

Information Gathering



Step 1: Reconnaissance



Overview

What Information does a hacker gather

Organize collected information

How is this information obtained

Google and Queries

What is Footprinting



What Information is gathered by the Hacker?

Whose system is it? Find the owner

What type of systems are used (job advertisements, Way back machine)

How big is the company? Have they merged, acquired, or downsized recently?

How do their sites communicate with each other?

What type of telephone/ PBX/ communication systems are used?

Is the IT support local or off site?

What is accessible from the Internet?
What services, routers, DMZ's?

Online
Information
Sources

Remote
Social
Engineering

Local Social
Engineering
Fire
Inspections

Organizing Collected Information

Leo: meta-text editor

<http://personalpages.tds.net/~edream/front.html>



Leo Tutorial:

http://www.3dtree.com/ev/e/sbooks/leo/sbframetoc_ie.htm



Free Mind Open Source mind mapping software

<http://freemind.sourceforge.net/>



IHMC CmapTools

<http://cmap.ihmc.us/conceptmap.html>

Leo meta-text editor

You can use Leo, a unique, powerful computer program that can be used to organize, analyze and describe text and text files. Leo runs on Windows, Mac, or Linux.

Use Leo:

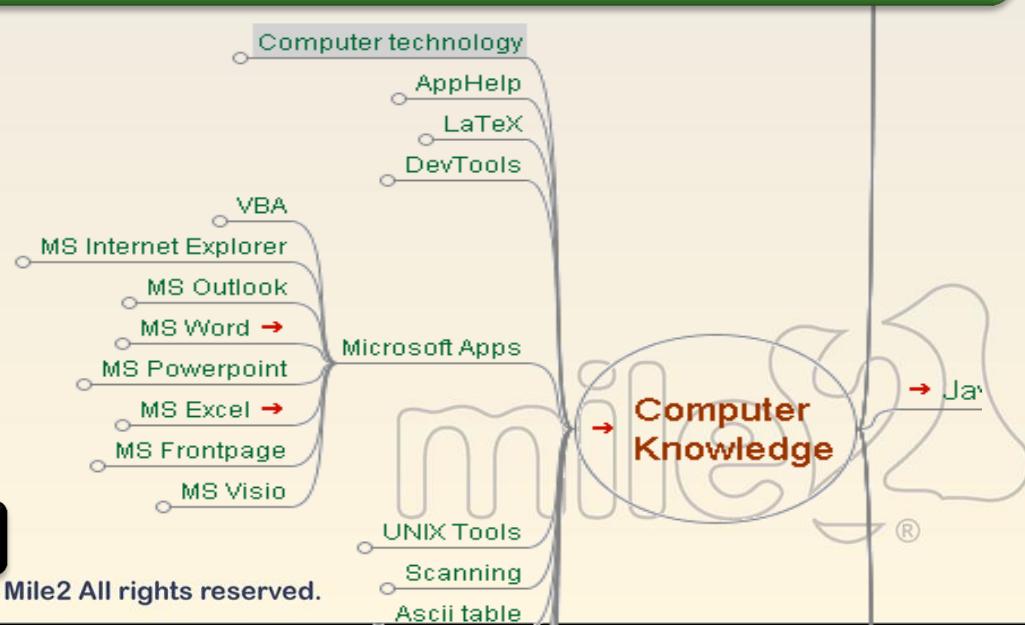
- to brainstorm a new project
- To manage your personal information
- to add multiple outlines and commentary to any text file
- as a tool to facilitate a new kind of literate programming.

Free Mind: Mind mapping

Keeping track of projects, including subtasks, state of subtasks and time recording

Project workplace management, including links to necessary files, executables, source of information and of course information

Organizational framework for internet research using Google and other sources

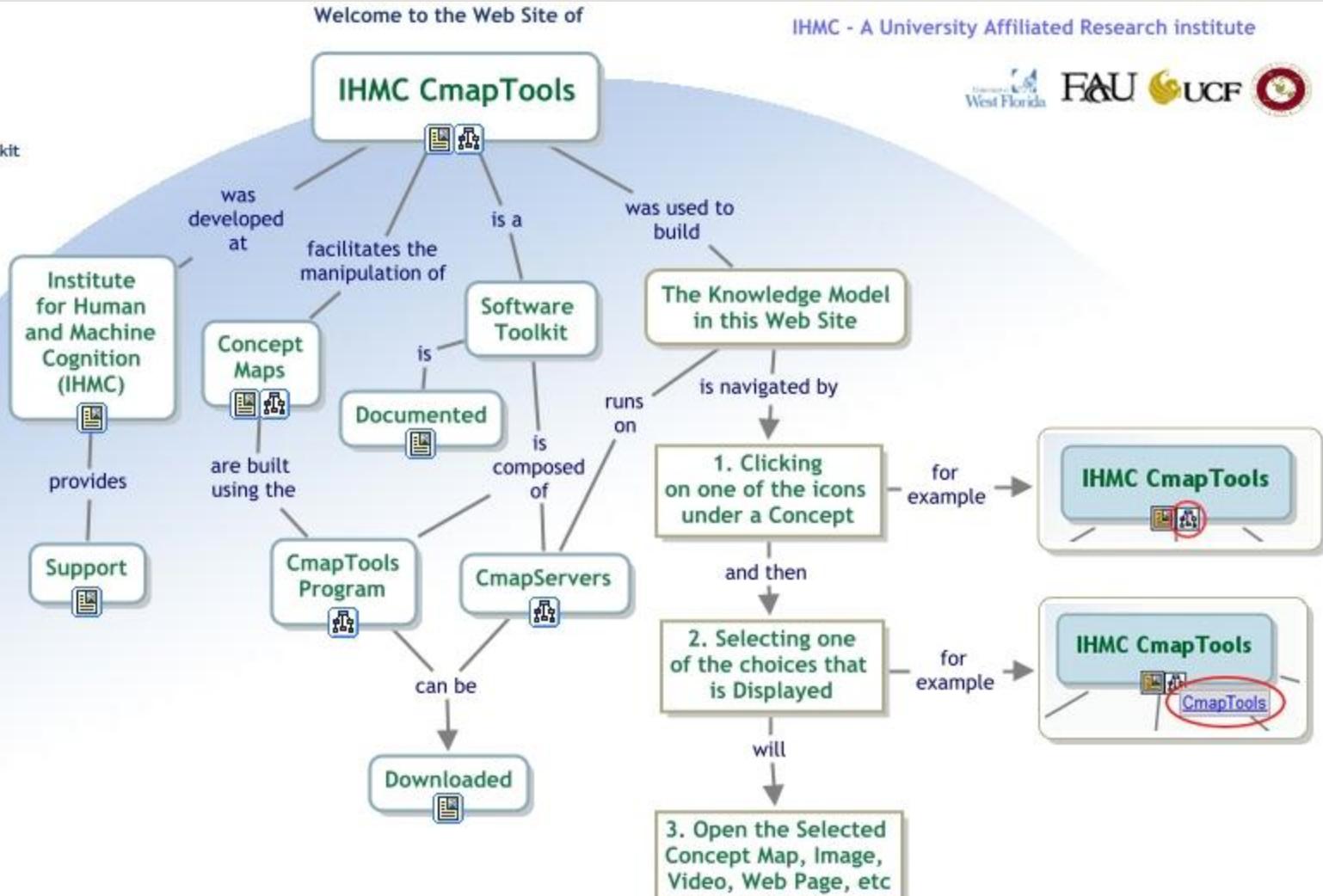


<http://freemind.sourceforge.net/>

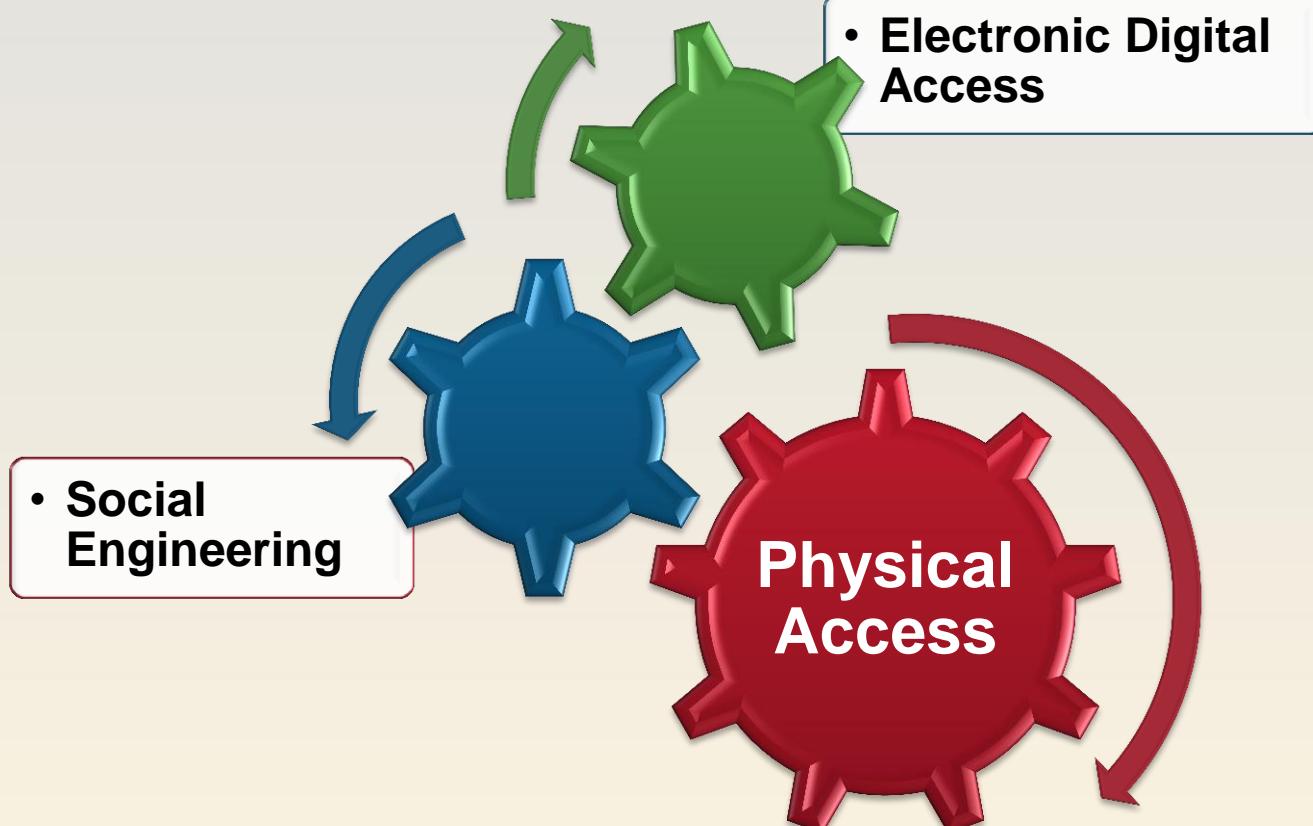
IHMC CmapTools



The IHMC CmapTools software empowers users to construct, navigate, share, and criticize knowledge models represented as Concept Maps



Methods of Obtaining Information



Physical Access

Physical/Human security is key to protecting a company's network.

