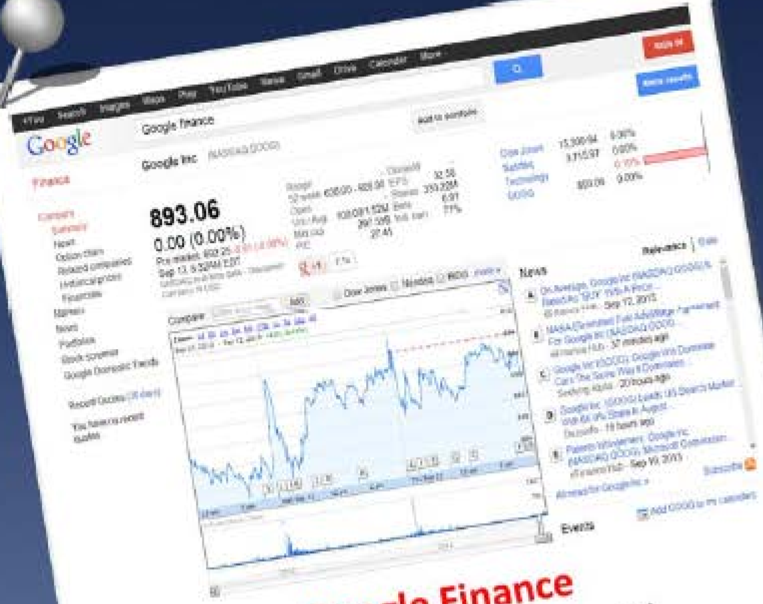
PrivateEye
http://www.privateeye.com

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

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

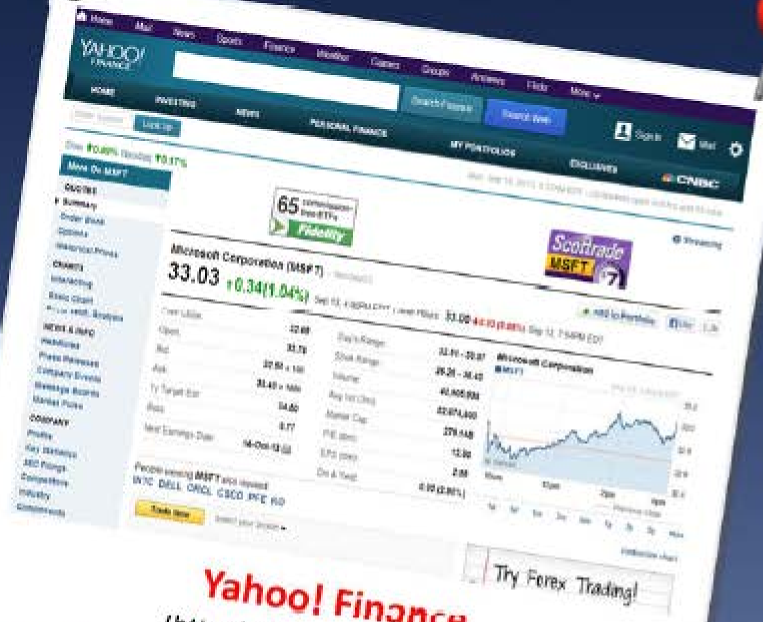
Gather Information from Financial Services

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



Google Finance

(https://www.google.com/finance)



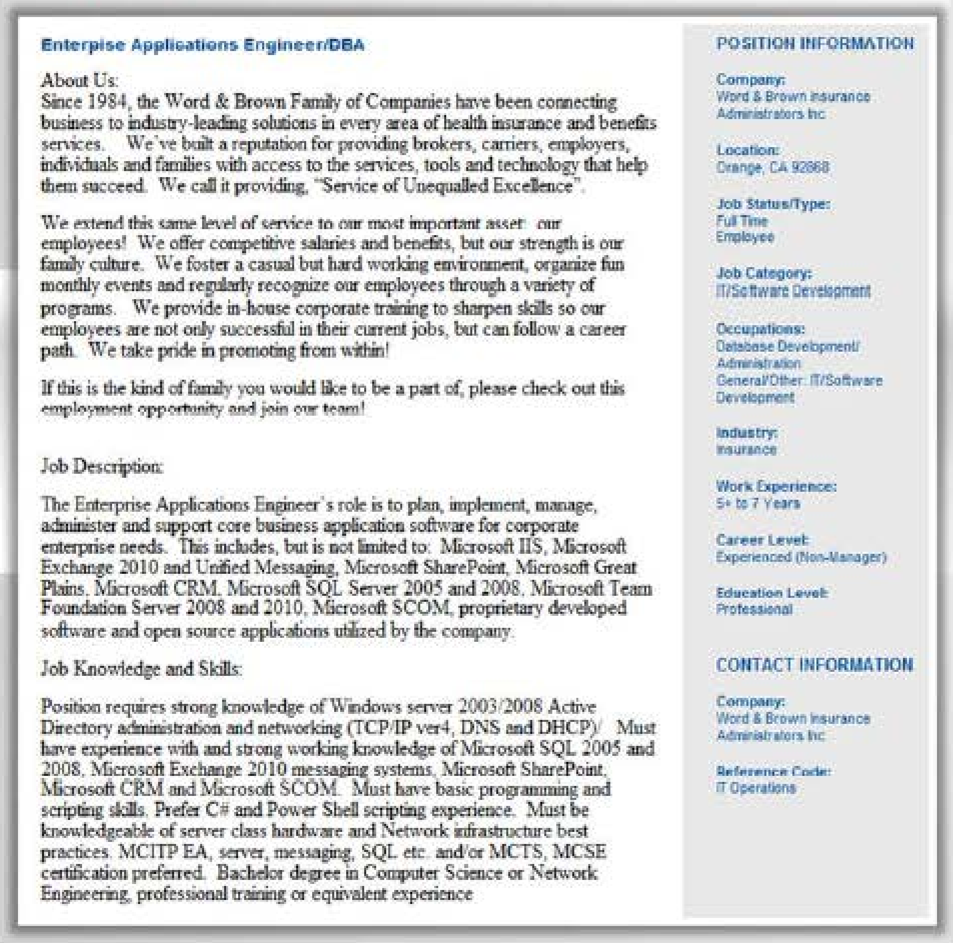
Yahoo! Finance

(http://finance.yahoo.com)

Footprinting through Job Sites

C|EH Certified Ethical Hacker

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

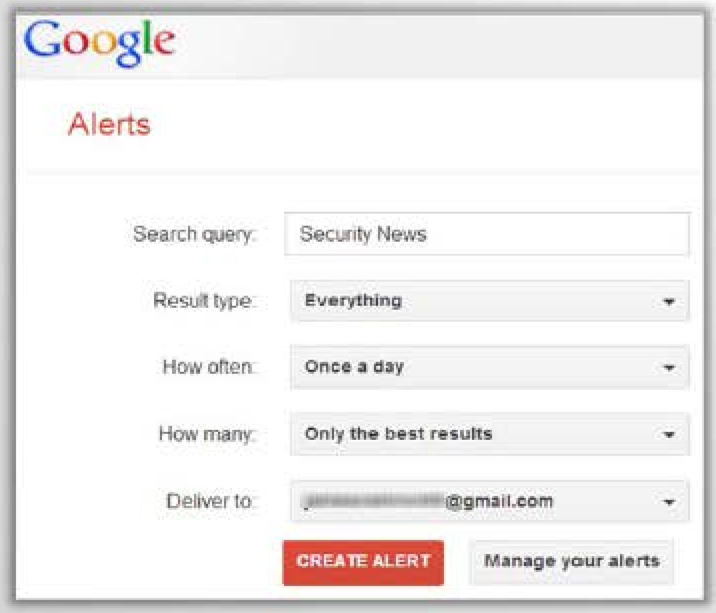
- http://www.linkedin.com
- http://www.monster.com
- http://www.careerbuilder.com
- http://www.dice.com
- http://www.simplyhired.com
- http://www.indeed.com
- http://www.usajobs.gov

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



Google

Alerts

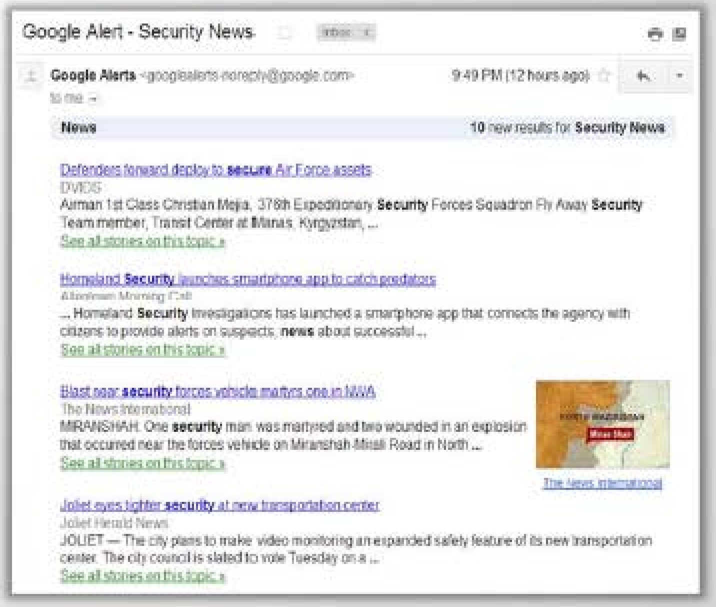
Search query: Security News

Result type: Everything

How often: Once a day

How many: Only the best results

Deliver to: [redacted]@gmail.com



Google Alert - Security News

Google Alerts <googlealerts-noreply@google.com> 9:49 PM (12 hours ago)

to me

News — 10 new results for **Security News**

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 Manas, Kyrgyzstan, ...
See all stories on this topic »

Homeland **Security** launches smartphone app to catch predators
Allentown Morning Call
... 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 martyrs 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 »
The News International

Joliet eyes tighter **security** at new transportation center
Joliet Herald News
JOLIET — The city plans to make video monitoring an expanded safety feature of its new transportation center. The city council is slated to vote Tuesday on a ...
See all stories on this topic »

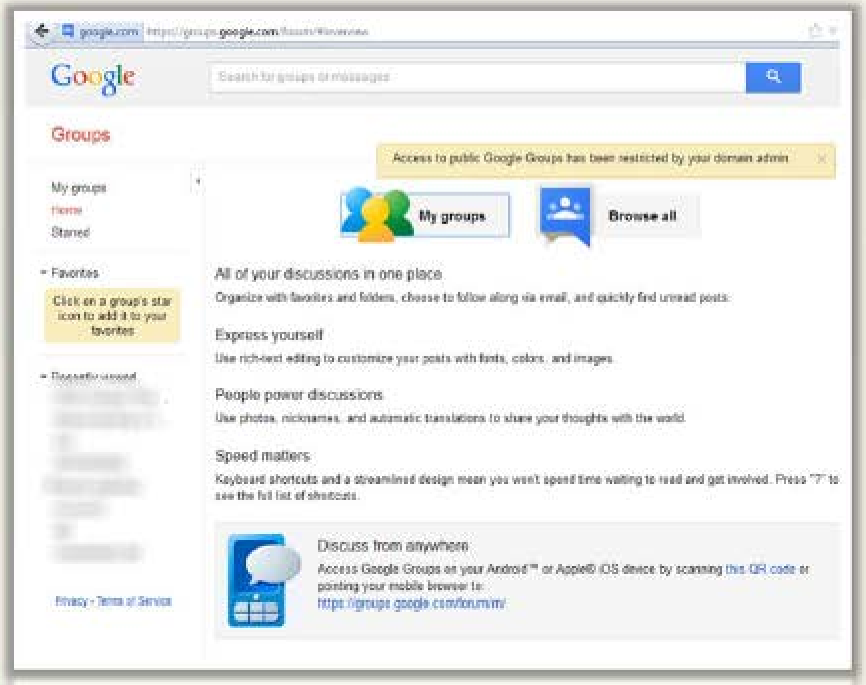
Information Gathering Using Groups, Forums, and Blogs

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

Google Groups



google.com https://groups.google.com/forum/#!overview
Google
Search for groups or messages
Groups
My groups
Home
Starred
Favorites
Recently viewed
My groups
Browse all
Privacy - Terms of Service

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

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

All of your discussions in one place

Organize with favorites and folders, choose to follow along via email, and quickly find unread posts.

Express yourself

Use rich-text editing to customize your posts with fonts, colors, and images.

People power discussions

Use photos, nicknames, and automatic translations to share your thoughts with the world.

Speed matters

Keyboard shortcuts and a streamlined design mean you won't spend time waiting to read and get involved. Press "?" to see the full list of shortcuts.

Discuss from anywhere

Access Google Groups on your Android™ or Apple® iOS device by scanning this QR code or pointing your mobile browser to: https://groups.google.com/forum/m/

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

C|EH Certified Ethical Hacker

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

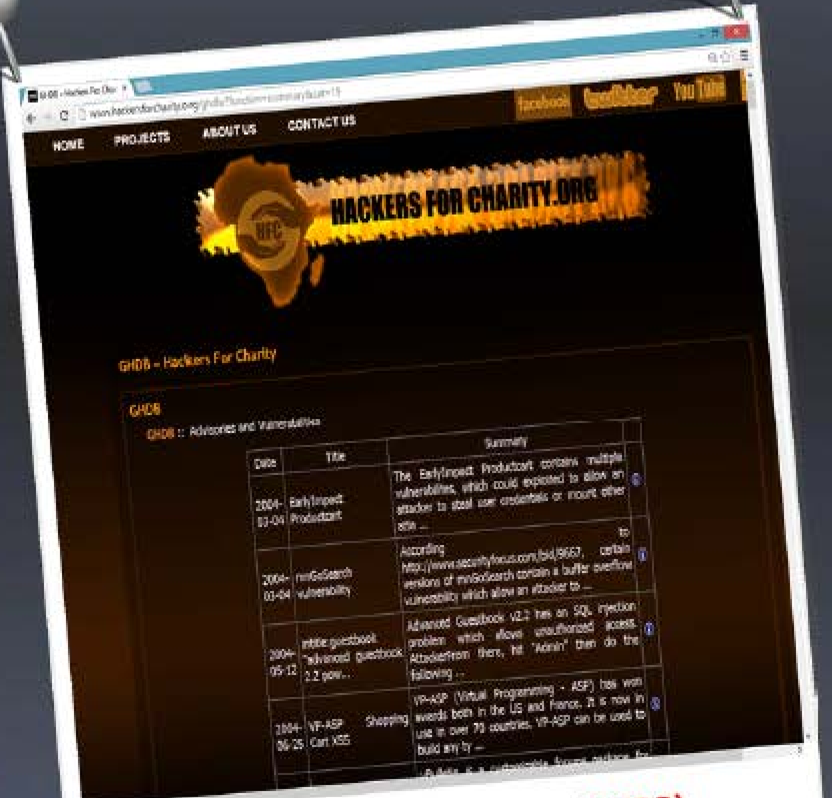
It uses advanced Google search operators to locate specific strings of text within the search results

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



GHDB – Hackers For Charity

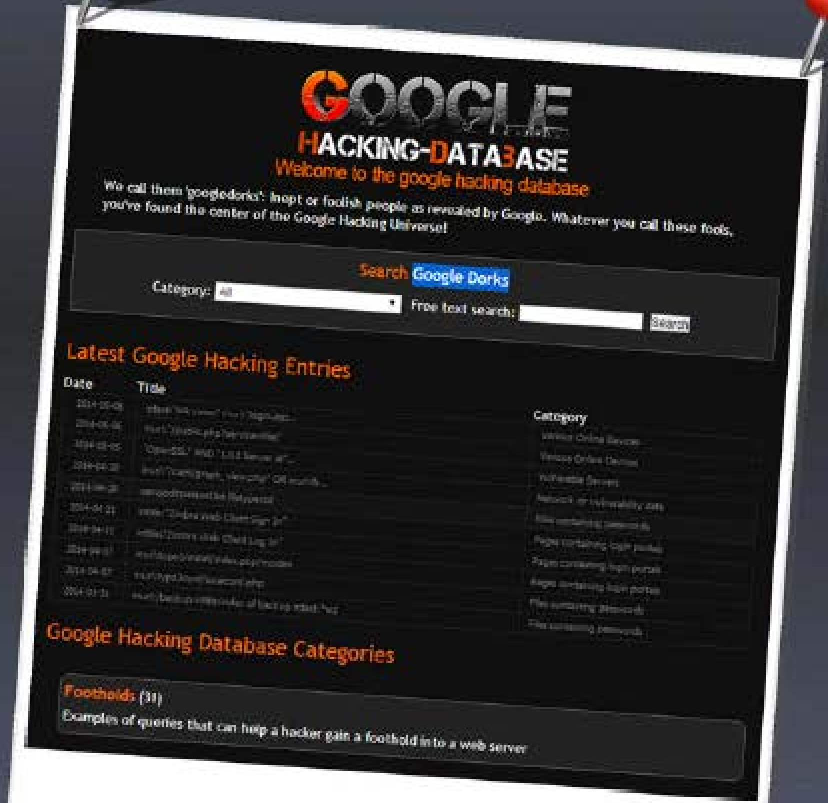
GHDB

GHDB :: Advisories and Vulnerabilities

Date	Title	Summary
2004-03-04	EarlyImpact Productcart	The EarlyImpact Productcart contains multiple vulnerabilites, which could exploited to allow an attacker to steal user credentials or mount other atta ...
2004-03-04	miniGoSearch vulnerability	According to http://www.securityfocus.com/bid/9667, certain versions of miniGoSearch contain a buffer overflow vulnerability which allow an attacker to ...
2004-05-12	intitle:guestbook "advanced guestbook 2.2 pow...	Advanced Guestbook v2.2 has an SQL injection problem which allows unauthorized access. AttackerFrom 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 ty ...

