Information Gathering

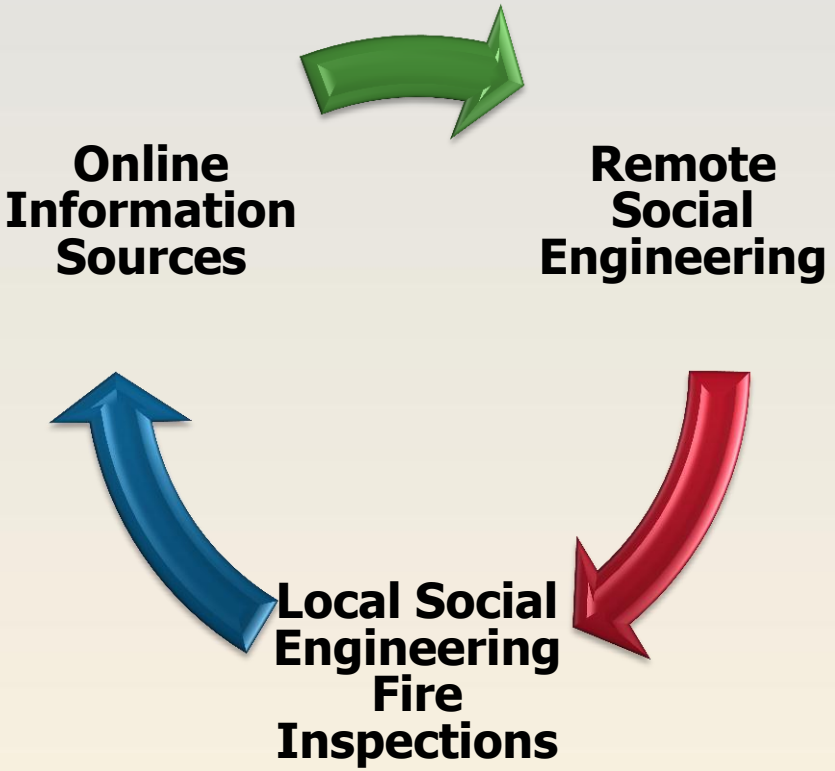
Step 1: Reconnaissance

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?



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:

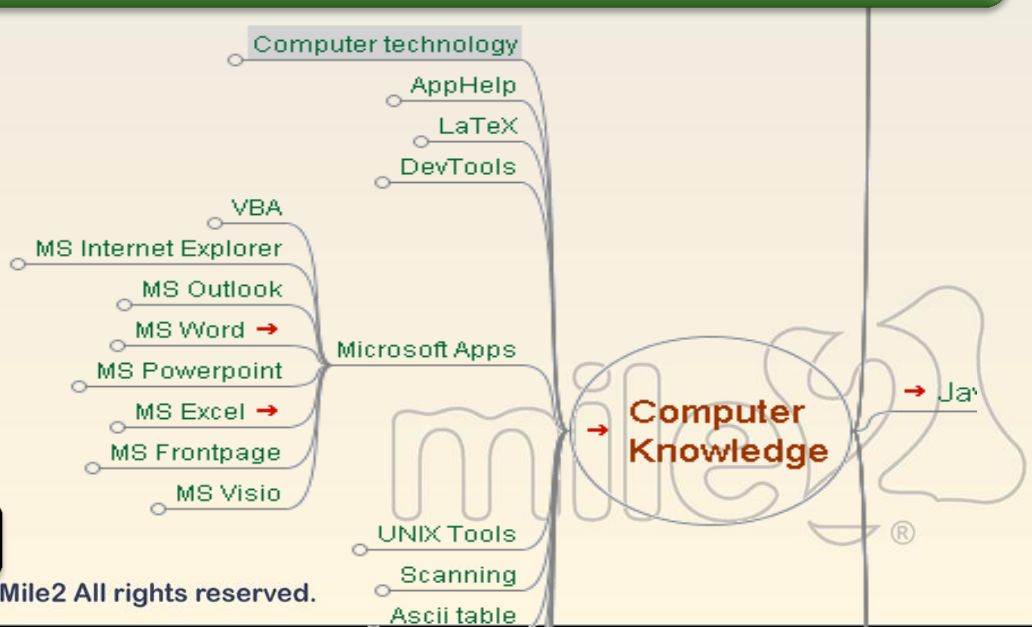
- to brainstorm a new project
- To manage your personal information
- to add multiple outlines and commentary to any text file
- as a tool to facilitate a new kind of literate programming.