Physical/Human security are measures that prevent or deter attackers from accessing a physical location.

It can be as simple as a locked file cabinet or as elaborate as a multi-million dollar complex with layers of surveillance.



Hacker's can use a form of social engineering to enter the business premises by fooling human security.

They could pose as a Pest control man, fire inspector, or an employee from another office to gain access to the facility.



Hackers may get sensitive information by dumpster diving, a.k.a. "dumpstering", "binning", "trashing", or "garbing".

Or better known as: Sucking sensitive data from a corporate network from a parking lot- Without a wireless device!



Social Access

Social engineering is the practice of persuading people to believe you are someone you are not to obtain confidential information by manipulation of legitimate users. Social engineers may use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies.

A hacker can obtain information about a target from the internet, news papers, employees, employee family members, consultants, vendors, customers, and security experts



Methods for obtaining information: Shoulder surfing, Way Back machine, Public websites, Yahoo People, Using various tools like, Sam Spade or Neotrace.

Authority

- Attackers pose as victim's boss, boss's secretary, other company personnel.

Strong Emotion

- Get victim into heightened emotional state so they don't pay as much attention to the details/facts.

Overloading

- Provide more information than target can handle so wrong statements go unnoticed, a.k.a.'Double Talk'.

Reciprocation

- *If a stranger does you a favor, then asks you for a favor, don't reciprocate without thinking carefully about what he's asking for. [Kevin Mitnick, The Art of Deception]*

Deceptive Relationships

- Depending on the target, an attacker may build a relationship over years just to exploit it.

Integrity and Consistency

- People will even carry out commitments they believe were made by their fellow employees.

Social Proof

- People usually rely on what other people are doing or saying to a certain degree.

Social Networks



facebook



Hackers use social networks to try and find work or social engineering targets.

If you watch a person's Myspace, Facebook, or Twitter account, you can even figure out when they are away from their home. Possible on vacation....hackers can gain physical entry to the target.

E-mail address or information that should not be available on Myspace

Instant Messengers and Chats

Personal information such as birth date, children, and pet names revealed, that are often used in passwords



Can create behavior profiles of target persons



Is this person typically online at work/at home?



(When is the right time to break in at work/at home or start a social engineering attack as an impersonator?)



“Now online in: Hawaii”



Only allow real “friends” access to your details. Be vague about your whereabouts (same goes for “out of office” replies).

Digital Access

Hackers obtain information from public sources, such as Public websites, DNS servers, search engines, hacker sites, as well as from the targeted systems.

Public sources of information:

- Domain Name Registration
- Domain Name Services
- Search engines
- SEC (Securities and Exchange Commission) Filings
- Way Back Machine

Banner Grabbing a Targeted system can provide information of what services and operating systems they have running, as well as other information.

Passive vs. Active Reconnaissance

Passive Reconnaissance is the process of collecting information about an intended target without direct contact with the target.



Active Reconnaissance is the process of collecting information about an intended target by making contact with the target through Social Engineering or Electronic probing of the target system.



Footprinting defined

The process of gathering data regarding a specific network environment, usually for the purpose of exploiting system vulnerabilities.



Footprinting begins by determining the location and objective of an intrusion.



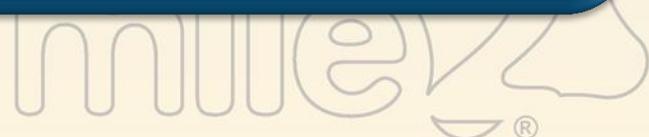
Then finally creating a network diagram and/or a company blueprint for later attack analysis.

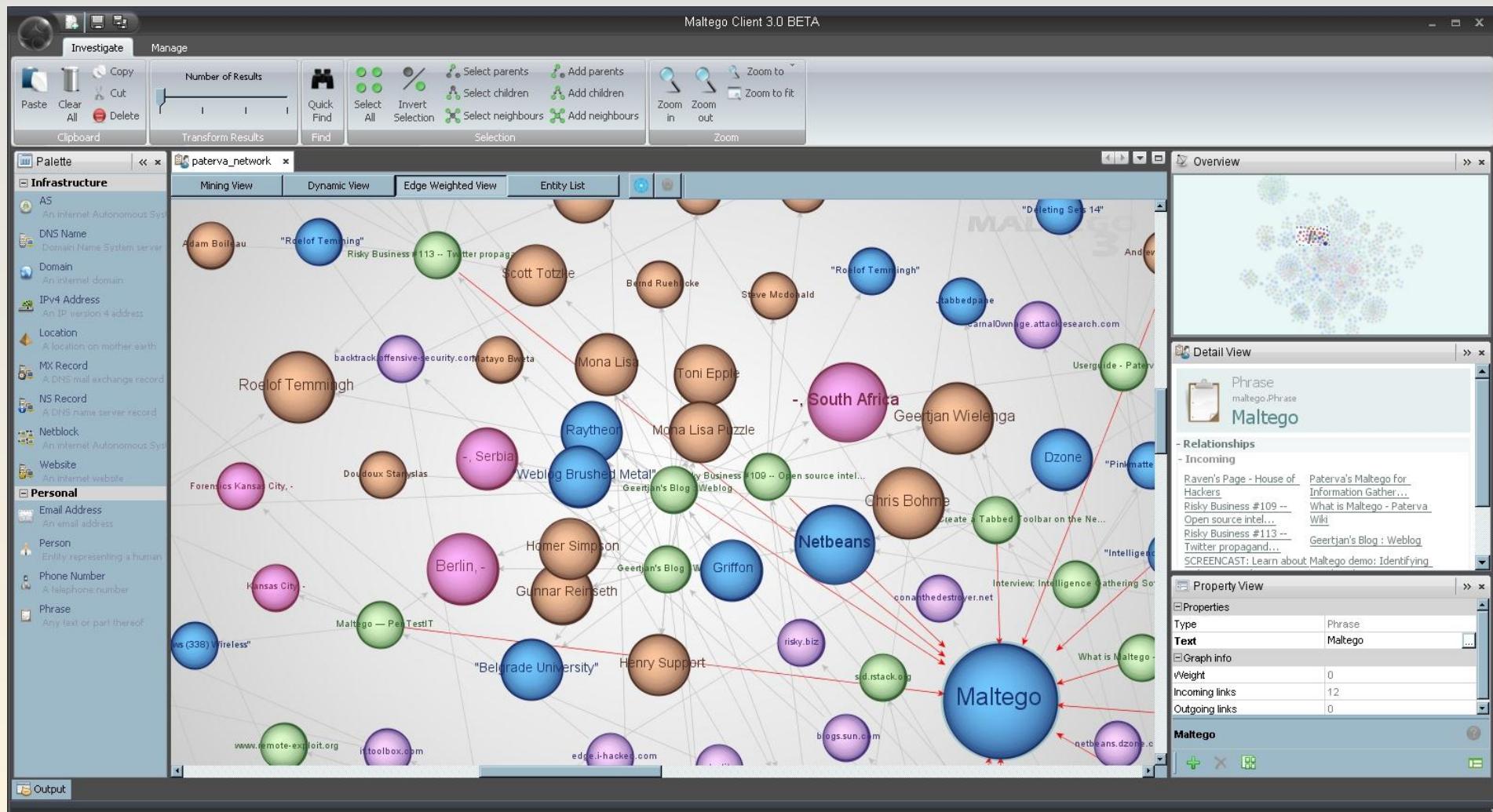
MALTEGO²



Maltego is an open source intelligence and forensics application. It allows for the mining and gathering of information as well as the representation of this information in a meaningful way.