Google Hacking Database (GHDB)

http://www.hackersforcharity.org



Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Google Dorks

Category: All ▾ Free text search: Search

Latest Google Hacking Entries

Date	Title	Category
2014-05-08	[illegible]	Various Online Devices
2014-05-06	[illegible]	Various Online Devices
2014-05-05	"OpenSSL" AND "1.0.1 Server at" ...	Vulnerable Servers
2014-04-28	[illegible]	Network or vulnerability data
2014-04-28	[illegible]	Files containing passwords
2014-04-21	intitle:"Zimbra Web Client Sign In"	Pages containing login portals
2014-04-11	intitle:"Zimbra Web Client Log In"	Pages containing login portals
2014-04-07	[illegible]	Pages containing login portals
2014-04-07	[illegible]	Files containing passwords
2014-03-31	[illegible]	Files 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

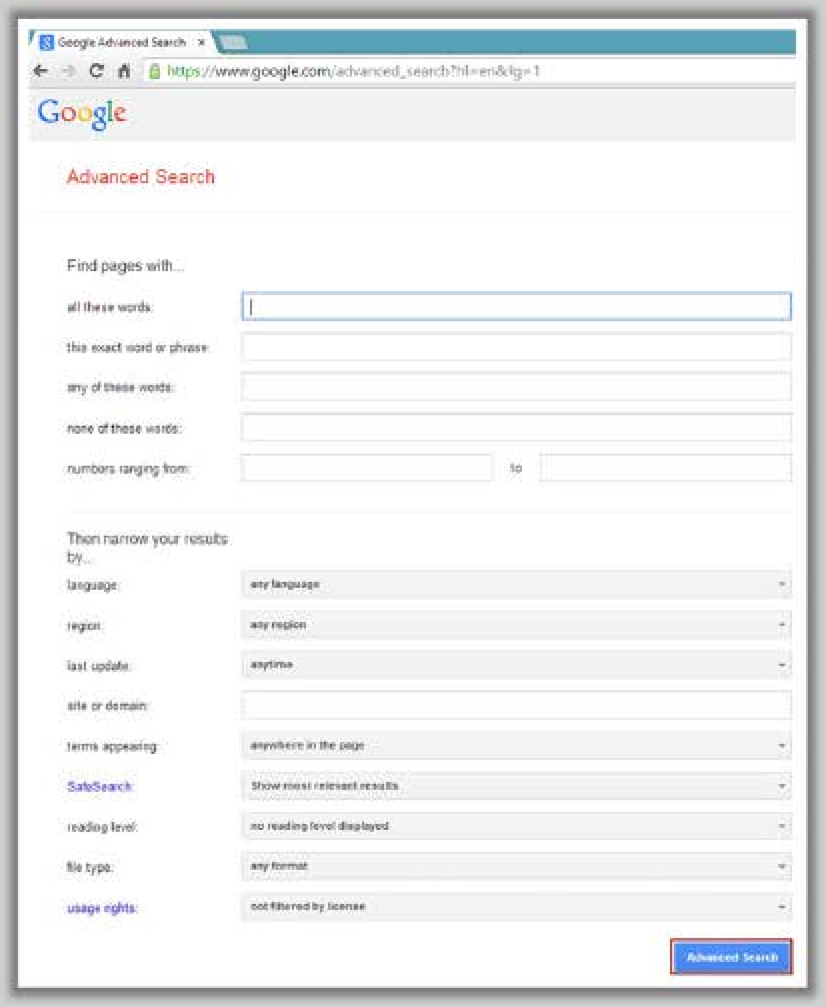
http://www.exploit-db.com

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



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: any language

region: any region

last update: anytime

site or domain:

terms appearing: anywhere in the page

SafeSearch: Show most relevant results

reading level: no reading level displayed

file type: any format

usage rights: not filtered by license

Footprinting Methodology

C|EH Certified Ethical Hacker

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

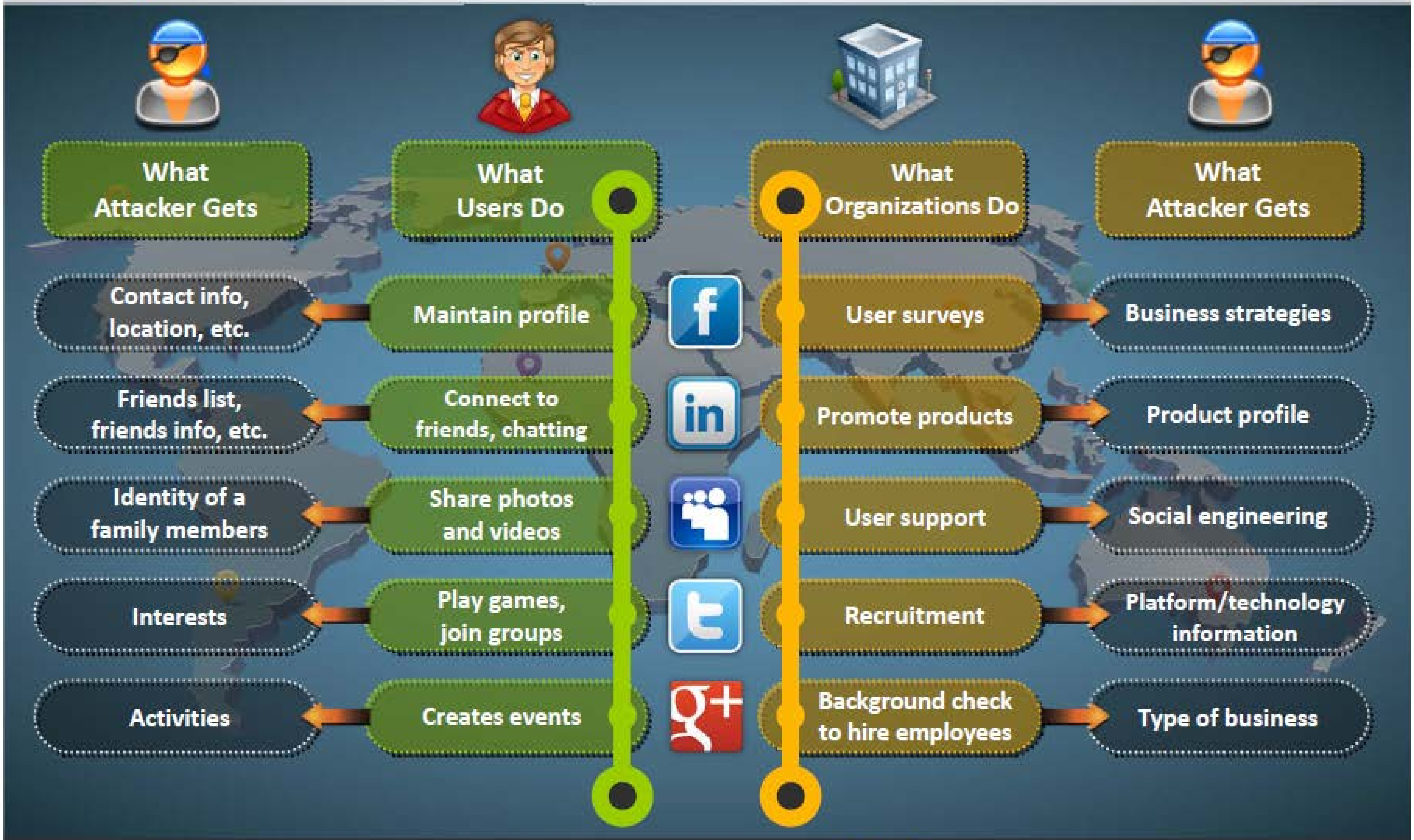
Attackers use social engineering trick to gather sensitive information from social networking websites such as **Facebook**, **MySpace**, **LinkedIn**, **Twitter**, **Pinterest**, **Google+**, etc.

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



What Attacker Gets	What Users Do	What Organizations Do	What Attacker Gets
Contact info, location, etc.	Maintain profile	User surveys	Business strategies
Friends list, friends info, etc.	Connect to friends, chatting	Promote products	Product profile
Identity of a family members	Share photos and videos	User support	Social engineering
Interests	Play games, join groups	Recruitment	Platform/technology information
Activities	Creates events	Background check to hire employees	Type of business

Footprinting Methodology

C|EH Certified Ethical Hacker

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

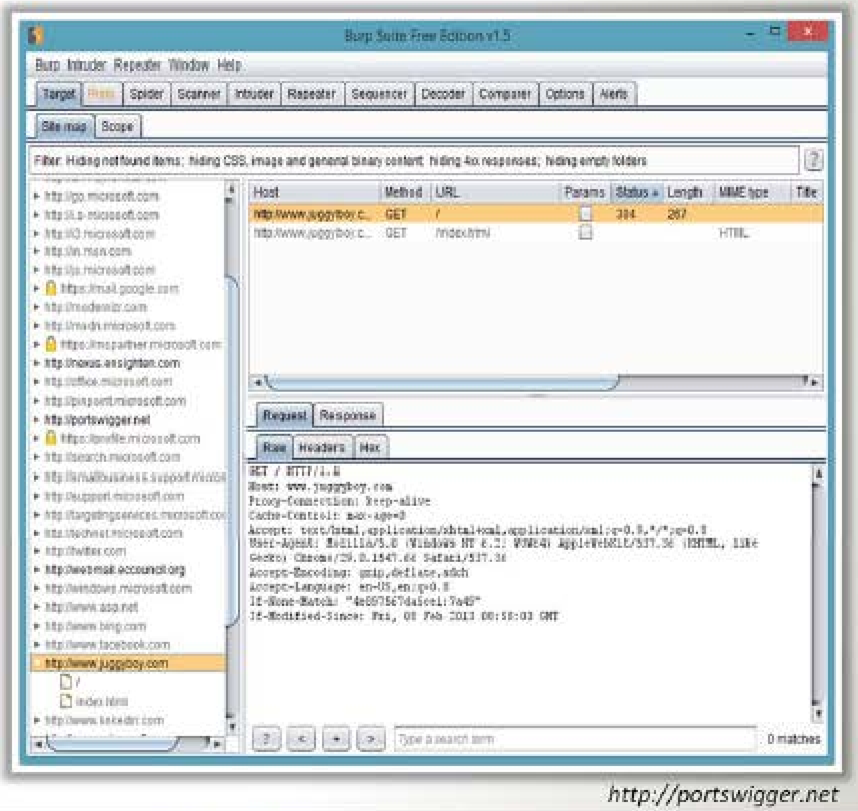
1 Website footprinting refers to **monitoring and analyzing the target organization's website** for information

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


Burp Suite Free Edition v1.5
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Options Alerts
Site map Scope
Request Response
Raw Headers Hex
? < + >
Type a search term
0 matches

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- http://go.microsoft.com
- http://i.s-microsoft.com
- http://i3.microsoft.com
- http://ie.msn.com
- http://js.microsoft.com
- https://mail.google.com
- http://modernizr.com
- http://msdn.microsoft.com
- https://mspartner.microsoft.com
- http://nexus.ensighten.com
- http://office.microsoft.com
- http://pinpoint.microsoft.com
- http://portswigger.net
- https://profile.microsoft.com
- http://search.microsoft.com
- http://smallbusiness.support.micros
- http://support.microsoft.com
- http://targetingservices.microsoft.co
- http://technet.microsoft.com
- http://twitter.com
- http://webmail.accountcl.org
- http://windows.microsoft.com
- http://www.asp.net
- http://www.bing.com
- http://www.facebook.com
- http://www.juggyboy.com
  - /
  - index.html
- http://www.linkedin.com

Host	Method	URL	Params	Status	Length	MIME type	Title
http://www.juggyboy.c...	GET	/	□	304	267		
http://www.juggyboy.c...	GET	/index.html	□			HTML	

```
GET / HTTP/1.1
Host: www.juggyboy.com
Proxy-Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/29.0.1547.66 Safari/537.36
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
If-None-Match: "4e0575c7da5ce1:7a45"
If-Modified-Since: Fri, 08 Feb 2013 08:58:03 GMT
```

http://portswigger.net

Website Footprinting (Cont'd)

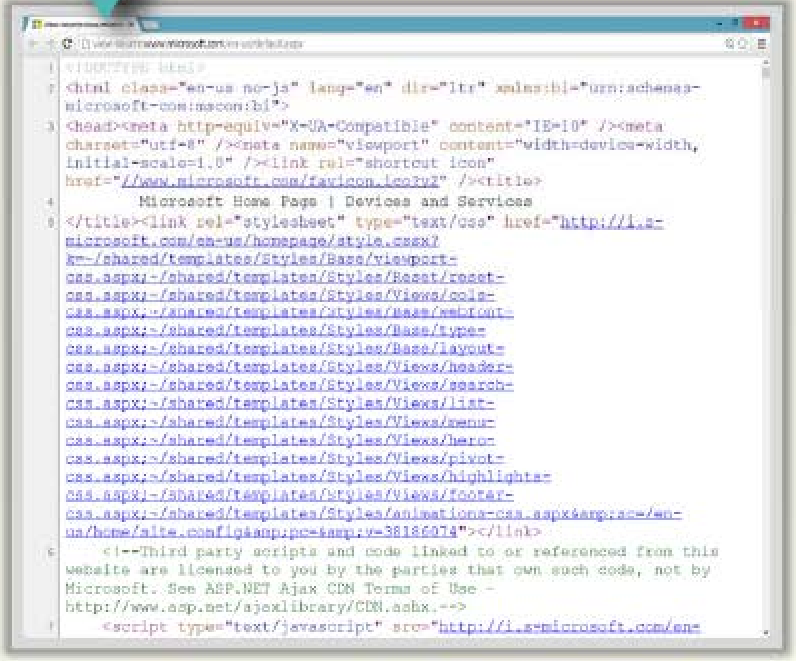
CEH Certified Ethical Hacker

Examining HTML source provide:

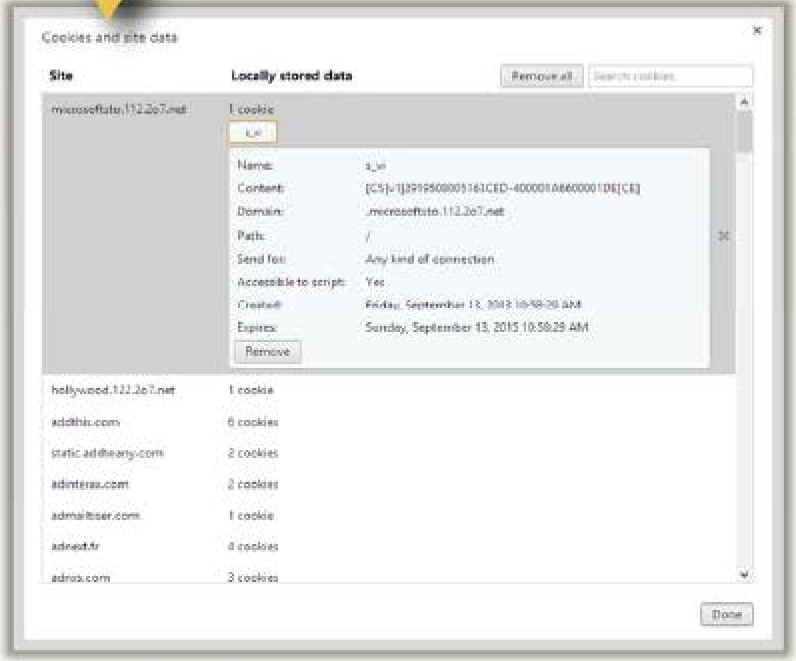
- Comments in the source code
- Contact details of web developer or admin
- File system structure
- Script type

Examining cookies may provide:

- Software in use and its behavior
- Scripting platforms used



```
<!DOCTYPE html>
<html class="en-us no-js" lang="en" dir="ltr" xmlns:bi="urn:schemas-
microsoft-com:mscom:bi">
<head><meta http-equiv="X-UA-Compatible" content="IE=10" /><meta
charset="utf-8" /><meta name="viewport" content="width=device-width,
initial-scale=1.0" /><link rel="shortcut icon"
href="//www.microsoft.com/favicon.ico?v2" /><title>
        Microsoft Home Page | Devices and Services
</title><link rel="stylesheet" type="text/css" href="http://i.s-
microsoft.com/en-us/homepage/style.cssx?
k=~/shared/templates/Styles/Base/viewport-
css.aspx;~/shared/templates/Styles/Reset/reset-
css.aspx;~/shared/templates/Styles/Views/cols-
css.aspx;~/shared/templates/Styles/Base/webfont-
css.aspx;~/shared/templates/Styles/Base/type-
css.aspx;~/shared/templates/Styles/Base/layout-
css.aspx;~/shared/templates/Styles/Views/header-
css.aspx;~/shared/templates/Styles/Views/search-
css.aspx;~/shared/templates/Styles/Views/list-
css.aspx;~/shared/templates/Styles/Views/menu-
css.aspx;~/shared/templates/Styles/Views/hero-
css.aspx;~/shared/templates/Styles/Views/pivot-
css.aspx;~/shared/templates/Styles/Views/highlights-
css.aspx;~/shared/templates/Styles/Views/footer-
css.aspx;~/shared/templates/Styles/animations-css.aspx&amp;sc=/en-
us/home/site.config&amp;pc=&amp;v=38186074"></link>
    <!--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.ashx.-->
    <script type="text/javascript" src="http://i.s-microsoft.com/en-
```



Cookies and site data

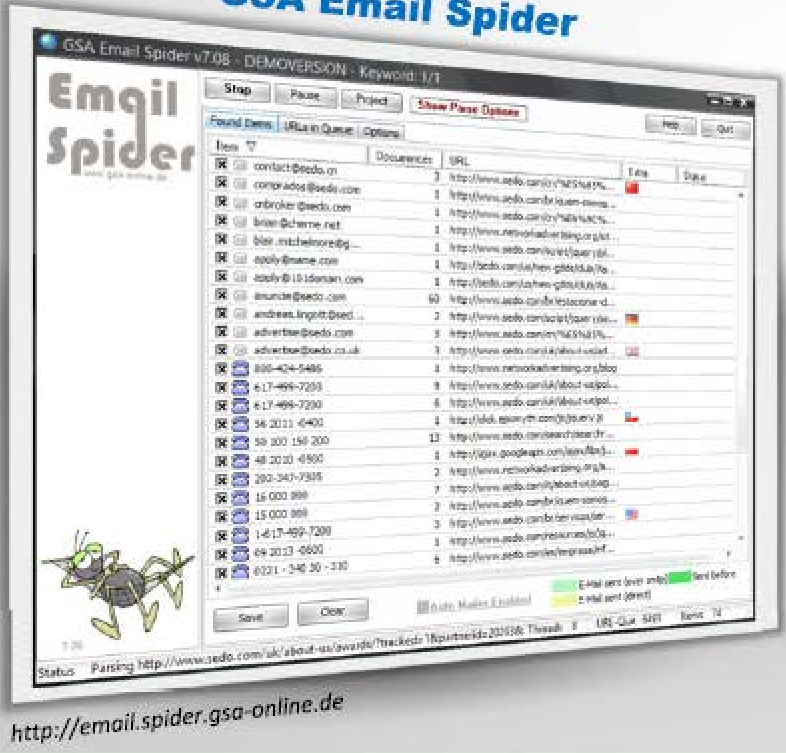
Site	Locally stored data
microsoftsto.112.2o7.net	1 cookie
hollywood.122.2o7.net	1 cookie
addthis.com	6 cookies
static.addtheany.com	2 cookies
adinteras.com	2 cookies
admailtiser.com	1 cookie
adnext.fr	4 cookies
adnxs.com	3 cookies

Name: s_vi
Content: [CS]v1|29195080005161CED-40000146600001DE[CE]
Domain: .microsoftsto.112.2o7.net
Path: /
Send for: Any kind of connection
Accessible to script: Yes
Created: Friday, September 13, 2013 10:58:29 AM
Expires: Sunday, September 13, 2015 10:58:29 AM

Website Footprinting using Web Spiders

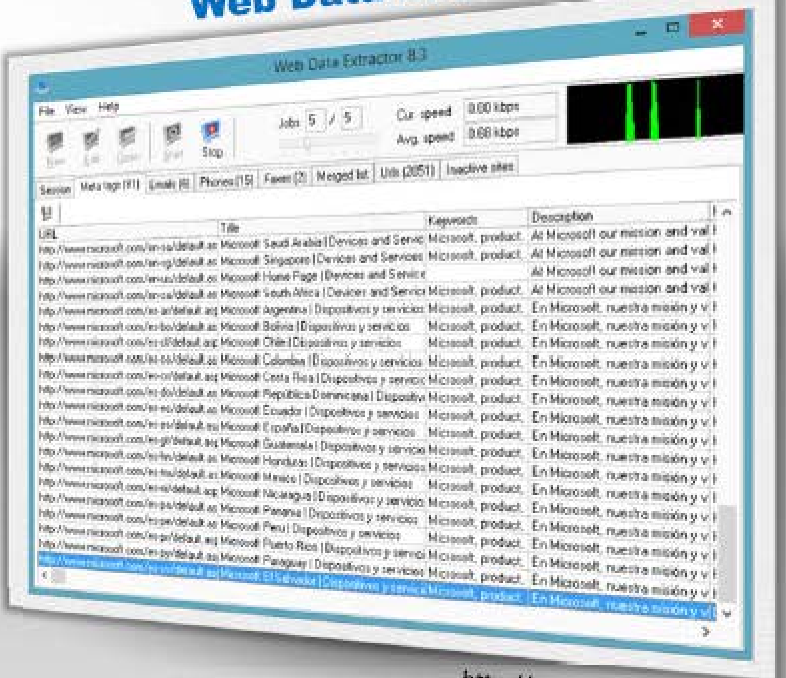
- Web spiders perform automated searches on the target website and collect specified information such as **employee names**, **email addresses**, etc.
- Attackers use the collected information to perform further **footprinting** and **social engineering attacks**

GSA Email Spider



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

Web Data Extractor



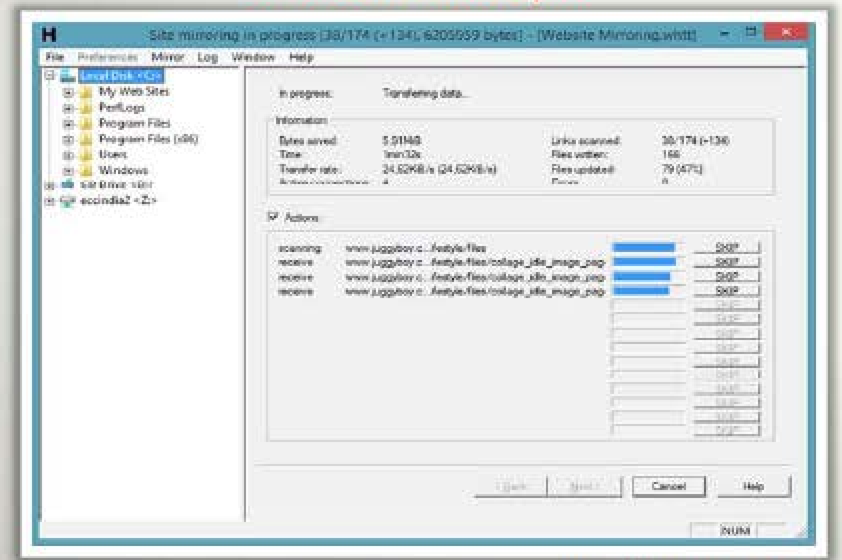
http://www.webextractor.com

Mirroring Entire Website

C|EH 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


Site mirroring in progress [38/174 (+134), 6205959 bytes] - [Website Mirroring.whtt]

In progress: Transferring data...

Information

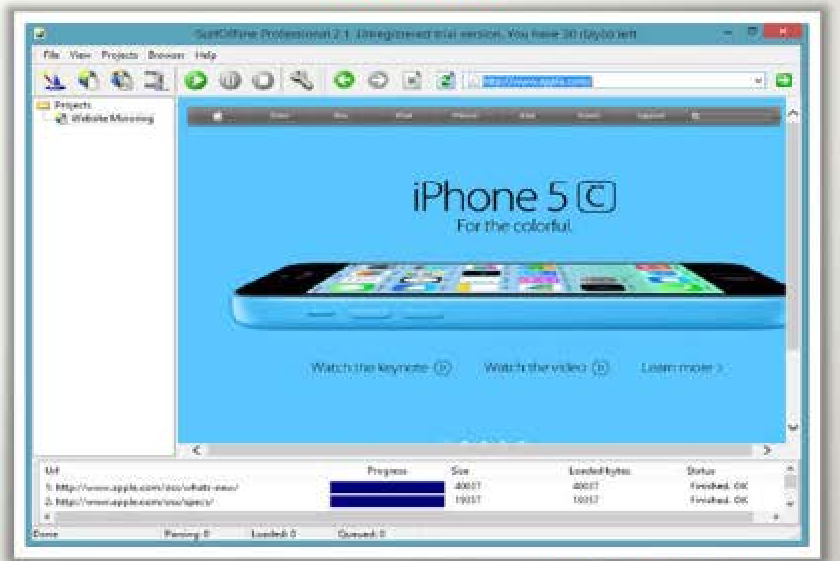
Bytes saved: 5.91MiB
Time: 1min32s
Transfer rate: 24.52KiB/s (24.52KiB/s)
Links scanned: 38/174 (+134)
Files written: 166
Files updated: 79 (47%)

☑ Actions

```
scanning   www.juggyboy.c.../lestyle/files
receive    www.juggyboy.c.../lestyle/files/collage_idle_image_.png
receive    www.juggyboy.c.../lestyle/files/collage_idle_image_.png
receive    www.juggyboy.c.../lestyle/files/collage_idle_image_.png
```

(http://www.httrack.com)

SurfOffline


SurfOffline Professional 2.1. Unregistered trial version. You have 30 day(s) left

Url	Progress	Size	Loaded bytes	Status
1. http://www.apple.com/iphone-5c/		40037	40037	Finished, OK
2. http://www.apple.com/iphone-5c/specs/		19037	19037	Finished, OK

Done Parsing: 0 Loaded: 0 Queued: 0

(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

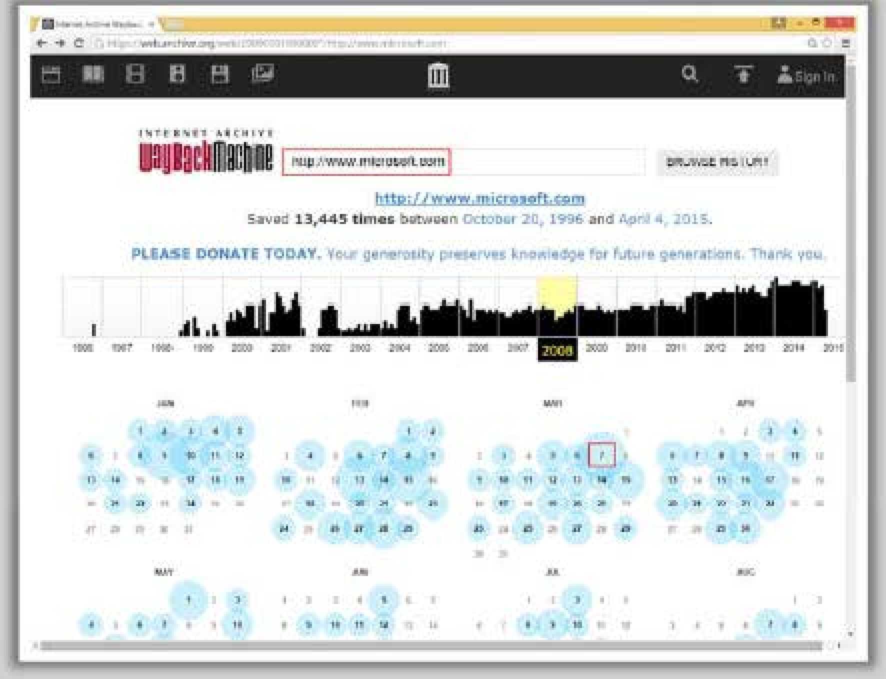
Offline Explorer Enterprise
http://www.metaproducts.com

GNU Wget
http://www.gnu.org

Hooeey Webprint
http://www.hooeeywebprint.com

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

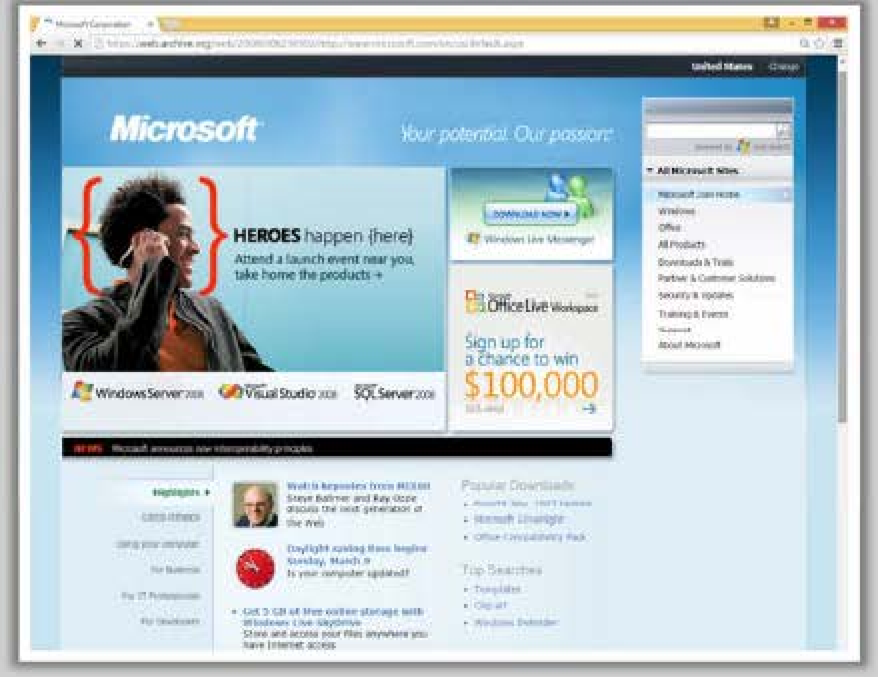
Internet Archive's Wayback Machine allows you to visit archived versions of websites



http://www.microsoft.com

Saved 13,445 times between October 20, 1996 and April 4, 2015.

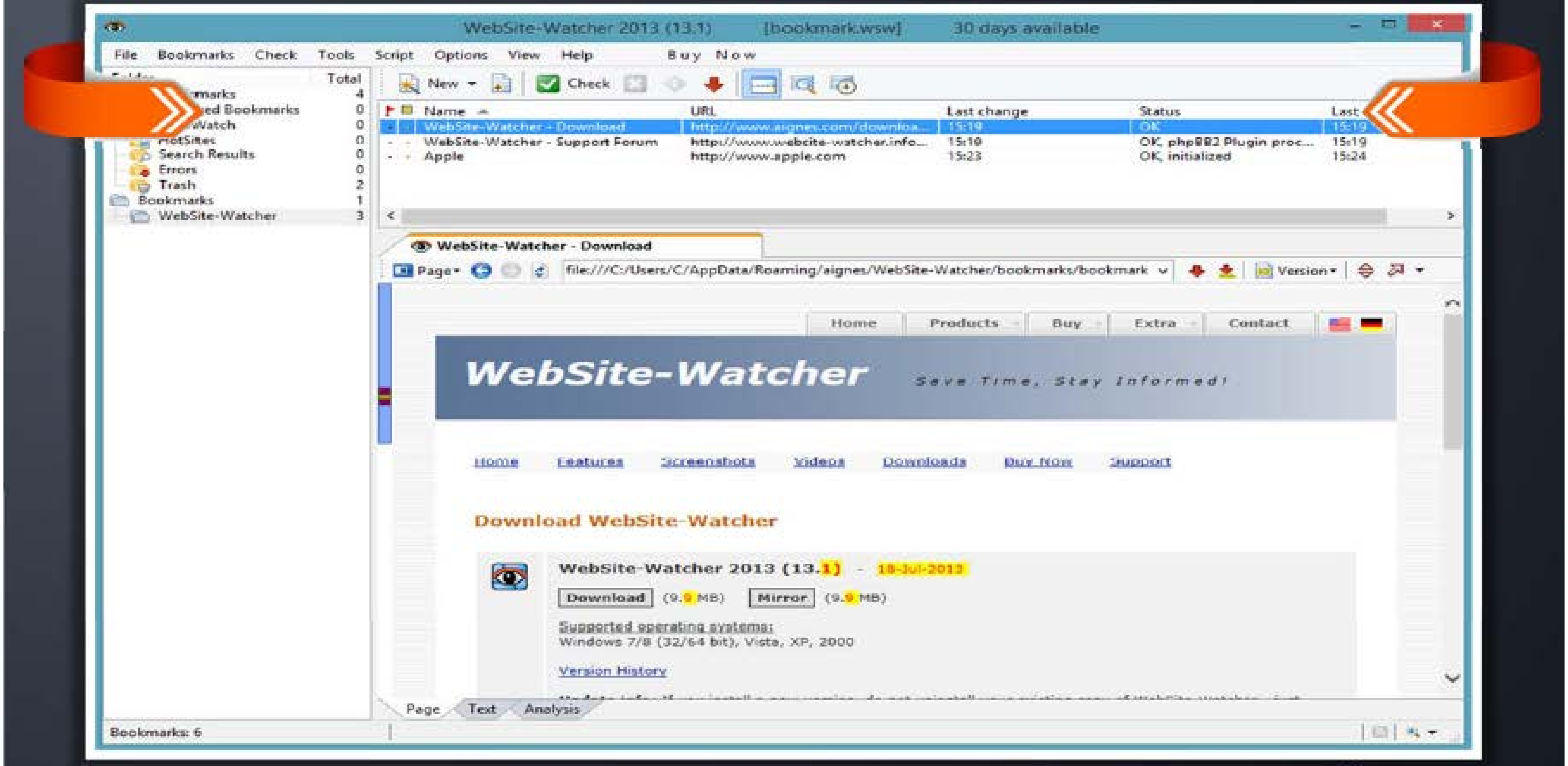
PLEASE DONATE TODAY. Your generosity preserves knowledge for future generations. Thank you.