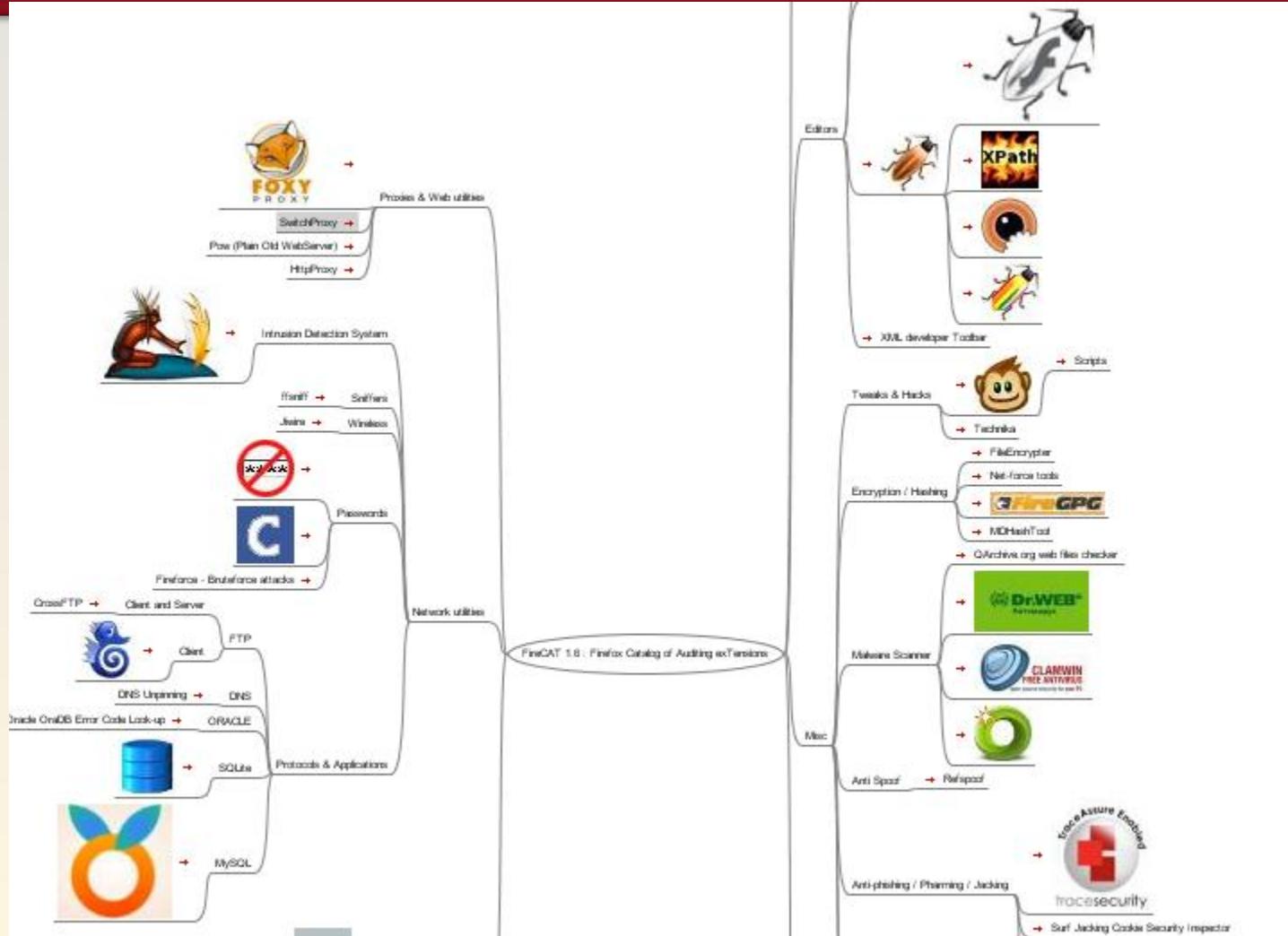
Coupled with its graphing libraries, Maltego, allows you to identify key relationships between information and identify previously unknown relationships between them. It is a must-have tool in the forensics, security and intelligence fields!





FireCAT

FireCAT (Firefox Catalog of Auditing exTension) is a mindmap collection of the most efficient and useful firefox extensions oriented application security auditing and assessment



Footprinting tools



Search Engines such as Google

Newsgroups

Facebook

Myspace

BackTrack Scripts

Information Gathering

DIG

Whois

All-nettools.com

Smartwhois

Allwhois.com

Dnsstuff.com

Samspade.org

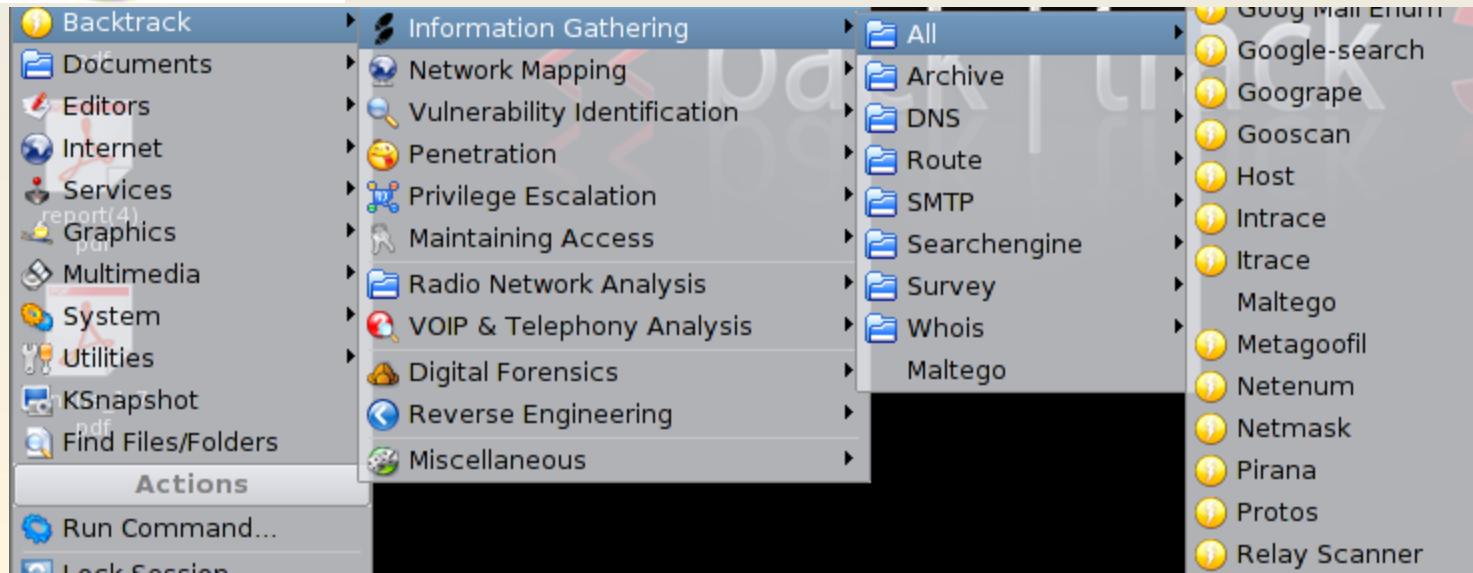
Nslookup

EDGAR

Traceroute

Visual route

Proxy traceroute



Google Hacking

Google dorks are the center of the Google Hacking. Many hackers use google to find vulnerable webpages and later use these vulnerabilities for hacking.

Example: CGI directories contain scripts which can often be exploited by attackers:

Google search ==> “index of cgi-bin”

Welcome to the Google Hacking Database (GHDB)!

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! Stop by our forums to see where the magic happens!

Advisories and Vulnerabilities (215 entries)

These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

Error Messages (68 entries)

Really retarded error messages that say WAY too much!

Files containing juicy info (230 entries)

No usernames or passwords, but interesting stuff none the less.

Files containing passwords (135 entries)

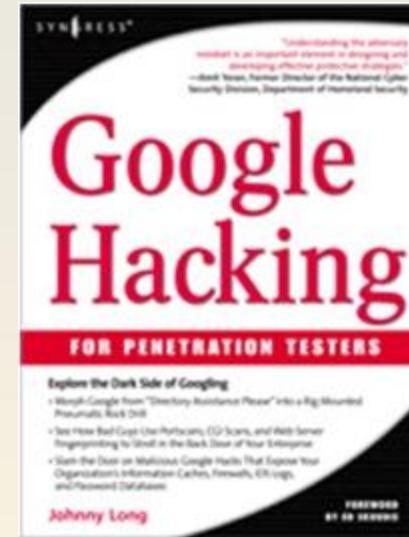
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

Files containing usernames (15 entries)

These files contain usernames, but no passwords... Still, google finding usernames on a web site..

Footholds (21 entries)

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



www.hackersforcharity.org/ghdb/

Google and Query Operators

Google Advanced Search [Advanced](#)

Use the form below and your advanced search will appear here

Find web pages that have...

all these words:

this exact wording or phrase: [tip](#)

one or more of these words: OR OR [tip](#)

But don't show pages that have...

any of these unwanted words: [tip](#)

Need more tools?

Results per page:

Language:

File type:

Search within a site or domain:
(e.g. youtube.com, .edu)

[Date, usage rights, numeric range, and more](#)

Date: (how recent the page is)

Usage rights:

Where your keywords show up:

Region:

Numeric range:

Google contains a wealth of public information, that if given the proper queries, can tell a hacker quite a bit about a target network.



Advanced searches can query on languages, file format, and particular domain names.



You can query the Google cache, for web pages that have links to a particular web page, and for web pages that are related to a particular web page.

Google (cont.)

site: restricts the results to those websites in the given domain.



allintitle: restricts the results to those with all of the query words in the title.



allinurl: restricts the results to those with all of the query words in the url.



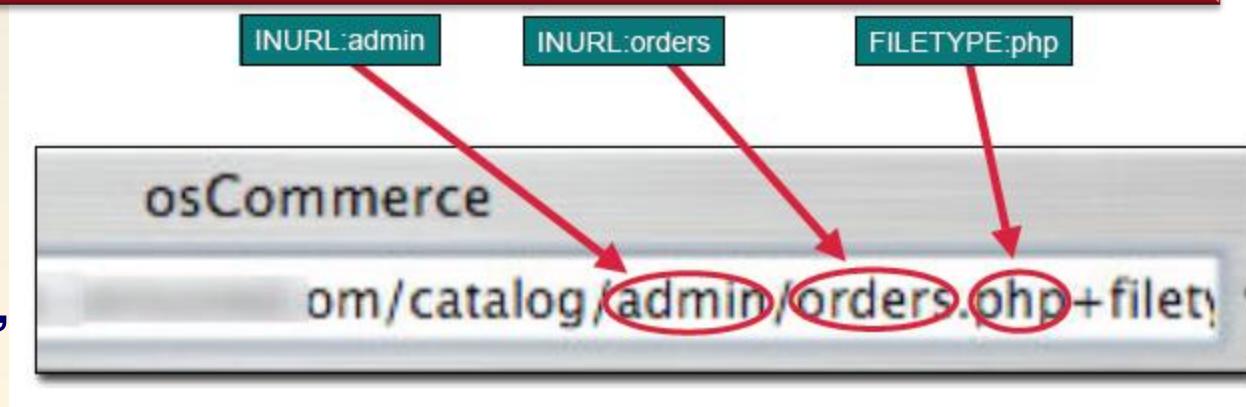
inurl: restrict the results to documents containing that word in the url.



intitle: restrict the results to documents containing that word in the title.