Microsoft announces new interoperability principles

Monitoring Web Updates Using Website-Watcher

Website-Watcher automatically checks web pages for updates and changes



WebSite-Watcher 2013 (13.1) [bookmark.wsw] 30 days available

	Total
...marks	4
...ed Bookmarks	0
...Watch	0
HotSites	0
Search Results	0
Errors	0
Trash	2
Bookmarks	1
WebSite-Watcher	3

Name	URL	Last change	Status	Last
WebSite-Watcher - Download	http://www.aignes.com/downloa...	15:19	OK	15:19
WebSite-Watcher - Support Forum	http://www.website-watcher.info...	15:10	OK, phpBB2 Plugin proc...	15:19
Apple	http://www.apple.com	15:23	OK, initialized	15:24

WebSite-Watcher - Download

file:///C:/Users/C/AppData/Roaming/aignes/WebSite-Watcher/bookmarks/bookmark

Download WebSite-Watcher

WebSite-Watcher 2013 (13.1) - 18-Jul-2013

Download (9.9 MB) Mirror (9.9 MB)

Supported operating systems:
Windows 7/8 (32/64 bit), Vista, XP, 2000

Version History

Bookmarks: 6

http://aignes.com

Web Updates Monitoring Tools

Change Detection
http://www.changedetection.com

Follow That Page
http://www.followthatpage.com

Page2RSS
http://page2rss.com

Watch That Page
http://www.watchthatpage.com

Check4Change
https://addons.mozilla.org

OnWebChange
http://onwebchange.com

Infominder
http://www.infominder.com

TrackedContent
http://trackedcontent.com

Websnitcher
http://websnitcher.com

Update Scanner
https://addons.mozilla.org

Footprinting Methodology

1 Footprinting through Search Engines

2 Footprinting Using Advanced Google Hacking Techniques

3 Footprinting through Social Networking Sites

4 Website Footprinting

5 **Email Footprinting**

6 Competitive Intelligence

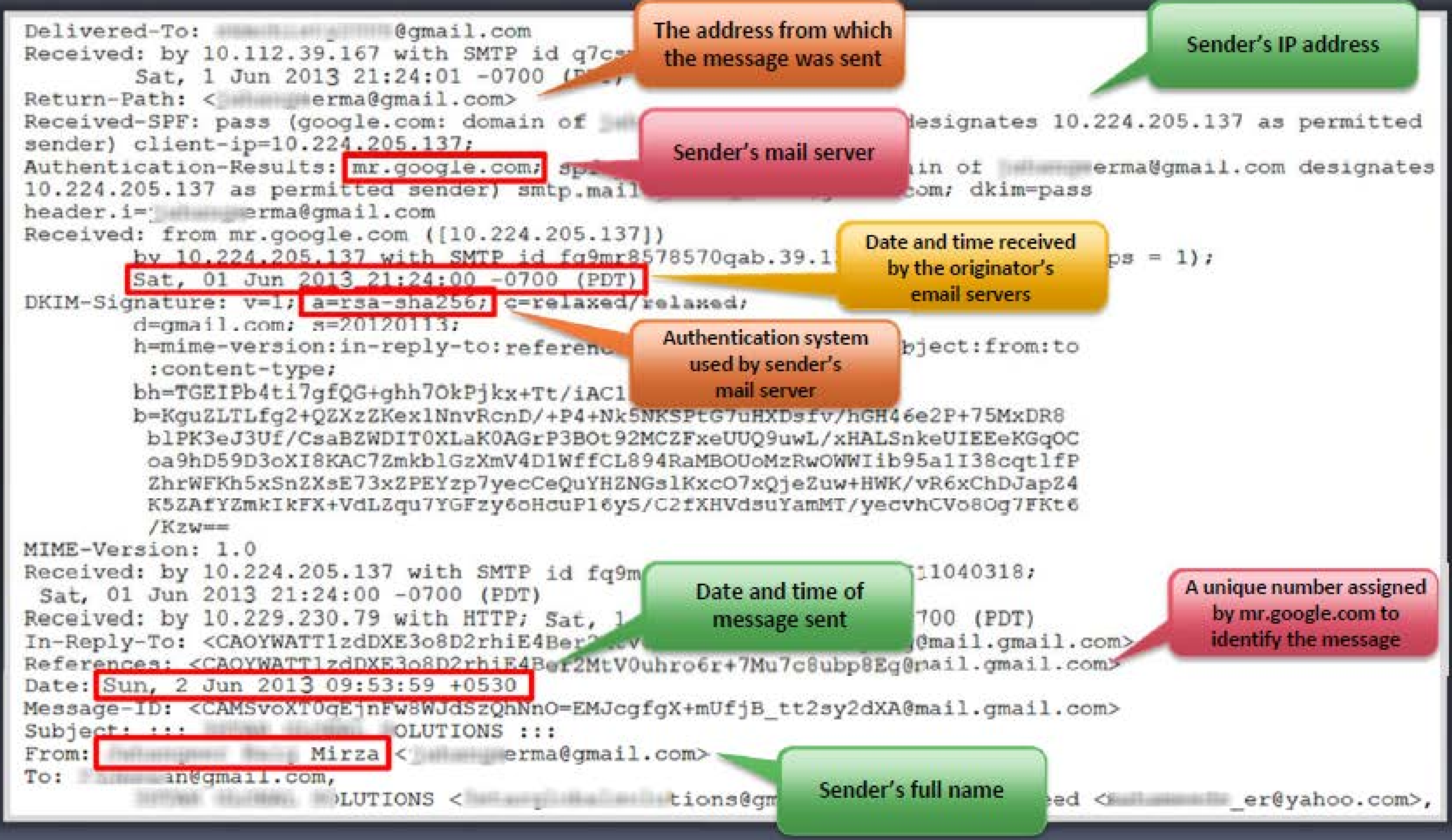
7 WHOIS Footprinting

8 DNS Footprinting

9 Network Footprinting

10 Footprinting through Social Engineering

Collecting Information from Email Header



```
Delivered-To: [redacted]@gmail.com
Received: by 10.112.39.167 with SMTP id q7c
        Sat, 1 Jun 2013 21:24:01 -0700 (
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; sp                      in of [redacted]erma@gmail.com designates
10.224.205.137 as permitted sender) smtp.mail                  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                 ps = 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:referen                 bject:from:to
         :content-type;
        bh=TGEIPb4ti7gfQG+ghh7OkPjkx+Tt/iAC1
        b=KguZLTLfg2+QZXzZKex1NnvRcnD/+P4+Nk5NKSPtG7uHXDsfv/hGH46e2P+75MxDR8
         b1PK3eJ3Uf/CsaBZWDIT0XLaK0AGrP3BOt92MCZFxeUUQ9uwL/xHALSnkeUIEEeKGqOC
         oa9hD59D3oXI8KAC7ZmkblGzXmV4D1WffCL894RaMBOUoMzRwOWWIib95a1I38cqt1fP
         ZhrWFKh5xSnZXsE73xZPEYzp7yecCeQuYHZNGslKxcO7xQjeZuw+HWK/vR6xChDJapZ4
         K5ZAfYZmkIkFX+VdLZqu7YGFzy6oHcuP16yS/C2fXHVdsuYamMT/yecvhCVo8Og7FKt6
         /Kzw==
MIME-Version: 1.0
Received: by 10.224.205.137 with SMTP id fq9m                 11040318;
 Sat, 01 Jun 2013 21:24:00 -0700 (PDT)
Received: by 10.229.230.79 with HTTP; Sat, 1                 700 (PDT)
In-Reply-To: <CAOYWATT1zdDXE3o8D2rhiE4Ber                   @mail.gmail.com>
References: <CAOYWATT1zdDXE3o8D2rhiE4Ber2MtV0uhro6r+7Mu7c8ubp8Eq@mail.gmail.com>
Date: Sun, 2 Jun 2013 09:53:59 +0530
Message-ID: <CAMSvoXT0qEjnFw8WJdSzQhNnO=EMJcgfgX+mUfjB_tt2sy2dXA@mail.gmail.com>
Subject: ::: [redacted]OLUTIONS :::
From: [redacted] Mirza <[redacted]erma@gmail.com>
To: [redacted]an@gmail.com,
        [redacted]OLUTIONS <[redacted]tions@gm                 ed <[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

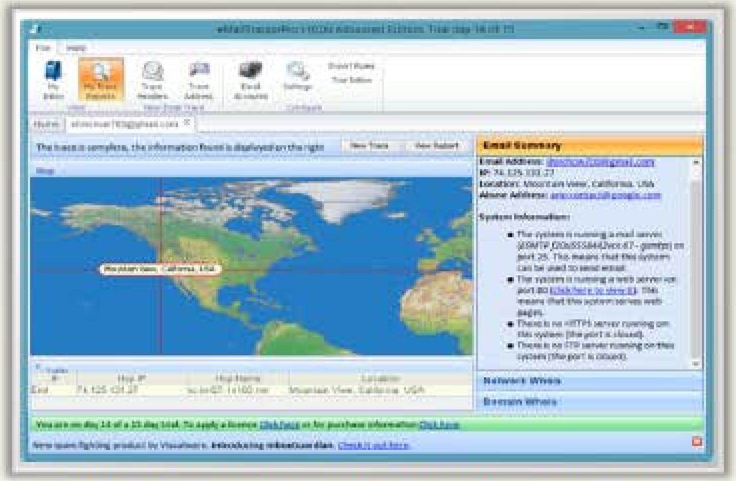
Authentication system used by sender's mail server

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



The trace is complete, the information found is displayed on the right

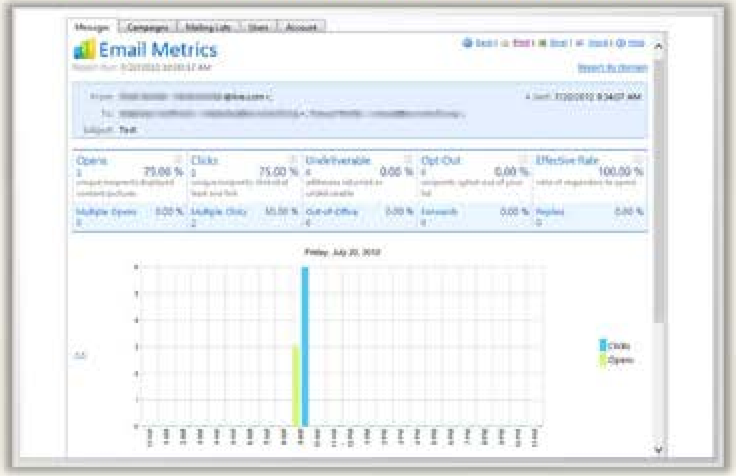
Location: Mountain View, California, USA

System Information:

- The system is running a mail server on port 25. This means that this system can be used to send email.
- The system is running a web server on port 80. This means that this system serves web pages.
- There is no HTTPS server running on this system (the port is closed).
- There is no FTP server running on this system (the port is closed).

End | 74.125 | Mountain View, California, USA

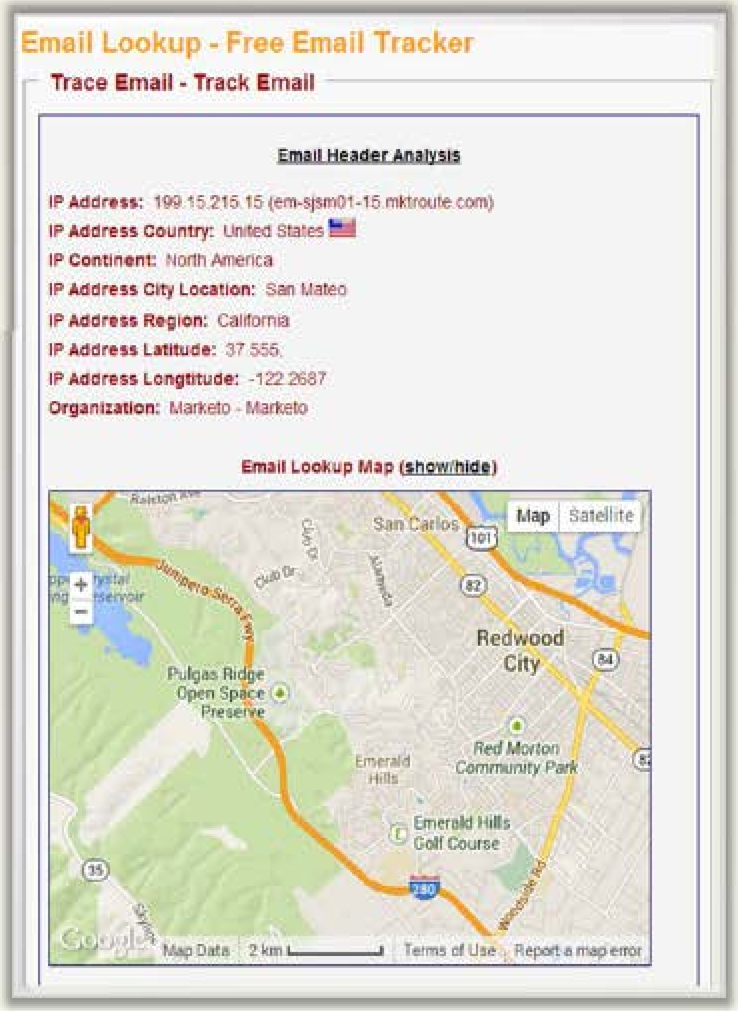
eMailTrackerPro (*http://www.emailtrackerpro.com*)



Subject: Test

Opens	Clicks	Undeliverable	Opt-Out	Effective Rate
75.00 %	75.00 %	0.00 %	0.00 %	100.00 %
Multiple Opens 0.00 %	Multiple Clicks 50.00 %	Out-of-Office 0.00 %	Forwards 0.00 %	Replies 0.00 %

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 Longtitude: -122.2687
Organization: Marketo - Marketo

Email Lookup Map (show/hide)

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

Email Tracking Tools (Cont'd)

C|EH Certified Ethical Hacker

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

CEH Certified Ethical Hacker

- 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

02 Search engines, Internet, and online DB

03 Press releases and annual reports

04 Trade journals, conferences, and newspaper

05 Patent and trademarks

06 Social engineering employees

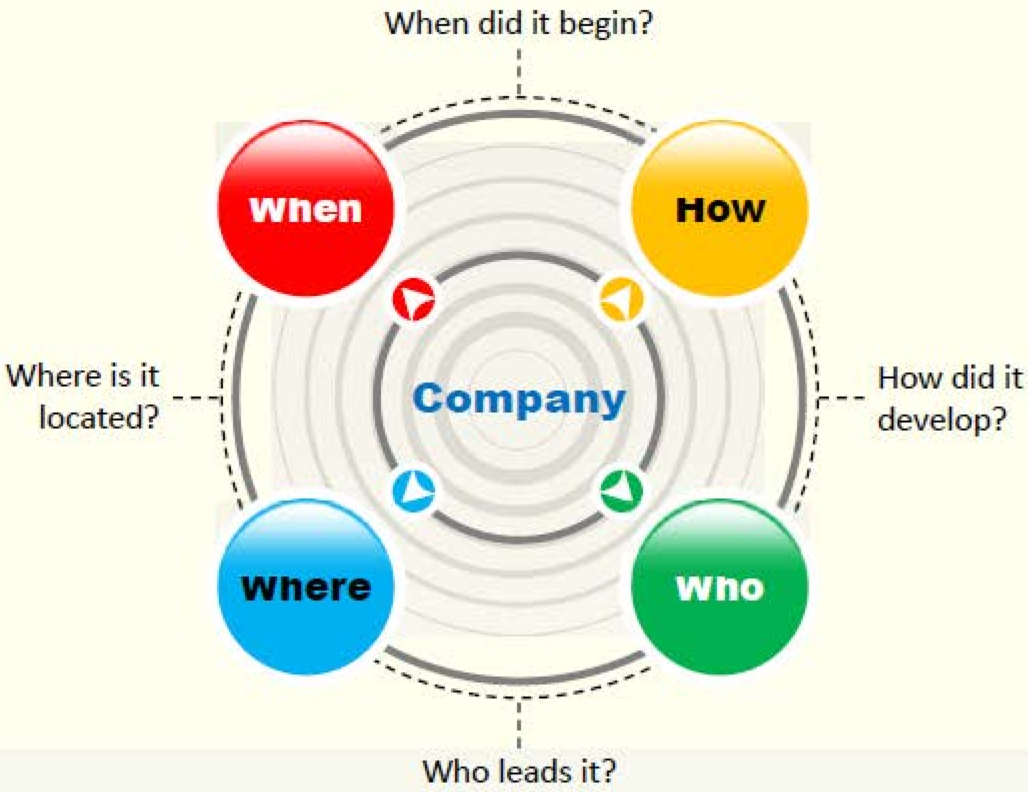
07 Product catalogues and retail outlets

08 Analyst and regulatory reports

09 Customer and vendor interviews

10 Agents, distributors, and suppliers

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



Visit These Sites

01. EDGAR Database

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

02. Hoovers

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

03. LexisNexis

http://www.lexisnexis.com

04. Business Wire

http://www.businesswire.com

Competitive Intelligence - What Are the Company's Plans?

01 **Market Watch** (*http://www.marketwatch.com*)

02 **The Wall Street Transcript** (*http://www.twst.com*)

03 **Lipper Marketplace** (*http://www.lippermarketplace.com*)

04 **Euromonitor** (*http://www.euromonitor.com*)

05 **Experian** (*http://www.experian.com*)

06 **SEC Info** (*http://www.secinfo.com*)

07 **The Search Monitor** (*http://www.thesearchmonitor.com*)

Competitive Intelligence - What Expert Opinions Say About the Company

CEH Certified Ethical Hacker

ABI/INFORM Global

http://www.proquest.com

Compete PRO™

http://www.compete.com

AttentionMeter

http://www.attentionmeter.com

Copernic Tracker

http://www.copernic.com

Jobitorial

http://www.jobitorial.com

SEMRush

http://www.semrush.com

Monitoring Website Traffic of Target Company

CEH Certified Ethical Hacker

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

Total visitors

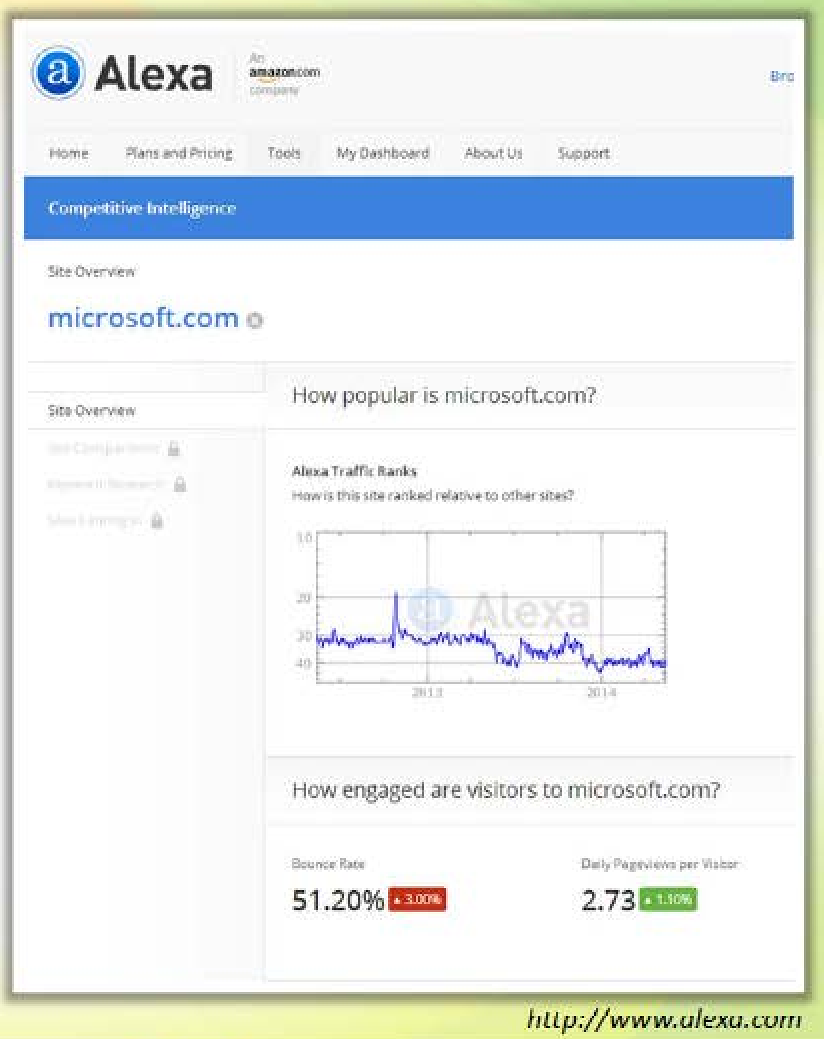
Page views

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



Site Overview

microsoft.com

How popular is microsoft.com?

Alexa Traffic Ranks

How is this site ranked relative to other sites?

How engaged are visitors to microsoft.com?

Bounce Rate

51.20% ▲ 3.00%

Daily Pageviews per Visitor

2.73 ▲ 1.10%

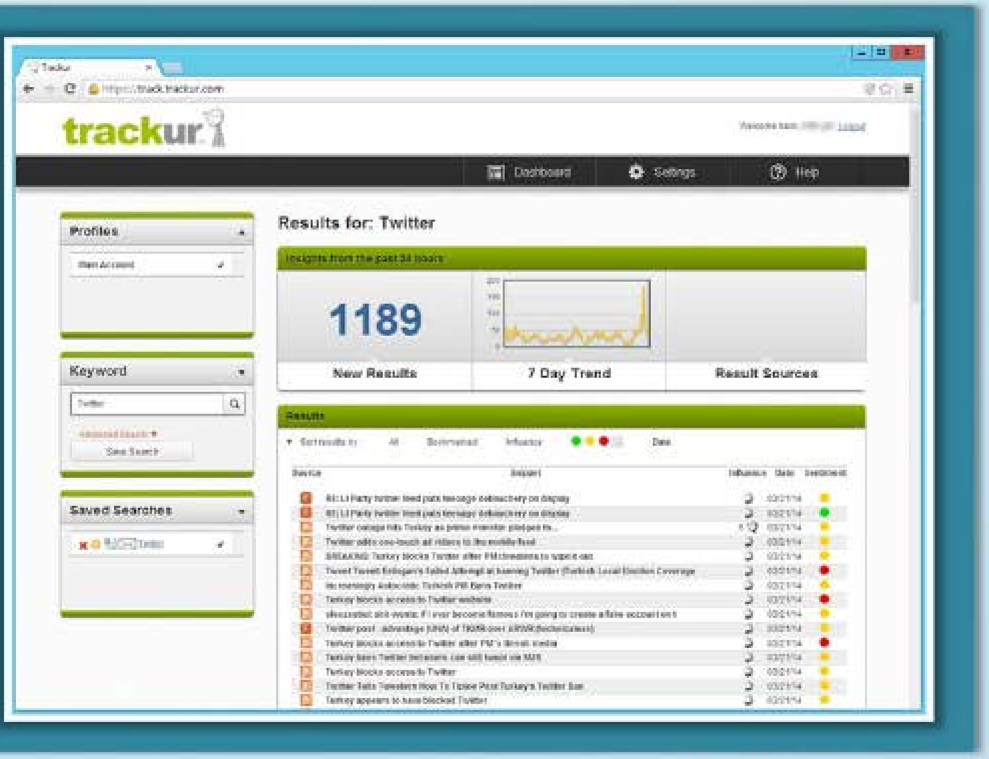
http://www.alexa.com

Tracking Online Reputation of the Target

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

An attacker makes use of ORM tracking tools to:

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



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

C|EH Certified Ethical Hacker

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)

ARIN

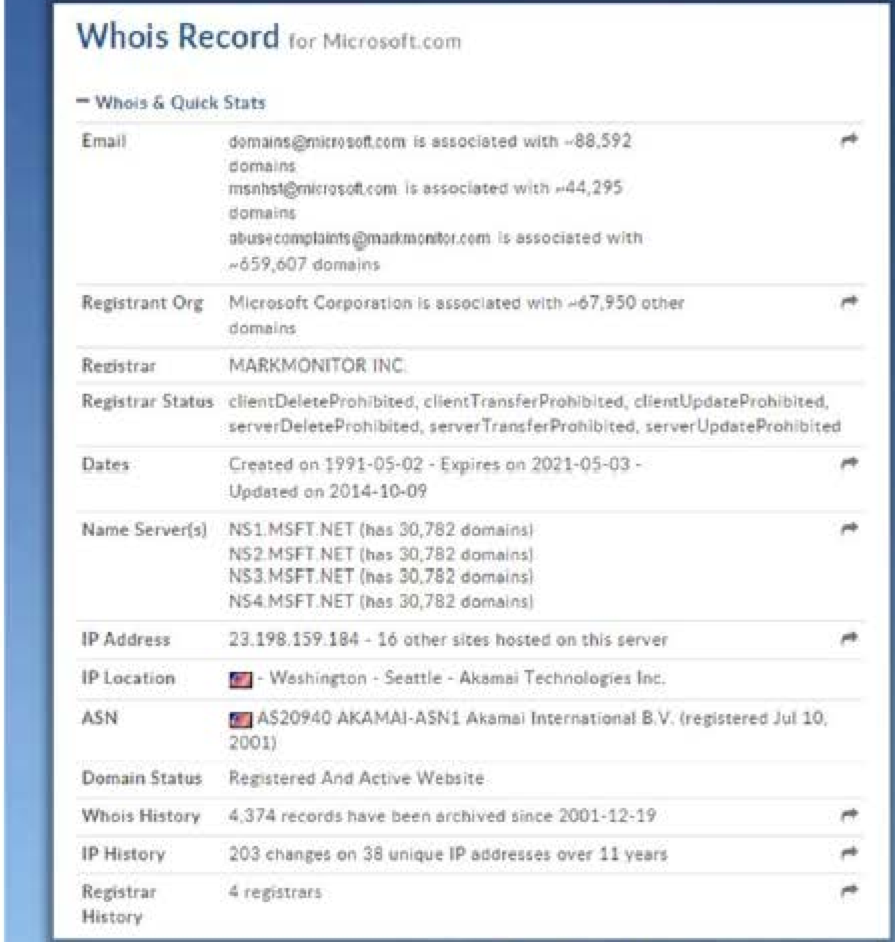
AFRINIC

RIPE NCC

LACNIC

APNIC

WHOIS Lookup Result Analysis

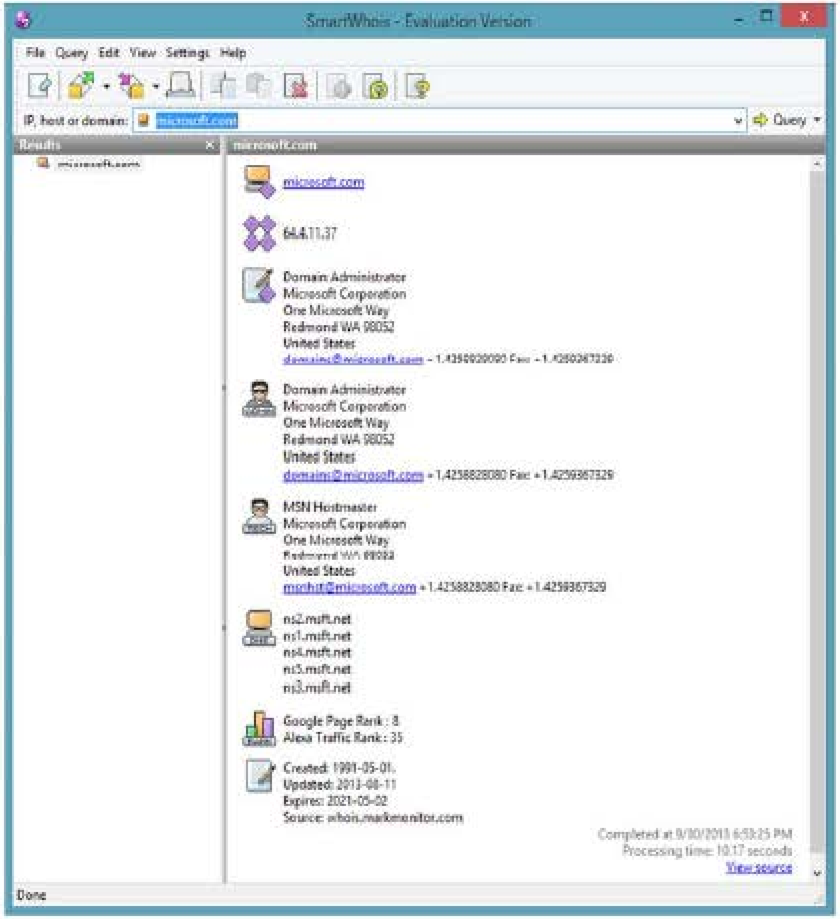


Whois Record for Microsoft.com

− 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 History	4 registrars

http://whois.domaintools.com


SmartWhois - Evaluation Version
File Query Edit View Settings Help
IP, host or domain:
Query
Results
microsoft.com

IP, host or domain: microsoft.com

microsoft.com

64.4.11.37

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
United States
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

Domain Administrator
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
United States
domains@microsoft.com +1.4258828080 Fax: +1.4259367329

MSN Hostmaster
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
United States
msnhst@microsoft.com +1.4258828080 Fax: +1.4259367329

ns2.msft.net
ns1.msft.net
ns4.msft.net
ns5.msft.net
ns3.msft.net

Google Page Rank : 8
Alexa Traffic Rank : 35

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

Completed at 9/30/2013 6:53:25 PM
Processing time: 10.17 seconds
View source

Done

http://www.tamos.com

WHOIS Lookup Tools

C|EH 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.sobolsoft.com

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

HotWhois
http://www.tialsoft.com

ActiveWhois
http://www.johnru.com

WhoisThisDomain
http://www.nirsoft.net

SoftFuse Whois
http://www.softfuse.com

Whois
http://technet.microsoft.com

WHOIS Lookup Tools (Cont'd)

C|EH Certified Ethical Hacker

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

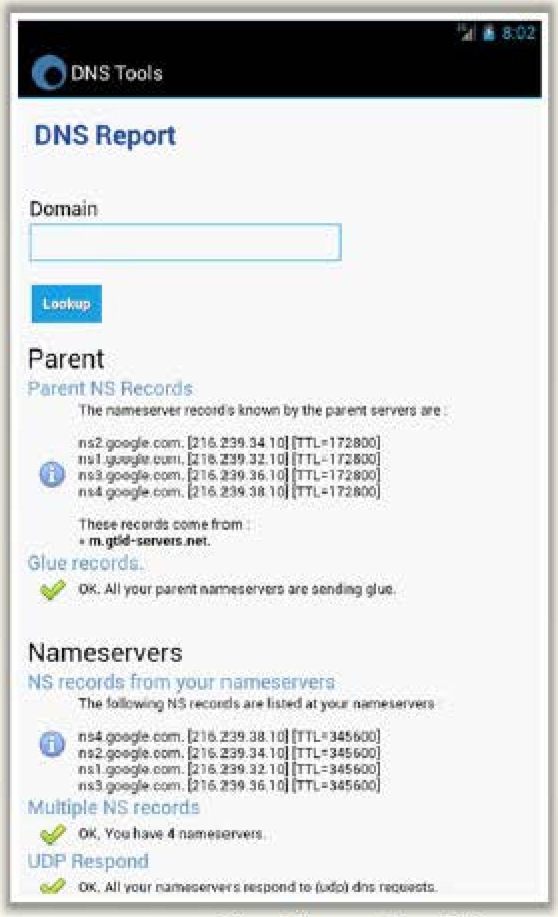
Network Solutions Whois
http://www.networksolutions.com

WebToolHub
http://www.webtoolhub.com/tn561381-whois-lookup.aspx

UltraTools
https://www.ultratools.com/whois/home

WHOIS Lookup Tools for Mobile

DNS Tools


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.gtld-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

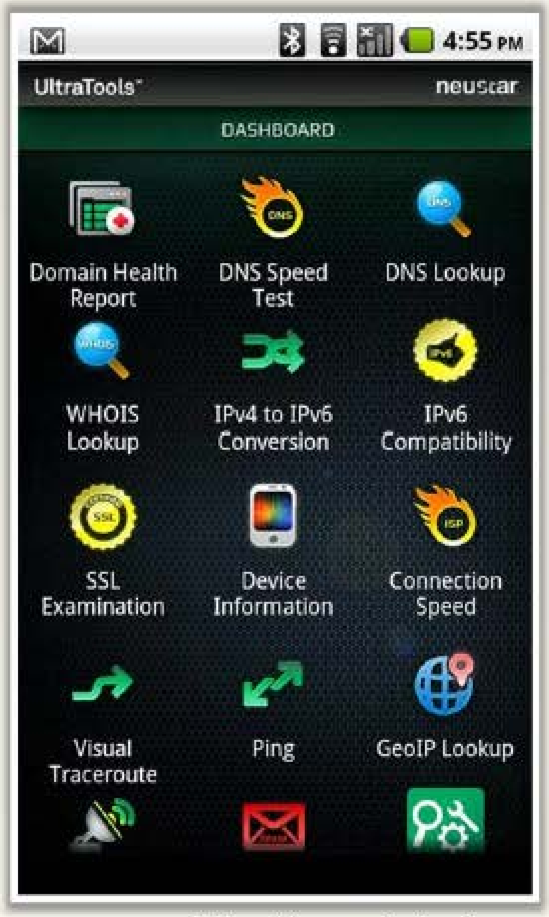
✓ OK. You have 4 nameservers.

UDP Respond

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

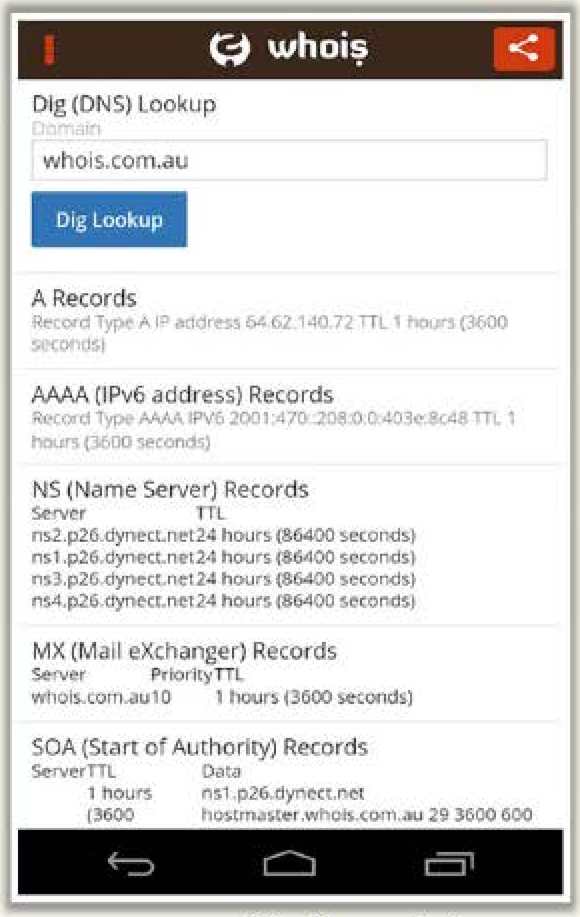
https://www.dnssniffer.com

UltraTools Mobile



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::208:0:0:403e:8c48 TTL 1 hours (3600 seconds)

NS (Name Server) Records

```
Server                TTL
ns2.p26.dynect.net24 hours (86400 seconds)
ns1.p26.dynect.net24 hours (86400 seconds)
ns3.p26.dynect.net24 hours (86400 seconds)
ns4.p26.dynect.net24 hours (86400 seconds)
```

MX (Mail eXchanger) Records