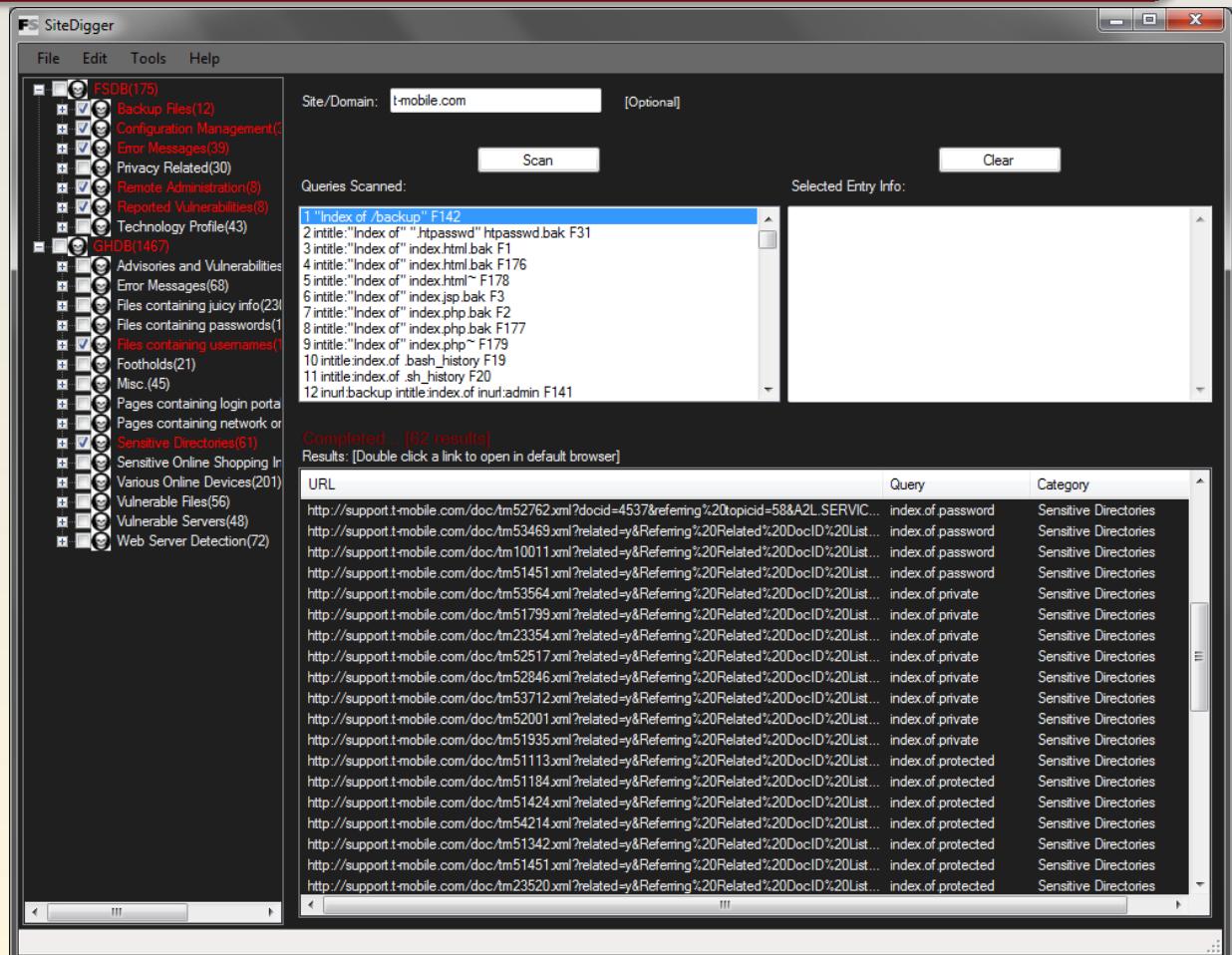
filetype: restricts results to only those containing that filetype.



Ref Book:
**“Google Hacking
for Penetration Testers”**

SiteDigger

SiteDigger searches Google's cache to look for vulnerabilities, errors, configuration issues, proprietary information, and interesting security nuggets on web sites.



No longer requires
Google API License Key.

Job Postings

Visit job posting sites:

- **Monster.com**
- **Careerbuilder.com**
- **Indeed.com**
- **Hotjobs.yahoo.com**
- **Dice.com**
- **Simplyhired.com**
- **Don't forget local/regional and organization/corporation sites**

Job postings often reveal technologies, products, and expertise in use (or desired for use) in a target organization

Blogs & Forums

<http://forum.cisco.com>

[Log In](#) | [Register](#) | [Contacts & Feedback](#) | [Help](#) | [Site Map](#) | [Select a Location / Language](#)



Search

[Products & Services](#) | [Ordering](#) | [Technical Support & Documentation](#) | [Learning & Events](#) | [Partners & Resellers](#) | [About Cisco](#)



HOME

NETWORKING PROFESSIONALS CONNECTION

NETWORK INFRASTRUCTURE

Enterprise Data Center Networking

Getting Started with LANs

LAN, Switching and Routing

Network Management

Remote Access

WAN, Routing and Switching

Meet the NetPros

LAN, Switching and Routing

Topic Points

★  rburts	2043
★  pkhatri	1790
★  glen.grant	1303
★  jon_marshall	1078

Networking Professionals Connection

Network Infrastructure

[Forum Log In](#) | [My NetPro](#) | [Subscriptions](#) | [Top NetPros](#) | [Webcasts](#) | [Ask The Experts](#) | [Reviews](#)

[Forum Topics](#) > [Conversations](#) > [Outline](#) > [Messages](#)

< [Previous Conversation](#) | [Next Conversation](#) >

LAN, Switching and Routing: Cisco 3560G-48PS and 6509

Posted by: urfankhaliq@hotmail.com - Aug 20, 2007, 4:00am PST

Hi all,

I have a couple of questions regarding the above switch and hope I can get some answers with your help...

Firstly the switch (WS-C3560-48PS-E) which is gigabit to the 48 ports, is that also gigabit only through the SFP's or are they 10 G?

Secondly if they ARE 10 G then when they are trunked to a 6509 (WS-X6408A-GBIC module) which I believe is a 1G port (correct me if im wrong), will it bring down the 3560 to 1G or will it not work?

As some background info the idea is to upgrade our network which consists of 6509 core with the WS-x6408A-GBIC fibre module which is connected to the edge switches (mixture of various 3500's). We would like to upgrade all edge switches to 3560G-48PS to enable gigabit to desktops but was just unsure of its compatibility with the current fibre module in the 6509 core.

Thanks in advance!

Many engineers publish detailed infrastructure and network device information, such as IP address's, firewall rules and even access passwords.

USENET and/or Google Groups can reveal inadvertently posted data/information that is publically viewable

groups.google.com

“cisco password 7”

Google groups

[Explore groups](#)

[What is Google Groups?](#)

[Take the tour »](#)

Find out what people are doing with Google Groups

[Search for a group](#)

 [Arts & Entertainment Groups](#)

 [Business Groups](#)

 [Computer Groups](#)

 [Health Groups](#)

 [Home Groups](#)

 [News Groups](#)

 [People Groups](#)

 [Recreation Groups](#)

 [School & University Groups](#)

 [Sci/Tech Groups](#)

 [Society & Humanities Groups](#)

[Browse group categories...](#)



Internet Archive: The WayBack Machine

<http://www.archive.org/>



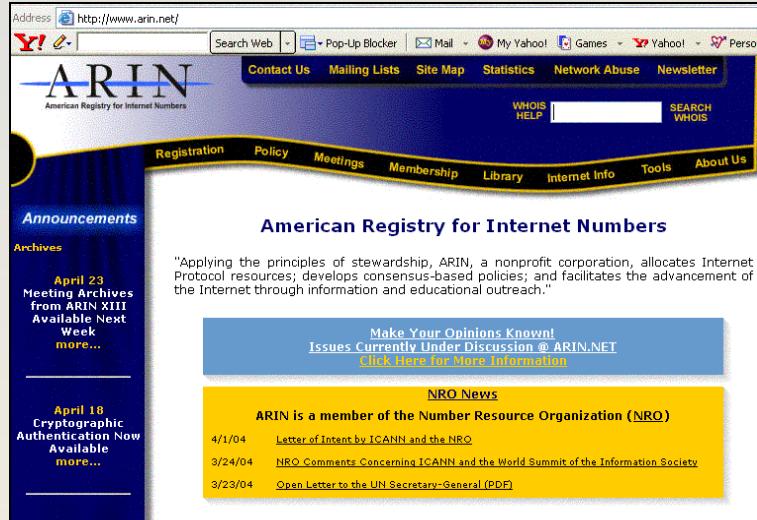
Browse through 150 billion web pages
archived from 1996 to a few months ago.



Point a Web site ripper/duplication tool to the results page to
create a local copy of all historical cached site versions.