```
Server          PriorityTTL
whois.com.au10       1 hours (3600 seconds)
```

SOA (Start of Authority) Records

```
ServerTTL         Data
     1 hours      ns1.p26.dynect.net
     (3600        hostmaster.whois.com.au 29 3600 600
```

http://www.whois.com.au

Footprinting Methodology

C|EH Certified Ethical Hacker

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

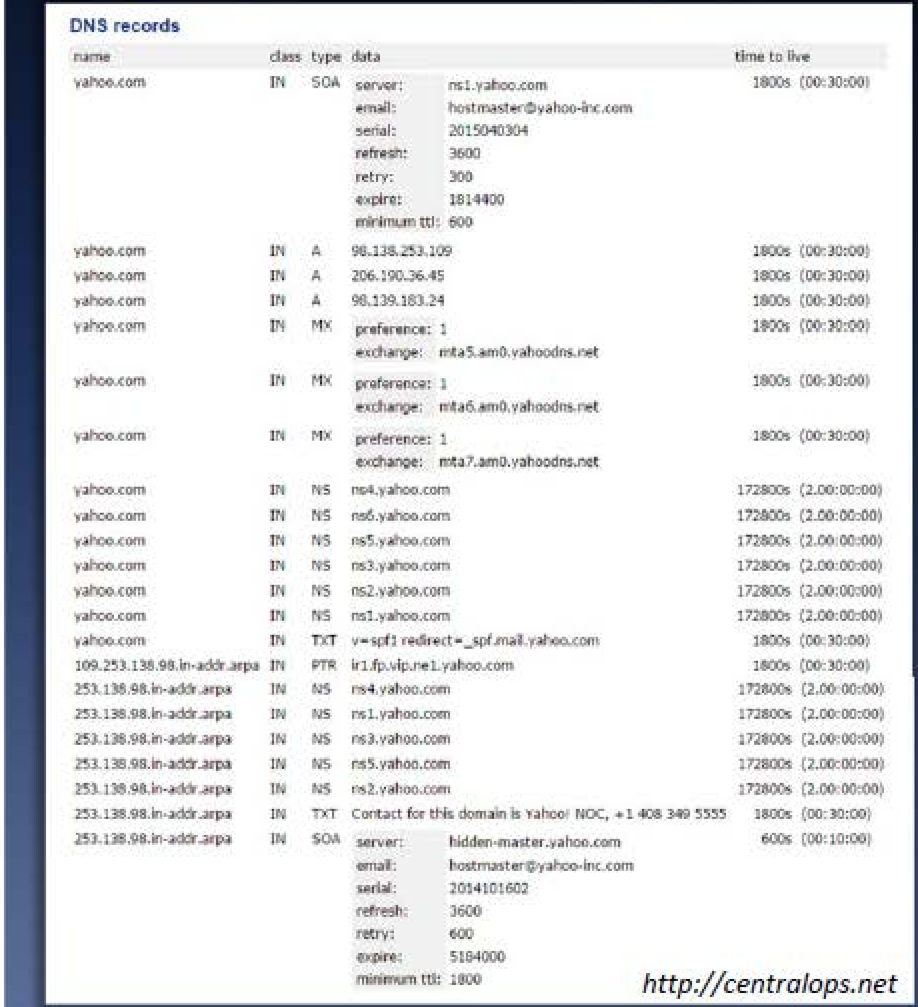
DNS Interrogation Tools

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

Extracting DNS Information (Cont'd)

C|EH Certified Ethical Hacker

Domain Dossier

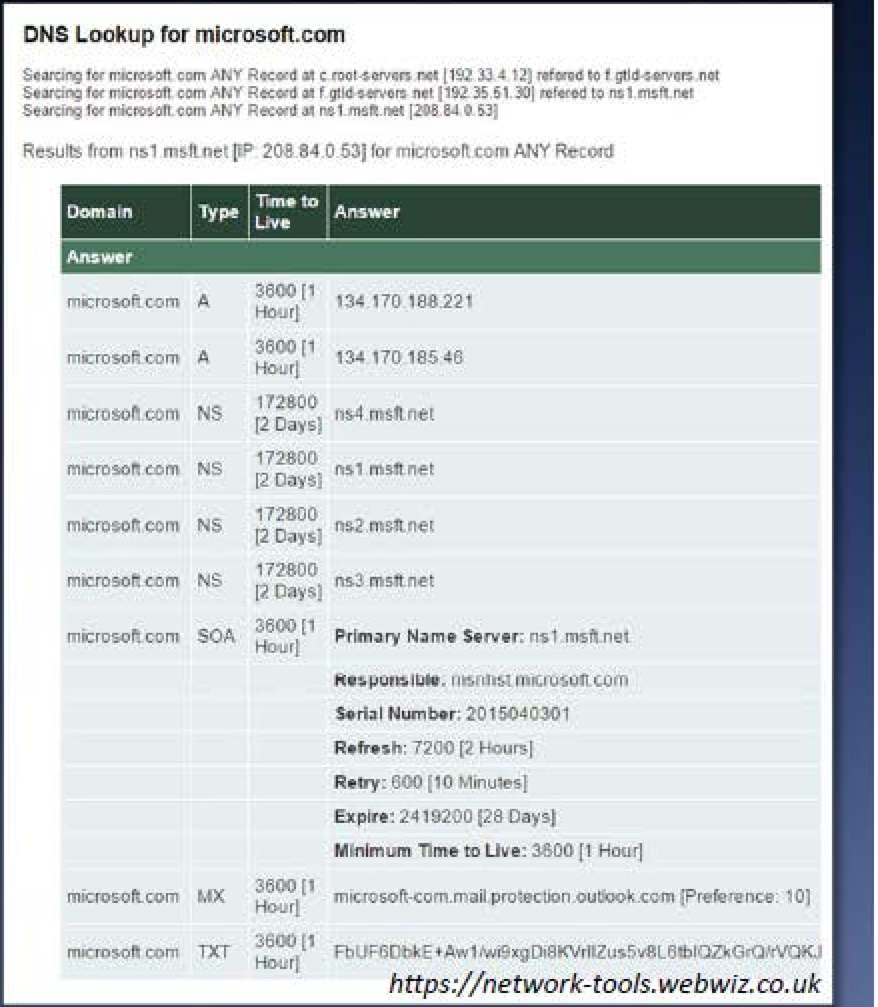


DNS records

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

Searcing for microsoft.com ANY Record at c.root-servers.net [192.33.4.12] refered to f.gtld-servers.net
Searcing for microsoft.com ANY Record at f.gtld-servers.net [192.35.51.30] 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: msnhst.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/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJ

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

DNS Interrogation Tools

C|EH 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

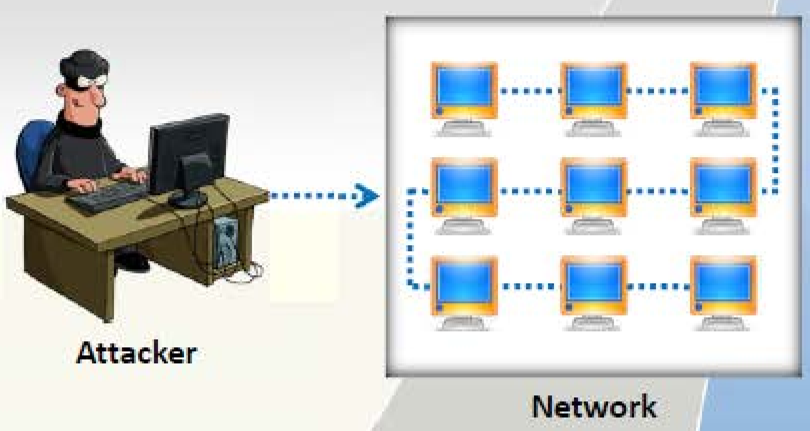
DNS Query Utility
http://www.dnsqueries.com

DNS Lookup
https://www.ultratools.com

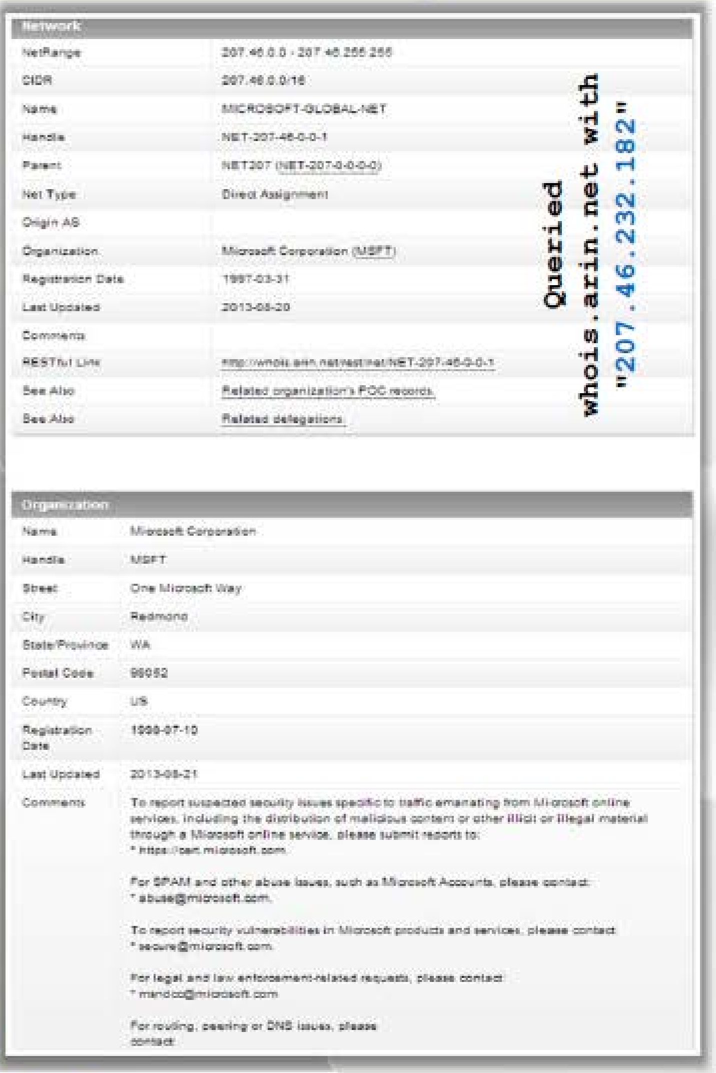
DNS Query Utility
http://www.webmaster-toolkit.com

Locate the Network Range

- 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



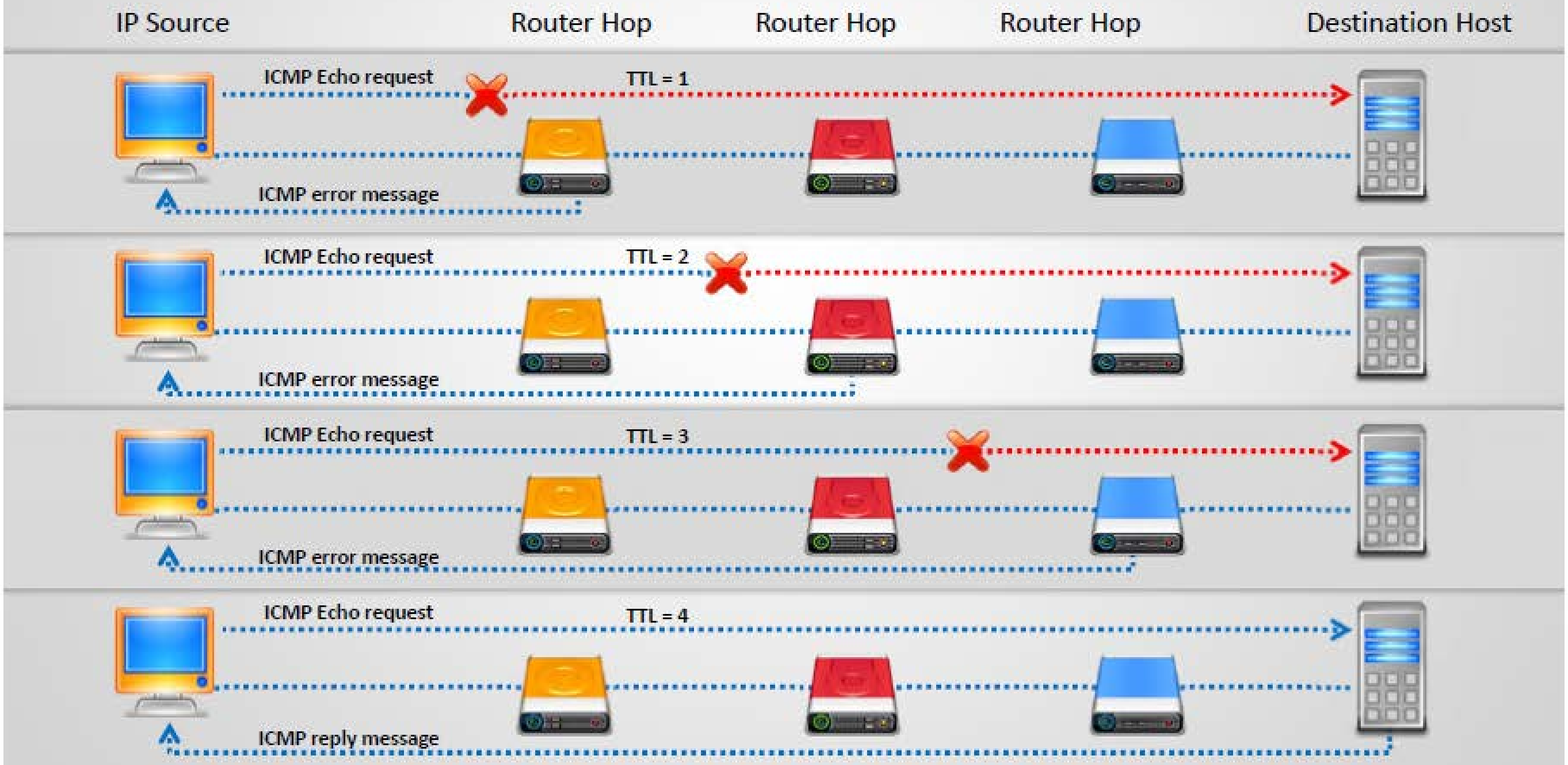
Queried whois.arin.net with "207.46.232.182"

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.

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://cert.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: * msndcc@microsoft.com For routing, peering or DNS issues, please contact:

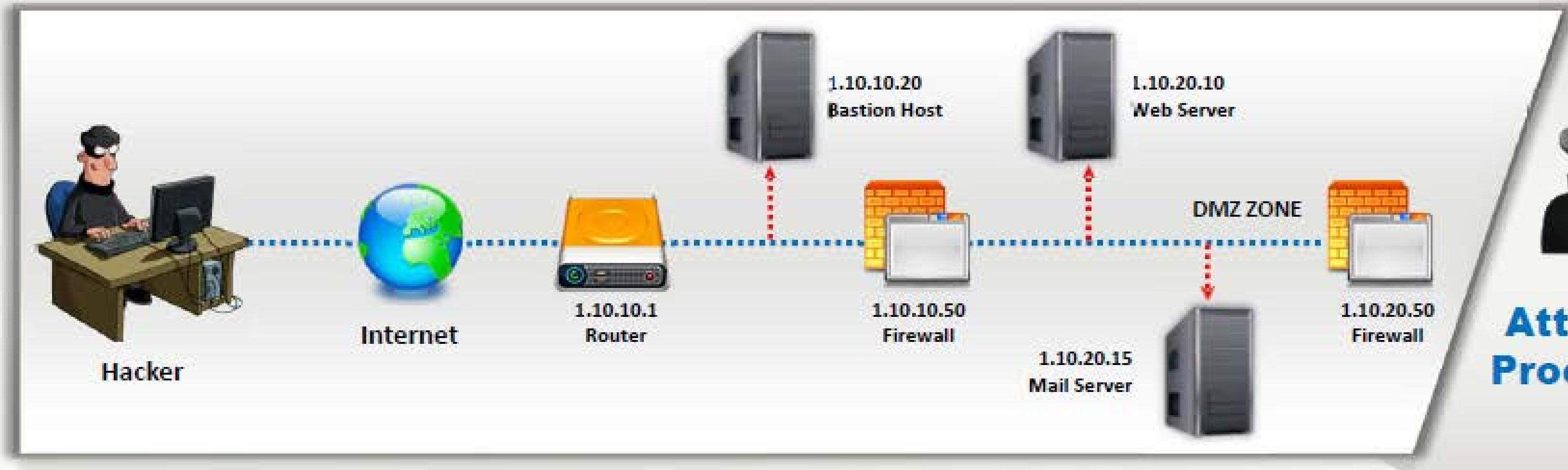
Traceroute

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



Traceroute Analysis

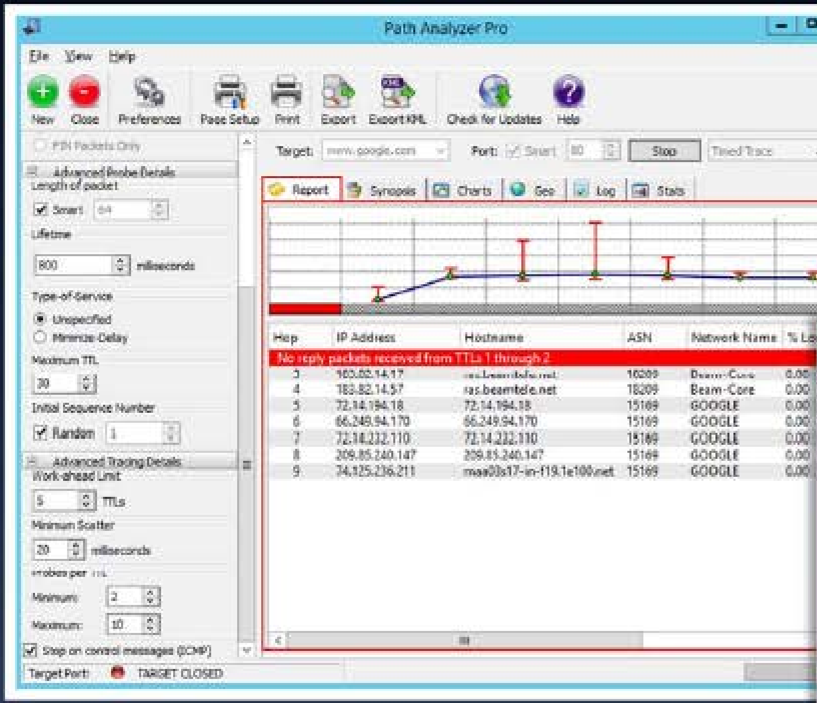
- Attackers conduct traceroute to extract information about: **network topology**, **trusted routers**, and **firewall locations**
  - For example: after running several **traceroutes**, an attacker might obtain the following information:
    - traceroute 1.10.10.20, second to last hop is 1.10.10.1
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



Attack Process

Traceroute Tools

Path Analyzer Pro


Path Analyzer Pro
File View Help
New Close Preferences Page Setup Print Export Export KML Check for Updates Help
Report Synopsis Charts Geo Log Stats

Target: www.google.com Port: ☑ Smart 80 Stop Timed Trace

○ FIN Packets Only

Advanced Probe Details

Length of packet ☑ Smart 64

Lifetime 800 milliseconds

Type-of-Service
● Unspecified
○ Minimize Delay

Maximum TTL 30

Initial Sequence Number ☑ Random 1

Advanced Tracing Details

Work-ahead Limit 5 TTLs

Minimum Scatter 20 milliseconds

Probes per TTL
Minimum: 2
Maximum: 10

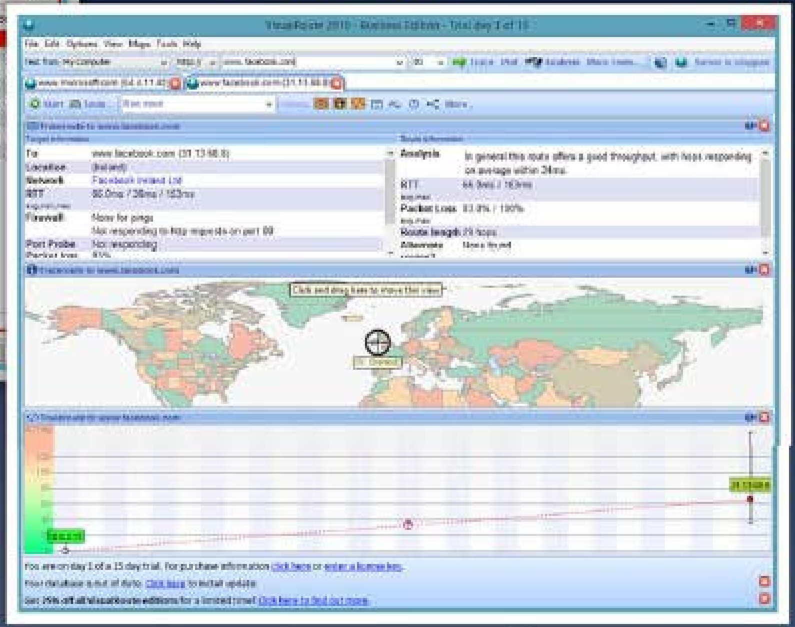
☑ Stop on control messages (ICMP)

Target Port: TARGET CLOSED

Hop	IP Address	Hostname	ASN	Network Name	% Lo
No reply packets received from TTLs 1 through 2					
3	183.82.14.17	ras.beamtele.net	18209	Beam-Core	0.00
4	183.82.14.57	ras.beamtele.net	18209	Beam-Core	0.00
5	72.14.194.18	72.14.194.18	15169	GOOGLE	0.00
6	66.249.94.170	66.249.94.170	15169	GOOGLE	0.00
7	72.14.232.110	72.14.232.110	15169	GOOGLE	0.00
8	209.85.240.147	209.85.240.147	15169	GOOGLE	0.00
9	74.125.236.211	maa03s17-in-f19.1e100.net	15169	GOOGLE	0.00

http://www.pathanalyzer.com

VisualRoute


VisualRoute 2010 - Business Edition - Trial day 1 of 15
File Edit Options View Maps Tools Help
Test from: My computer
www.facebook.com
Trace
Start
Traceroute to www.facebook.com
Target information
Route information
Click and drag here to move the view

To	www.facebook.com (31.13.68.8)
Location	(Ireland)
Network	Facebook Ireland Ltd
RTT	80.0ms / 38ms / 163ms
Firewall	None for pings Not responding to http requests on port 80
Port Probe	Not responding

Analysis	In general this route offers a good throughput, with hops responding on average within 24ms.
RTT	44.9ms / 163ms
Packet Loss	83.8% / 100%
Route length	29 hops
Alternate	None found

You are on day 1 of a 15 day trial. For purchase information click here or enter a license key.

Your database is out of date. Click here to install update.

Get 25% off all VisualRoute editions for a limited time! Click here to find out more.

http://www.visualroute.com

Traceroute Tools (Cont'd)

Network Pinger
http://www.networkpinger.com

GEOSpider
http://www.oreware.com

vTrace
http://vtrace.pl

Trout
http://www.mcafee.com

Roadkil's Trace Route
http://www.roadkil.net

Magic NetTrace
http://www.tialsoft.com

3D Traceroute
http://www.d3tr.de

AnalogX HyperTrace
http://www.analogx.com

Network Systems Traceroute
http://www.net.princeton.edu

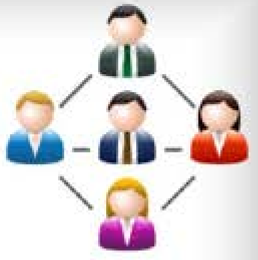
Ping Plotter
http://www.pingplotter.com

Footprinting Methodology

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

Footprinting through Social Engineering

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



Social engineers attempt to gather:

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

Social engineering techniques:

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

Collect Information Using Eavesdropping, Shoulder Surfing, and Dumpster Diving

Eavesdropping

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

Shoulder Surfing

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

Dumpster Diving

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

Module Flow

1 Footprinting Concepts

2 Footprinting Methodology

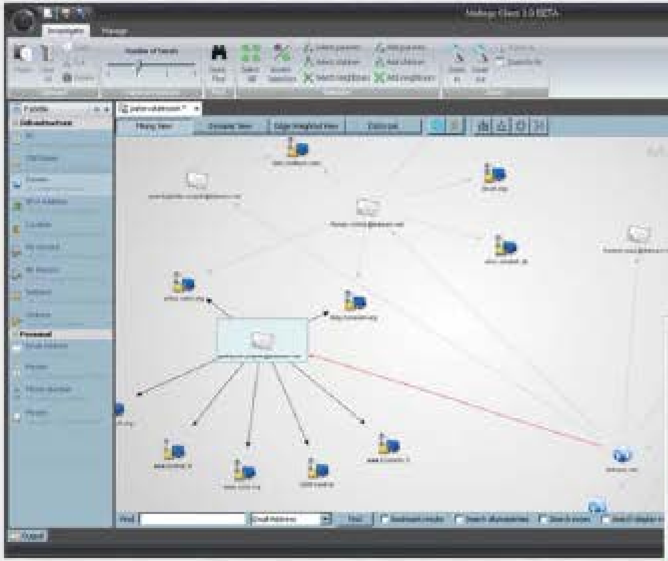
3 Footprinting Tools

4 Footprinting Countermeasures

5 Footprinting Penetration Testing

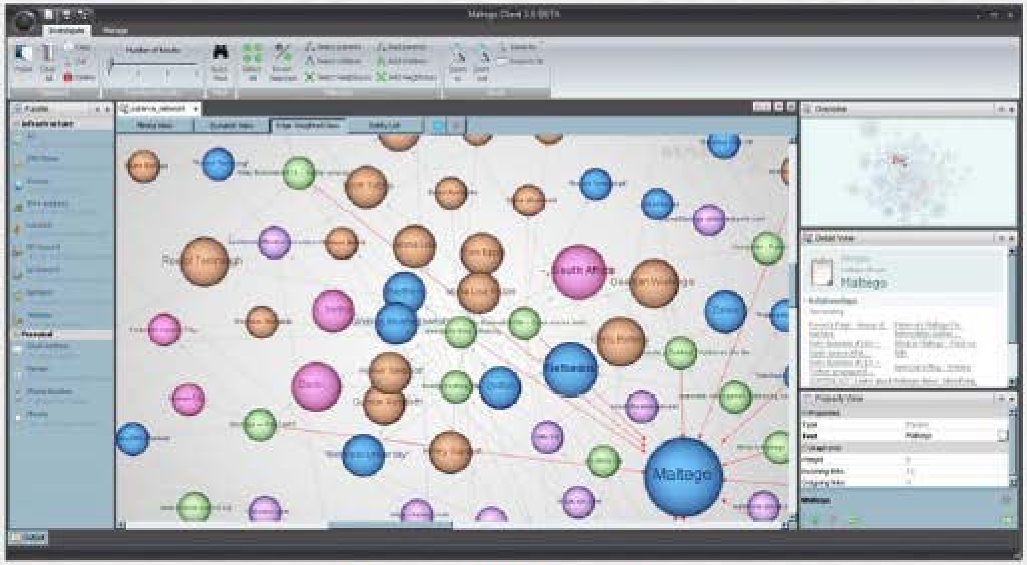
Footprinting Tool: Maltego

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



Internet Domain

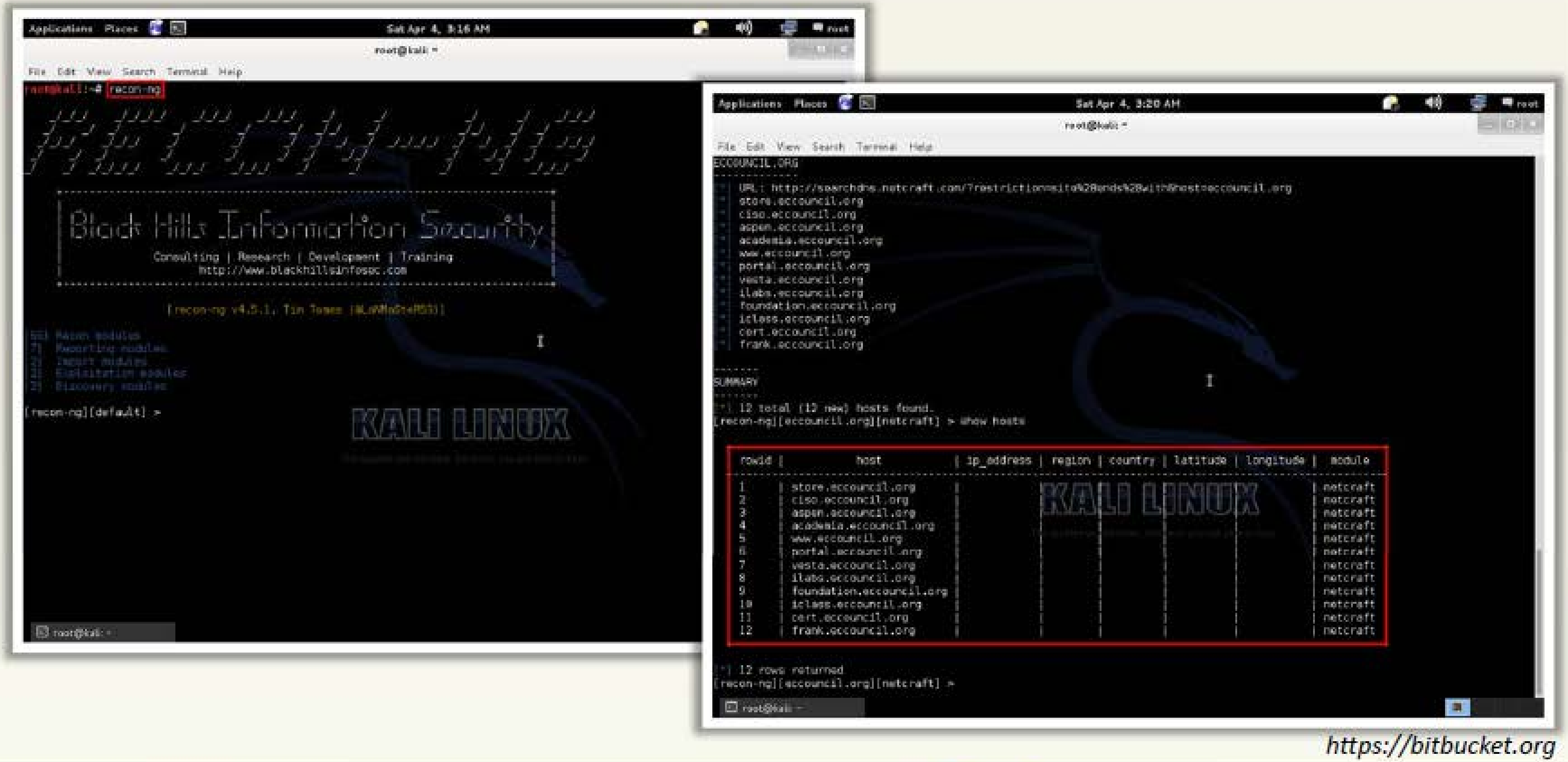
http://www.paterva.com



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



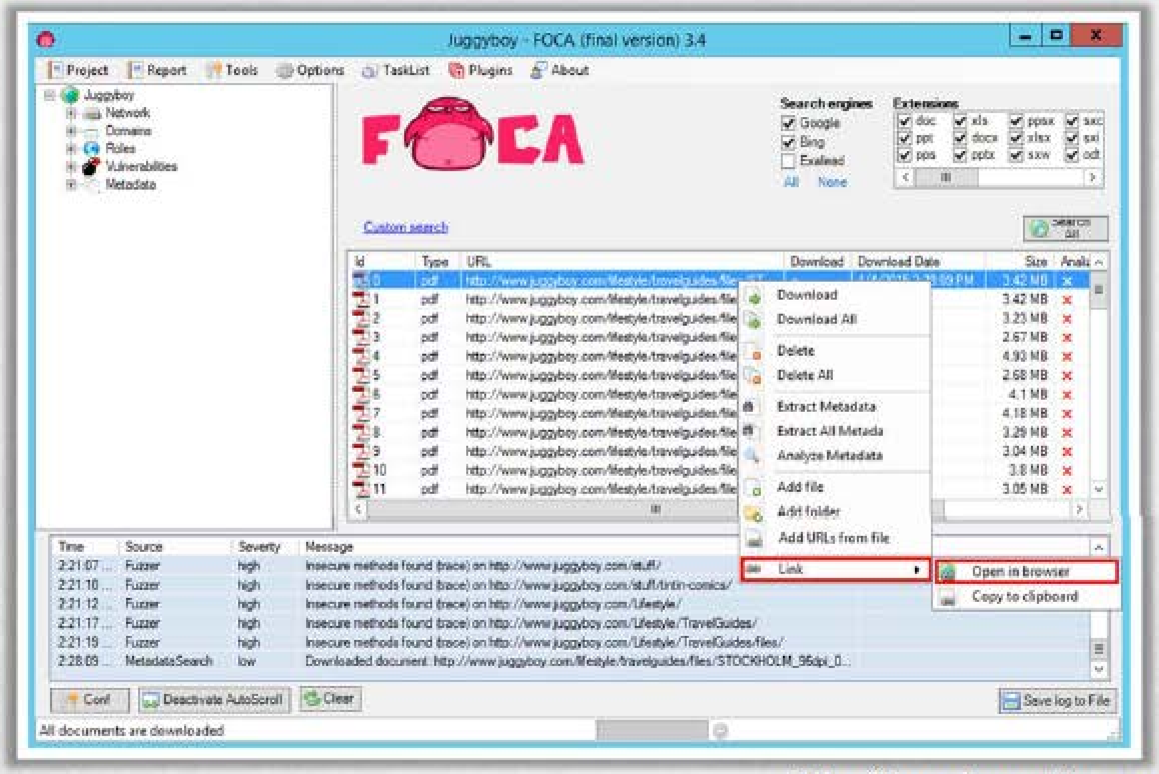
```
root@kali:~# recon-ng

 ---------------------------------------------------------------
 | Black Hills Information Security                             |
 |         Consulting | Research | Development | Training       |
 |              http://www.blackhillsinfosec.com                |
 ---------------------------------------------------------------

              [recon-ng v4.5.1, Tim Tomes (@LaNMaSteR53)]

[66] Recon modules
[7]  Reporting modules
[2]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

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

```
ECCOUNCIL.ORG
-------------
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=eccouncil.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

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.



Search engines: ☑ Google ☑ Bing ☐ Exalead

Extensions: ☑ doc ☑ xls ☑ ppsx ☑ sxc ☑ ppt ☑ docx ☑ xlsx ☑ sxi ☑ pps ☑ pptx ☑ sxw ☑ odt

Id	Type	URL	Download	Download Date	Size	Analy
0	pdf	http://www.juggyboy.com/lifestyle/travelguides/files/ST...	•	1/4/2015 2:28:09 PM	3.42 MB	×
1	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			3.42 MB	×
2	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			3.23 MB	×
3	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			2.67 MB	×
4	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			4.93 MB	×
5	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			2.68 MB	×
6	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			4.1 MB	×
7	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			4.18 MB	×
8	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			3.29 MB	×
9	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			3.04 MB	×
10	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			3.8 MB	×
11	pdf	http://www.juggyboy.com/lifestyle/travelguides/file			3.05 MB	×