Domain Name Registration



ARIN's database contains information on networks, autonomous system numbers (ASNs), network-related handles, and Points of Contact (POCs).

Do not search on domain names at a RIR, instead search on other information, such as an IP address or organization name.

Regional Internet Registries

Allow searching the world-wide IANA database

- **AfriNIC - Africa, portions of the Indian Ocean**
- **APNIC - Portions of Asia, portions of Oceania**
- **ARIN - Canada, many Caribbean and North Atlantic islands, and the United States**
- **LACNIC - Latin America, portions of the Caribbean**
- **RIPE NCC - Europe, the Middle East, Central Asia**

INTERNIC is the repository for Name Registrations:
<http://www.internic.net/alpha.html>

WHOIS

WHOIS is a great way of querying the Domain Name Registration database to find out who registered a particular domain name. Other information is listed there as well.

WHOIS information is public information, so anyone can retrieve it....at anytime.

Here's a few sites that do WHOIS queries:

- RIR sites
- www.centralops.net
- www.allwhois.com
- www.dnsstuff.com
- www.dnstools.com
- www.serversniff.net
- www.internic.net
- www.all-nettools.com
- www.dirk-loss.de/onlinetools



WHOIS Output

CustName: ██████████.com
 Address: 117 Kendrick Street Ste 800
 City: Needham
 StateProv: MA
 PostalCode: 02494
 Country: US
 RegDate: 2001-12-29
 Updated: 2003-05-30

NetRange: 65.214.43.0 - 65.214.43.255
 CIDR: 65.214.43.0/24

NetName: UU-65-214-43
 NetHandle: NET-65-214-43-0-1
 Parent: NET-65-192-0-0-1
 NetType: Reassigned

Comment:
 RegDate: 2001-12-29
 Updated: 2003-05-30

RTechHandle: OA12-ARIN
 RTechName: UUnet Technologies, Inc., Technologies
 RTechPhone: +1-800-900-0241
 RTechEmail: help4u@mci.com

OrgAbuseHandle: ABUSE3-ARIN
 OrgAbuseName: abuse
 OrgAbusePhone: +1-800-900-0241
 OrgAbuseEmail: abuse-mail@mci.com

OrgNOCHandle: OA12-ARIN
 OrgNOCName: UUnet Technologies, Inc., Technologies
 OrgNOCPhone: +1-800-900-0241
 OrgNOCEmail: help4u@mci.com

OrgTechHandle: SWIPP-ARIN
 OrgTechName: swipper
 OrgTechPhone: +1-800-900-0241
 OrgTechEmail: swipper@mci.com

ARIN WHOIS database, last updated 2006-05-23 19:10

Domain Dossier Investigate domains and IP addresses

domain or IP address

- domain whois record DNS records traceroute
 network whois record service scan

user: 68.15.227.17 [anonymous] 49/50
[log in](#) | [get account](#)

CentralOps.net

Address: <http://www.internic.net/whois.html>
[Google](#) Search Web AutoFill Options

InterNIC Home Registrars FAQ Whois

Whois Search

Whois (.aero, .arpa, .biz, .com, .coop, .edu, .info, .int, .museum, .net, and .org):

Domain (ex. internic.net)
 Registrar (ex. ABC Registrar, Inc.)
 Nameserver (ex. NS.EXAMPLE.COM or 192.16.0.192)

 For Whois information about **country-code (two-letter) top-level domains**, try [Uwhois.com](#)

 Results for .com and .net are provided courtesy of VeriSign Global Registry Services. For these top-level domains, the results of a successful search will contain only technical information about the registered domain name and referral information for the registrar of the domain name. In the Shared Registration System model, registrars are responsible for maintaining Whois domain name contact information. Please refer to the registrar's Whois service for additional information.

This page last updated 10/22/2001

DNS Databases

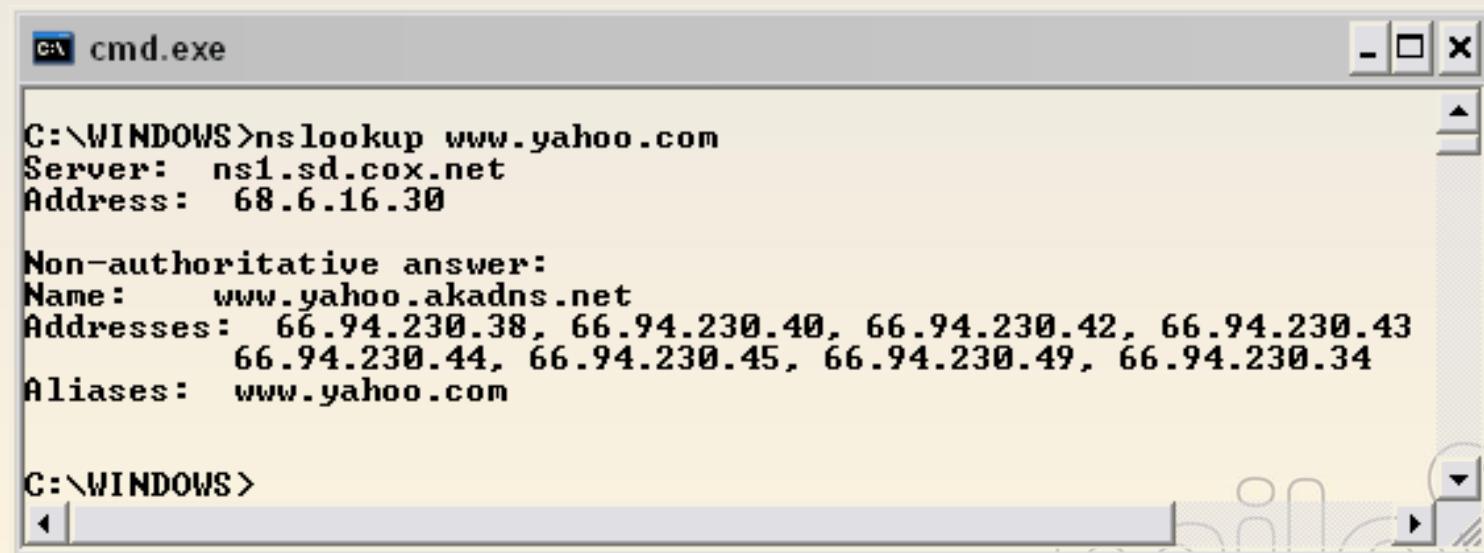
DNS databases contain information about FQDNs and IP addresses. They also contain information such as which servers are the Mail servers and Active Directory servers.

Record Name	Record Type	Purpose
Host	A	Maps a domain name to an IP address
Pointer	PTR	Maps an IP address to a domain name
Name Server	NS	Identifies a server name for a delegated zone
Start of Authority	SOA	Configures settings for zone transfers and record caching
Service Locator	SRV	Used to locate services (servers) in the network
Mail	MX	Identifies SMTP servers

Using Nslookup

Nslookup is used to query domain name servers. The output information can be used to diagnose DNS issues. However, hackers can use Nslookup's output to determine what servers to target.

Both Unix and Windows come with an Nslookup client and it is built into many tools.

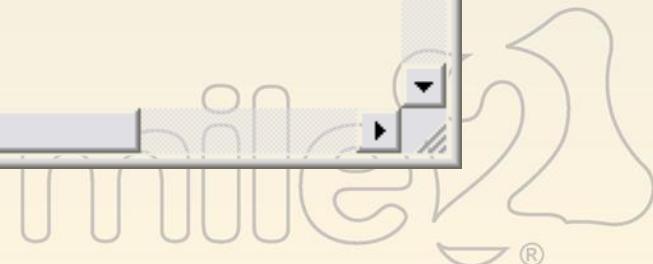


A screenshot of a Windows command prompt window titled "cmd.exe". The window shows the output of the "nslookup www.yahoo.com" command. The output includes the server address (ns1.sd.cox.net), the address of the website (68.6.16.30), and a non-authoritative answer section providing multiple IP addresses for the website: 66.94.230.38, 66.94.230.40, 66.94.230.42, 66.94.230.43, 66.94.230.44, 66.94.230.45, 66.94.230.49, and 66.94.230.34. It also lists the aliases for the website as "www.yahoo.com".

```
C:\WINDOWS>nslookup www.yahoo.com
Server: ns1.sd.cox.net
Address: 68.6.16.30

Non-authoritative answer:
Name: www.yahoo.akadns.net
Addresses: 66.94.230.38, 66.94.230.40, 66.94.230.42, 66.94.230.43
          66.94.230.44, 66.94.230.45, 66.94.230.49, 66.94.230.34
Aliases: www.yahoo.com

C:\WINDOWS>
```



Dig for Unix / Linux

Dig is a Unix utility that performs DNS queries, similar to Nslookup. The syntax of dig is:

dig <FQDN> <record type>

```
root@slax:~# dig yahoo.com mx

; <>> DiG 9.3.1 <>> yahoo.com mx
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47329
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 5, ADDITIONAL: 19

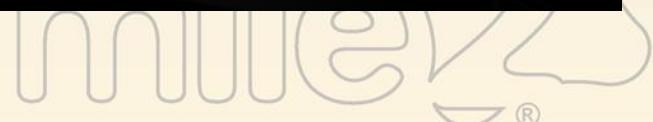
;; QUESTION SECTION:
;yahoo.com.           IN      MX

;; ANSWER SECTION:
yahoo.com.        4840    IN      MX      1 mx2.mail.yahoo.com.
yahoo.com.        4840    IN      MX      1 mx3.mail.yahoo.com.
yahoo.com.        4840    IN      MX      5 mx4.mail.yahoo.com.
yahoo.com.        4840    IN      MX      1 mx1.mail.yahoo.com.

;; AUTHORITY SECTION:
yahoo.com.       141582  IN      NS      ns1.yahoo.com.
yahoo.com.       141582  IN      NS      ns2.yahoo.com.
yahoo.com.       141582  IN      NS      ns3.yahoo.com.
yahoo.com.       141582  IN      NS      ns4.yahoo.com.
yahoo.com.       141582  IN      NS      ns5.yahoo.com.
```