```
Time       Source          Severity  Message
2:21:07 ... Fuzzer          high      Insecure methods found (trace) on http://www.juggyboy.com/stuff/
2:21:10 ... Fuzzer          high      Insecure methods found (trace) on http://www.juggyboy.com/stuff/tintin-comics/
2:21:12 ... Fuzzer          high      Insecure methods found (trace) on http://www.juggyboy.com/Lifestyle/
2:21:17 ... Fuzzer          high      Insecure methods found (trace) on http://www.juggyboy.com/Lifestyle/TravelGuides/
2:21:19 ... Fuzzer          high      Insecure methods found (trace) on http://www.juggyboy.com/Lifestyle/TravelGuides/files/
2:28:09 ... MetadataSearch  low       Downloaded document: http://www.juggyboy.com/lifestyle/travelguides/files/STOCKHOLM_96dpi_0...
```

All documents are downloaded

https://www.elevenpaths.com

Additional Footprinting Tools

Prefix WhoIs	*http://pwhois.org*
NetScanTools Pro	*http://www.netscantools.com*
Tctrace	*http://www.phenoelit.org*
Autonomous System Scanner (ASS)	*http://www.phenoelit.org*
DNS-Digger	*http://www.dnsdigger.com*
Netmask	*http://www.phenoelit.org*
Binging	*http://www.blueinfy.com*
SearchBug	*http://www.searchbug.com*
TinEye	*http://www.tineye.com*
Robtex	*http://www.robtex.com*

Additional Footprinting Tools (Cont'd)

CEH Certified Ethical Hacker

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

C|EH 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)

C|EH Certified Ethical Hacker

- 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**

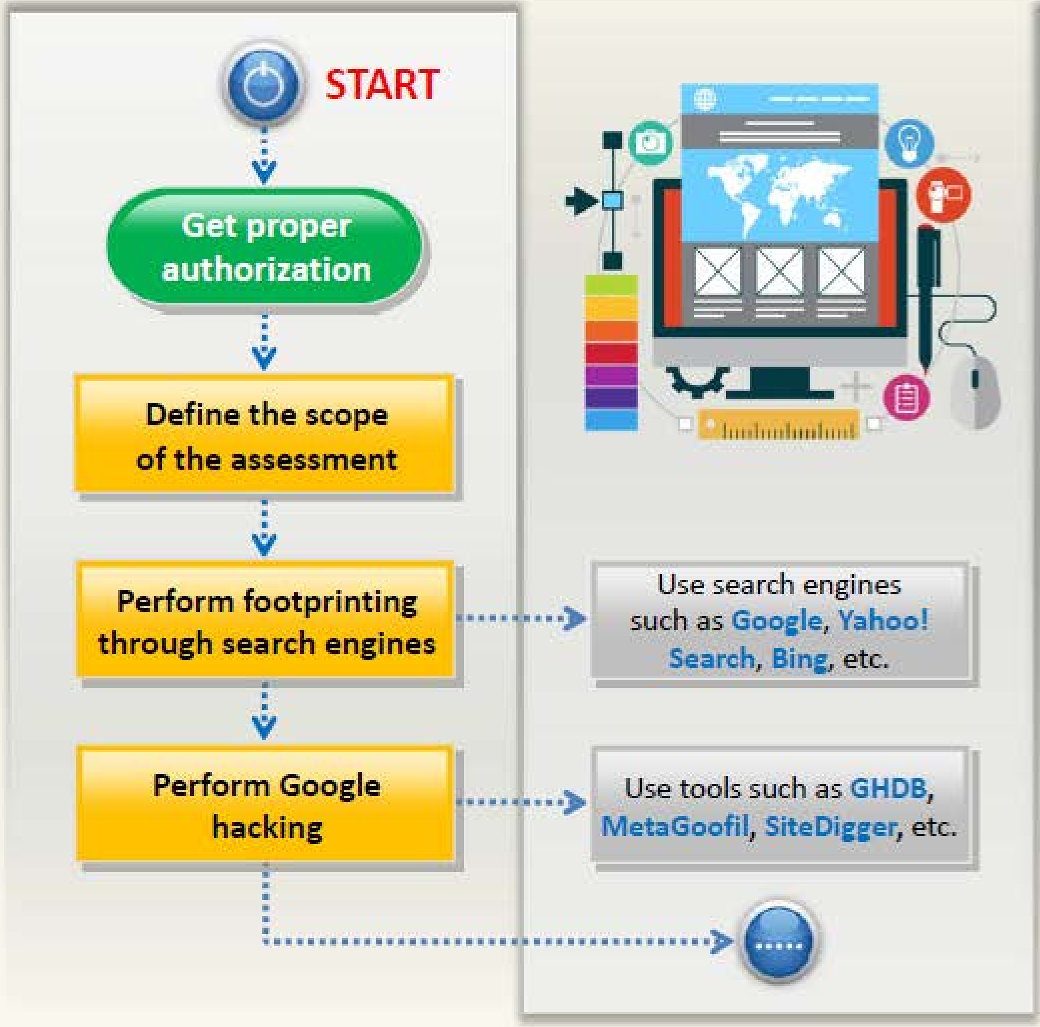
Footprinting pen testing helps organization to:

Prevent **information leakage**

Prevent **social engineering attempts**

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

Footprinting Pen Testing (Cont'd)



START

Get proper authorization

Define the scope of the assessment

Perform footprinting through search engines

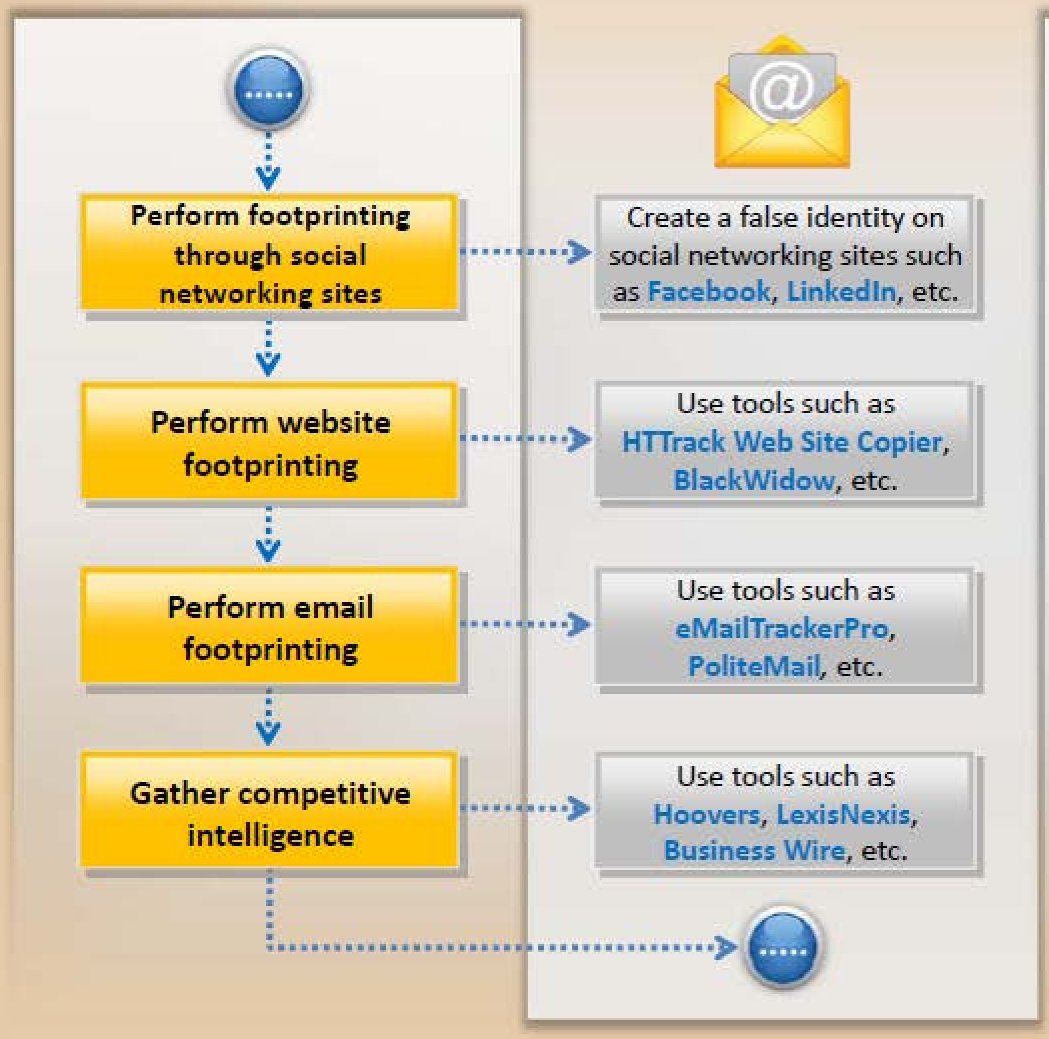
Use search engines such as Google, Yahoo! Search, Bing, etc.

Perform Google hacking

Use tools such as GHDB, MetaGoofil, SiteDigger, etc.

- 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)



Perform footprinting through social networking sites → Create a false identity on social networking sites such as Facebook, LinkedIn, etc.

Perform website footprinting → Use tools such as HTTrack Web Site Copier, BlackWidow, etc.

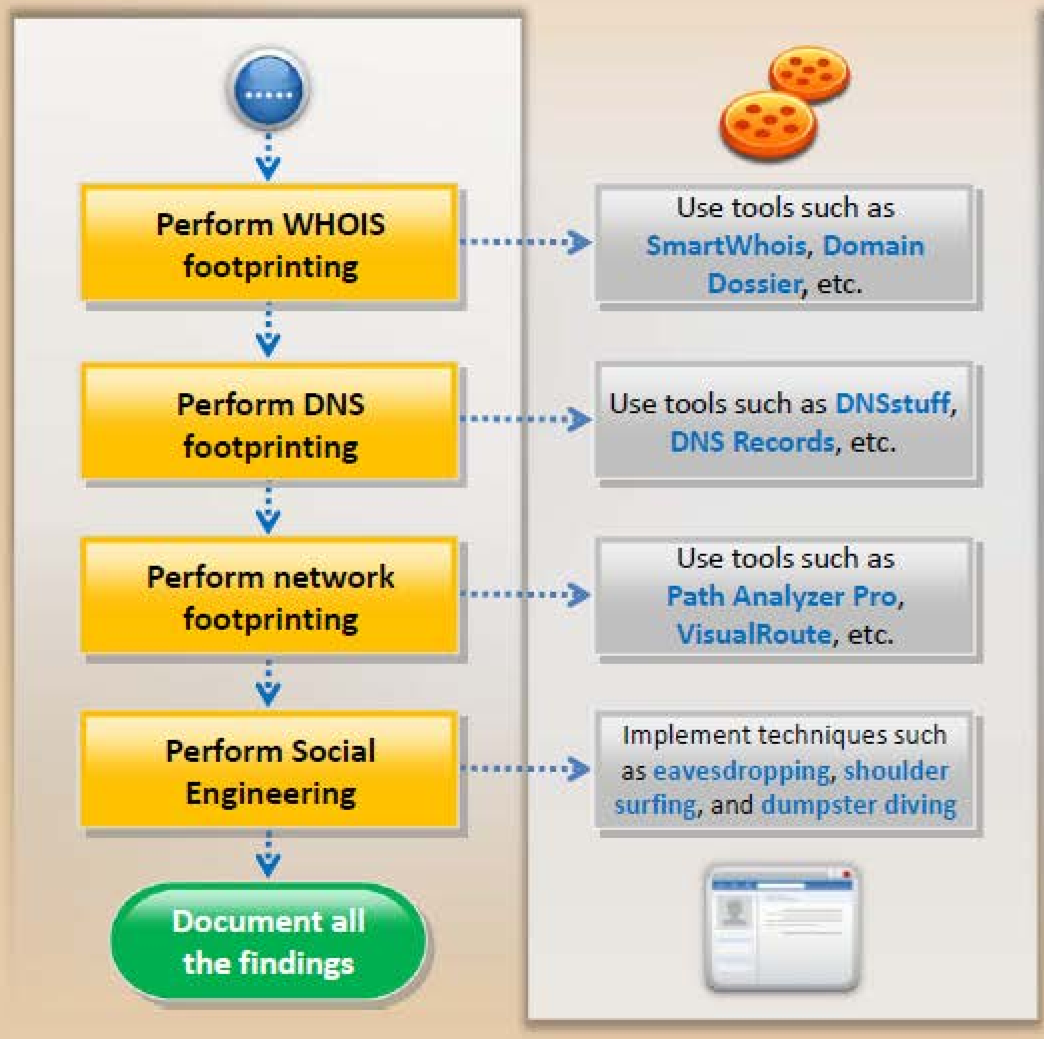
Perform email footprinting → Use tools such as eMailTrackerPro, PoliteMail, etc.

Gather competitive intelligence → Use tools such as Hoovers, LexisNexis, Business Wire, etc.

- 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)

C|EH Certified Ethical Hacker



Perform WHOIS footprinting

Use tools such as SmartWhois, Domain Dossier, etc.

Perform DNS footprinting

Use tools such as DNSstuff, DNS Records, etc.

Perform network footprinting

Use tools such as Path Analyzer Pro, VisualRoute, etc.

Perform Social Engineering

Implement techniques such as eavesdropping, shoulder surfing, and dumpster diving

Document all the findings

- 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

C|EH Certified Ethical Hacker

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:

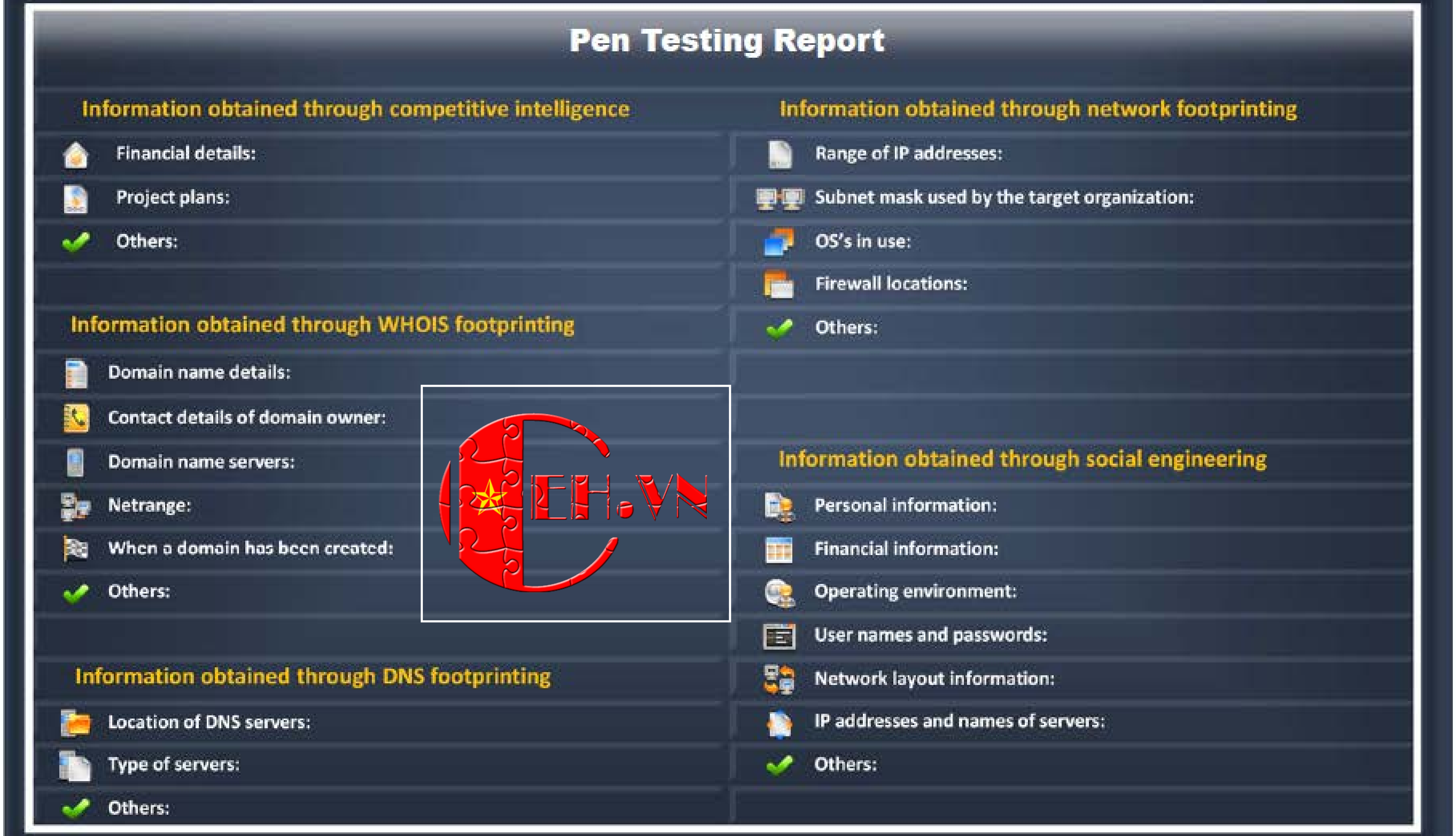
Information obtained through website footprinting

- 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

C|EH Certified Ethical Hacker

□ 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