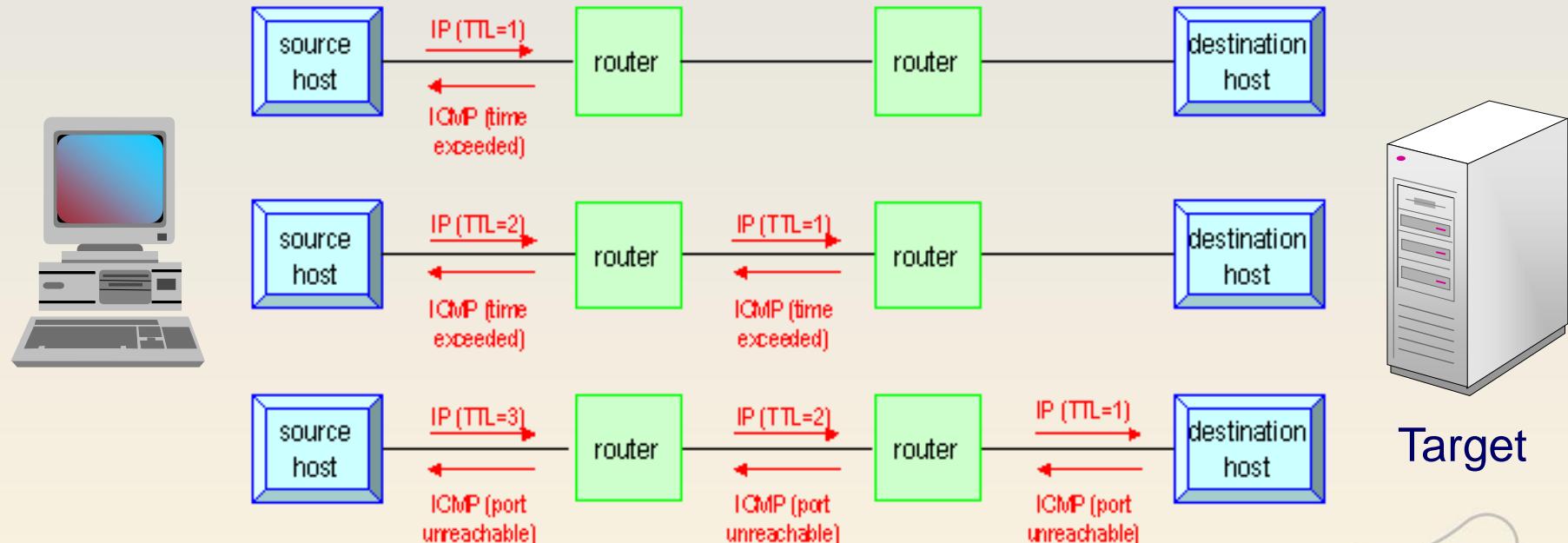


<<back|track.
network security suite.



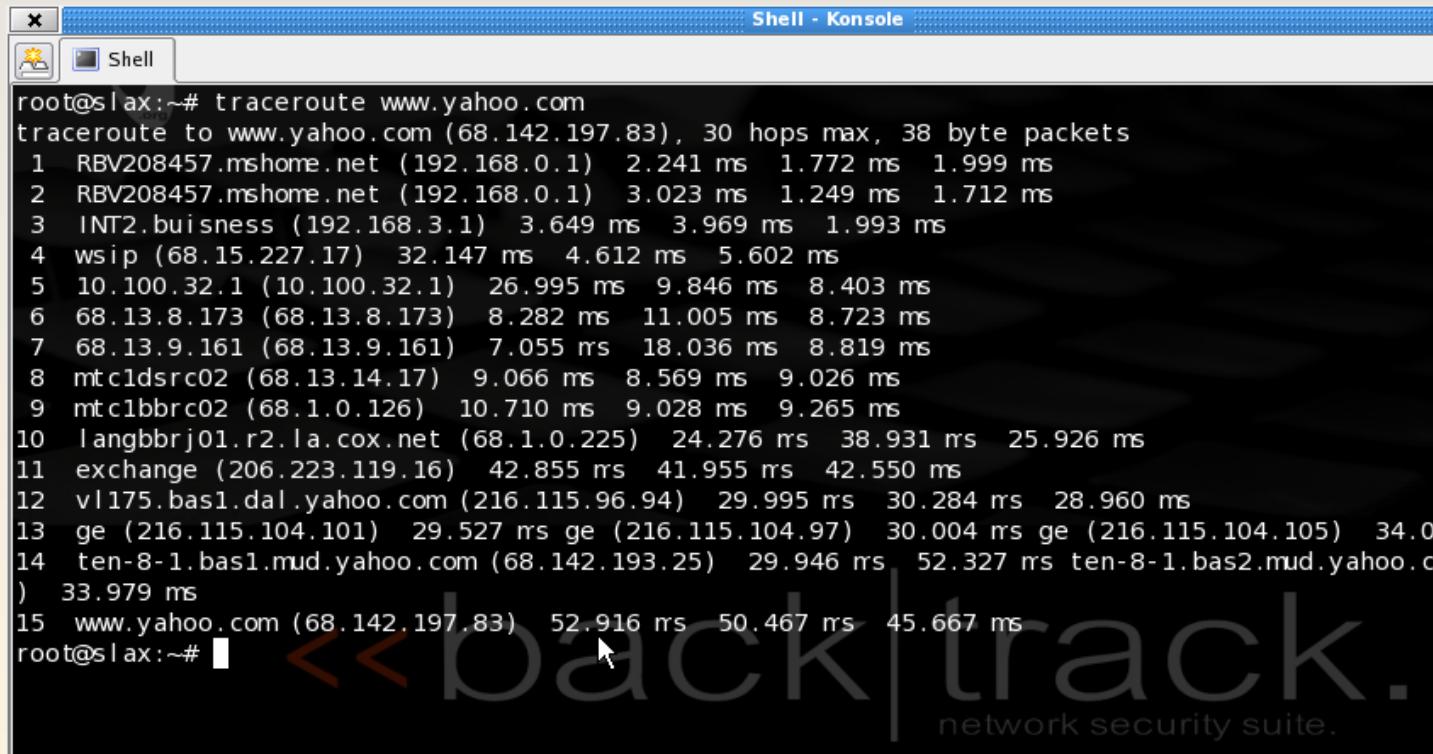
Traceroute Operation

Traceroute is used to determine the path taken from the attackers to a target network by exploiting the 'TTL' (Time To Live) to get to the target machine.



Traceroute (cont.)

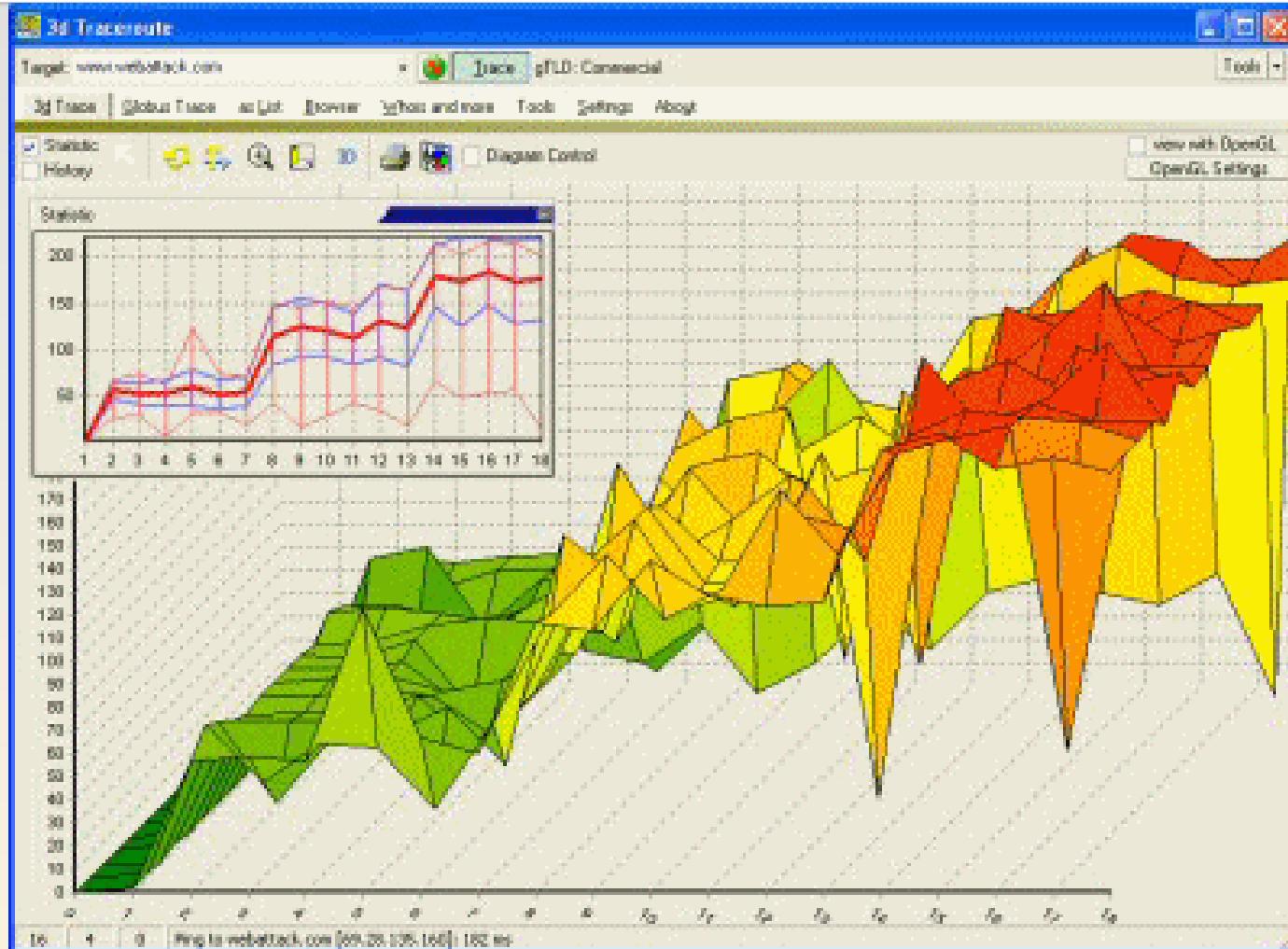
In this example, the Linux traceroute command is used to determine the path taken to get to a Yahoo web server. It shows the number of hops, the response time for each router along the path, and the names of each router.



```
Shell - Konsole
root@slax:~# traceroute www.yahoo.com
traceroute to www.yahoo.com (68.142.197.83), 30 hops max, 38 byte packets
 1 RBV208457.mshome.net (192.168.0.1)  2.241 ms  1.772 ms  1.999 ms
 2 RBV208457.mshome.net (192.168.0.1)  3.023 ms  1.249 ms  1.712 ms
 3 INT2.business (192.168.3.1)  3.649 ms  3.969 ms  1.993 ms
 4 wsip (68.15.227.17)  32.147 ms  4.612 ms  5.602 ms
 5 10.100.32.1 (10.100.32.1)  26.995 ms  9.846 ms  8.403 ms
 6 68.13.8.173 (68.13.8.173)  8.282 ms  11.005 ms  8.723 ms
 7 68.13.9.161 (68.13.9.161)  7.055 ms  18.036 ms  8.819 ms
 8 mtc1dsr02 (68.13.14.17)  9.066 ms  8.569 ms  9.026 ms
 9 mtc1bbrc02 (68.1.0.126)  10.710 ms  9.028 ms  9.265 ms
10 langbbrj01.r2.la.cox.net (68.1.0.225)  24.276 ms  38.931 ms  25.926 ms
11 exchange (206.223.119.16)  42.855 ms  41.955 ms  42.550 ms
12 v1175.bas1.dal.yahoo.com (216.115.96.94)  29.995 ms  30.284 ms  28.960 ms
13 ge (216.115.104.101)  29.527 ms ge (216.115.104.97)  30.004 ms ge (216.115.104.105)  34.05
14 ten-8-1.bas1.mud.yahoo.com (68.142.193.25)  29.946 ms  52.327 ms ten-8-1.bas2.mud.yahoo.co
) 33.979 ms
15 www.yahoo.com (68.142.197.83)  52.916 ms  50.467 ms  45.667 ms
root@slax:~#
```



3D Traceroute



<http://www.d3tr.de/>

Opus online traceroute

The Opus online traceroute can be found at
<http://www.opus1.com/www/traceroute.html>



Internet Services

TECH SUPPORT

Opus One Traceroute Tool

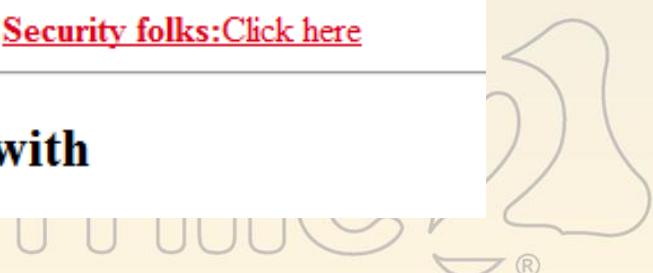
Enter the name or IP address of the site to trace to:

or

[Spam Fighters: Click here](#)

[Security folks: Click here](#)

Fun things to fiddle with



People Search Engines

<http://pipl.com/>

- The most comprehensive people search engine on the web.

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

- Company info and people search; over 40m people and almost 4m companies

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

- Free People Search and Public Information Search Engine - Premium Services: Search by Phone Number Search by SS# Run a Background Check

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

- “The world's most accurate people search.” Search by name, email, location or tag

<http://wink.com/>

- Wink People Search provides free people search across over 400 Million online profiles - including Facebook, MySpace, LinkedIn, and all the other big social networks. You can search for people by name, location, work, school or interests.

Lists of more specialized people search engines:

- http://www.search-engine-index.co.uk/People_Search/

Intelius info and Background Check Tool



<http://www.intelius.com>

[Sign In – My Intelius](#)

[View My Reports](#)

Verification Services

- ▶ [Background Check](#)
- ▶ [Reverse Phone Lookup](#)
- ▶ [Property & Neighborhood](#)

Information Services

- ▶ [People Search](#)
- ▶ [Email Search](#)
- ▶ [Social Net Search](#)

Protection Services

- ▶ [Reverse Cell Phone Directory](#)
- ▶ [Identity Protect](#)
- ▶ [Criminal & Sex Offender](#)

Business Services

- ▶ [Employee Screening](#)
- ▶ [Tenant Screening](#)
- ▶ [All Products & Services](#)

People Search

[Name](#) [Address](#) [Email](#) [Social Security #](#) [Social Net Search](#)

First Name	MI	Last Name
<input type="text"/>	<input type="text"/>	<input type="text"/>
State		
All States	<input type="button" value="Search"/>	Advanced Search

[View Sample Report](#)

What is a People Search?

People Search is great way to find and reconnect with family, old friends, relatives — just about anyone! People Search reports include phone numbers, address history, ages, birthdates, household members, home value, income and more.

Reverse Phone Lookup

[Phone](#)

Phone Number: (ex. 555-555-5555)

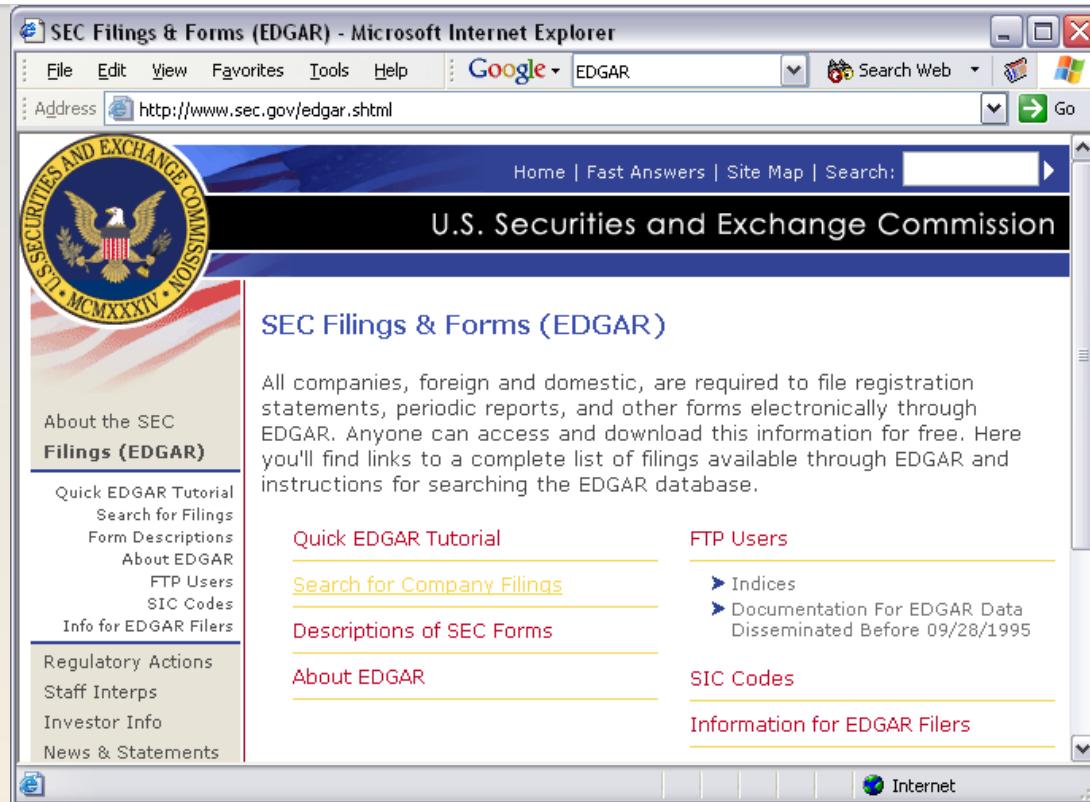
[Search](#)

[View Sample Report](#)

What is a Reverse Phone Lookup?

Know who is calling you or your family! The report includes name, phone owner details, and more for any cell phone, unlisted, non-published, or other phone numbers.

EDGAR For USA Company Info

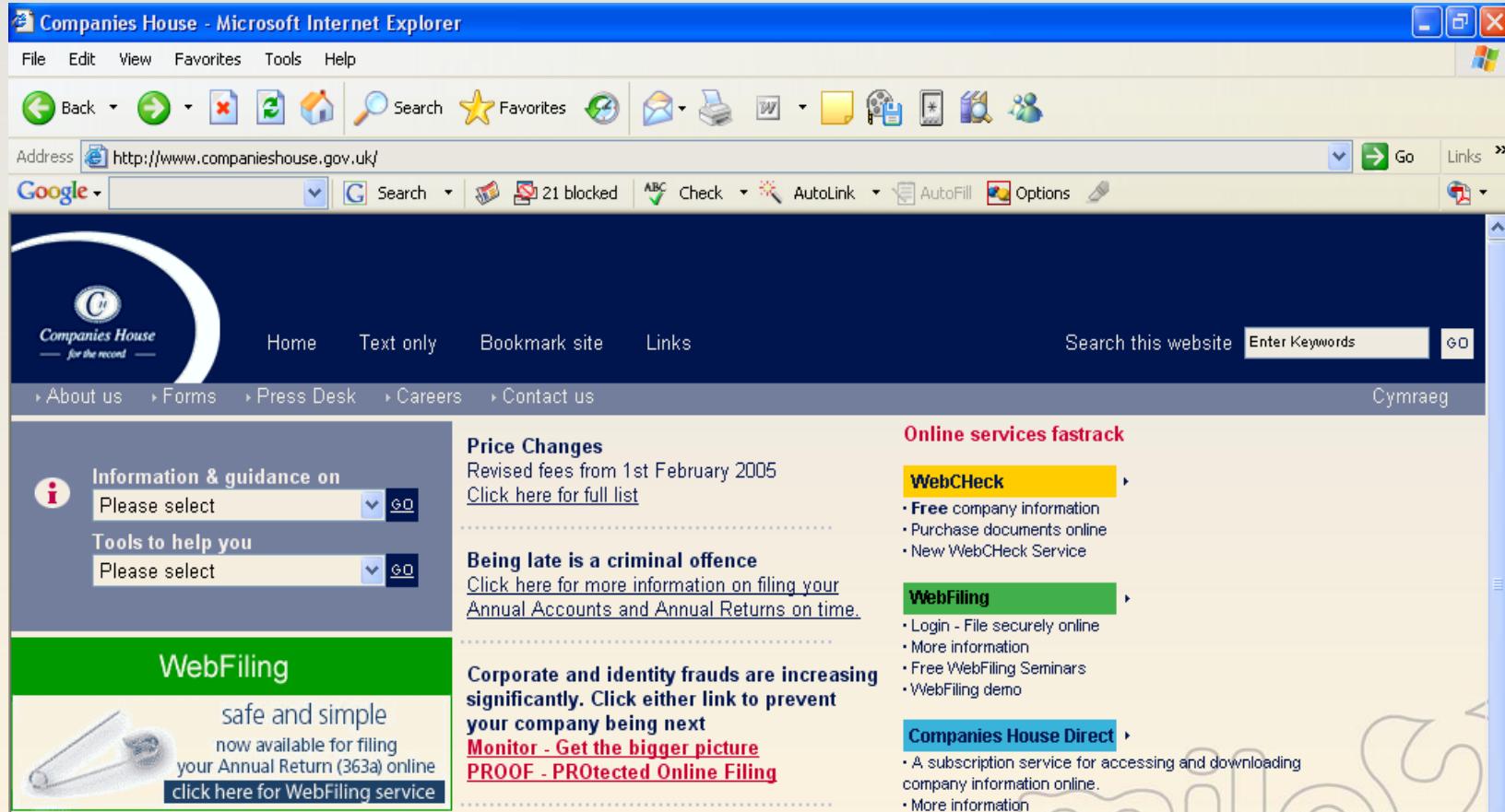


The screenshot shows the SEC Filings & Forms (EDGAR) page in Microsoft Internet Explorer. The title bar reads "SEC Filings & Forms (EDGAR) - Microsoft Internet Explorer". The address bar shows "http://www.sec.gov/edgar.shtml". The main content area features the U.S. Securities and Exchange Commission logo and the text "U.S. Securities and Exchange Commission". On the left, there's a sidebar with links like "About the SEC", "Filings (EDGAR)", "Quick EDGAR Tutorial", "Search for Filings", "Form Descriptions", "About EDGAR", "FTP Users", "SIC Codes", "Info for EDGAR Filers", "Regulatory Actions", "Staff Interps", "Investor Info", and "News & Statements". The main content area has sections for "SEC Filings & Forms (EDGAR)", "Quick EDGAR Tutorial", "FTP Users", "Search for Company Filings", "Descriptions of SEC Forms", "About EDGAR", "SIC Codes", and "Information for EDGAR Filers".

EDGAR, the Electronic Data Gathering, Analysis and Retrieval system, collects, validates and archives submissions made by companies to the U.S. Securities and Exchange Commission (SEC).



<http://www.companieshouse.gov.uk/>



The screenshot shows a Microsoft Internet Explorer window displaying the official website of the UK Companies House. The address bar at the top contains the URL <http://www.companieshouse.gov.uk/>. The page itself has a dark blue header with the 'Companies House' logo and navigation links for Home, Text only, Bookmark site, Links, and a search bar. Below the header, there's a menu with links to About us, Forms, Press Desk, Careers, and Contact us. A sidebar on the left features sections for 'Information & guidance on' (with dropdown menus for 'Please select') and 'Tools to help you' (also with dropdown menus). A green 'WebFiling' section highlights the service as 'safe and simple' and 'now available for filing your Annual Return (363a) online'. The main content area includes sections for 'Price Changes', 'Being late is a criminal offence', 'Corporate and identity frauds are increasing significantly', and 'Online services fasttrack' which lists WebCheck, WebFiling, and Companies House Direct services.



Client Email Reputation

WatchGuard ReputationAuthority

IP / Domain Lookup Top Threats Tips & Resources ▾ Log In/Register ▾ About Reputation

hsbc.com

Total IPs: 152 ⓘ
SPF record: Present ⓘ
[Learn more about Domain Reputation](#)

Reputation: █ Good █ Suspect █ Bad

Reputation Range: All

Showing page 1 of 7 [»](#) [»»](#) [Printable Version](#) : 

IP Address Information ⓘ				Domain/IP ⓘ			Overall IP ⓘ		
IP Address	ISP	ISP Domain	Ctry	Rep.	Good	Bad	Rep.	Good	Bad
193.108.75.62	HSBC BANK PLC U	-	UK	<div style="width: 89%;">█</div>	89%	11%	<div style="width: 99%;">█</div>	99%	1%
203.112.90.35	HSBC BANKING AN	HSBC.COM.H	HK	<div style="width: 88%;">█</div>	88%	12%	<div style="width: 97%;">█</div>	97%	3%
203.112.84.13	HSBC BANKING AN	HSBC.COM.H	HK	<div style="width: 88%;">█</div>	88%	12%	<div style="width: 97%;">█</div>	97%	3%
204.178.86.20	MCI COMMUNICATI	ALTER.NET	US	<div style="width: 96%;">█</div>	96%	4%	<div style="width: 99%;">█</div>	99%	1%
205.214.176.20	HSBC BANK USA	-	US	<div style="width: 95%;">█</div>	95%	5%	<div style="width: 99%;">█</div>	99%	1%
193.108.75.63	HSBC BANK PLC U	-	UK	<div style="width: 64%;">█</div>	64%	36%	<div style="width: 99%;">█</div>	99%	1%

<http://www.reputationauthority.org/>

Web Server Info Tool: Netcraft

80%

40%

0%



- Apache
- Microsoft
- Sun
- nginx
- Google
- NCSA
- lighttpd
- Other



Netcraft.com may be queried for an organization's web server software and underlying operating system.

Also may contain uptime information – useful for the hacker who wants to know if a system has been patched!

Footprinting Countermeasures

Sanitize DNS registration and contact information. Be as generic as possible (e.g. “IT Director”, main company phone number 555-5000, techsupport@acme.com)

Have two DNS servers, one internal, one external in the DMZ. The external DNS should contain only resource records of the DMZ hosts (not internal hosts). For additional safety, do not allow zone transfers to any IP address.

Regularly scan search engines to see if links to your private services are available (Terminal Server, OWA, VPN, etc.)

Consider carefully crafted job postings and calls for bids to reveal less about the IT infrastructure.

Be aware of the possible leakage of information due to disgruntled employees during layoffs/mergers.

Address <http://www.domainsbypoxy.com/popup/whoisexample.aspx?se=%2B&app%5Fhdr=0&ci=5165>

Google Search ABC Check Look for Map AutoFill Options

ICANN, the international governing body for domain names, requires every Registrar to maintain a publicly accessible "WHOIS" database displaying all contact information for all domain names registered.

Example: John Smith lives at 1234 Elm Street, Hometown AZ 85000. His home phone is 480-555-5555. He buys "ProxiedDomain.com".

- With a public registration, John's personal information is available for anyone to see.
- With a private registration, John's personal information is shielded from public display, and a private email address allows John to control who reaches him.

Public

Registration WHOIS Listing

Registrant:

John Smith
1234 Elm Street
Hometown, AZ 85000
Registered through: Domains Priced Right
Domain Name: ProxiedDomain.com
Created on: 15-Oct-02
Expires on: 15-Oct-03
Last Updated on: 17-Oct-02

Administrative Contact:

John Smith
john@ProxiedDomain.com
1234 Elm Street
Hometown, AZ 85000
(480) 555-5555

Technical Contact:

John Smith
john@ProxiedDomain.com
1234 Elm Street
Hometown, AZ 85000
(480) 555-5555

Private

Registration WHOIS Listing

Registrant:

Domains By Proxy, Inc.
DomainsByProxy.com
15111 N. Hayden Road Suite 160/PMB 353
Scottsdale, AZ 85260
Registered through: Domains Priced Right
Domain Name: ProxiedDomain.com
Created on: 15-Oct-02
Expires on: 15-Oct-03
Last Updated on: 17-Oct-02

Administrative Contact:

Domains By Proxy, Inc.
ProxiedDomain.com@DomainsByProxy.com
DomainsByProxy.com
15111 N. Hayden Road Suite 160/PMB 353
Scottsdale, AZ 85260
(480) 624-2599

Technical Contact:

Domains By Proxy, Inc.
ProxiedDomain.com@DomainsByProxy.com
DomainsByProxy.com
15111 N. Hayden Road Suite 160/PMB 353
Scottsdale, AZ 85260
(480) 624-2599

Close



Review

What Information is gathered by the Hacker?



What is Passive vs. Active Reconnaissance



Methods of obtaining Information



Google and Query Operators



Footprinting Defined



Tools used to Footprint



Footprinting Countermeasures

Module 3 Lab Information Gathering Passive Recon