Free Mind: Mind mapping

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

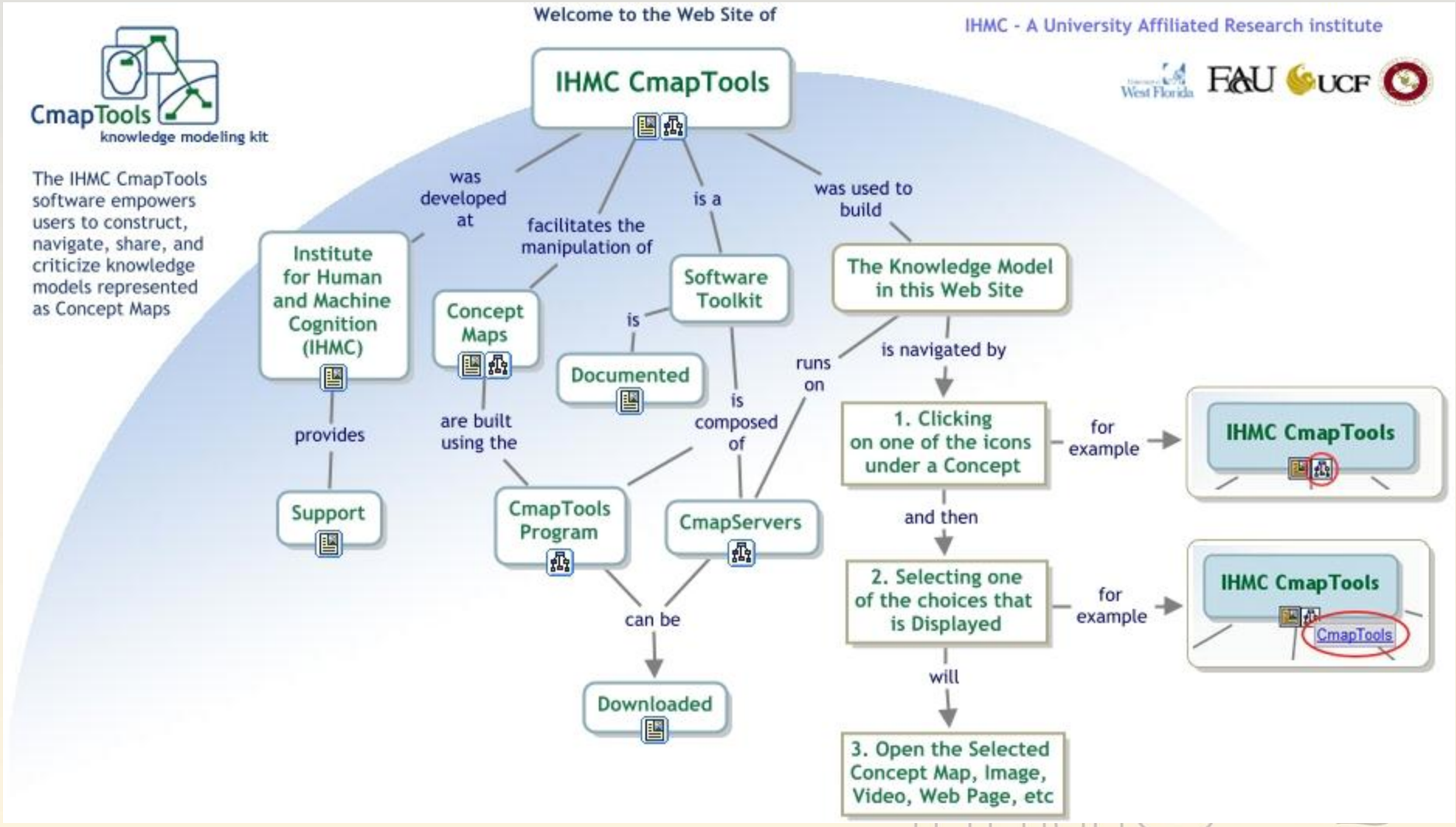
Project workplace management, including links to necessary files, executables, source of information and of course information

Organizational framework for internet research using Google and other sources

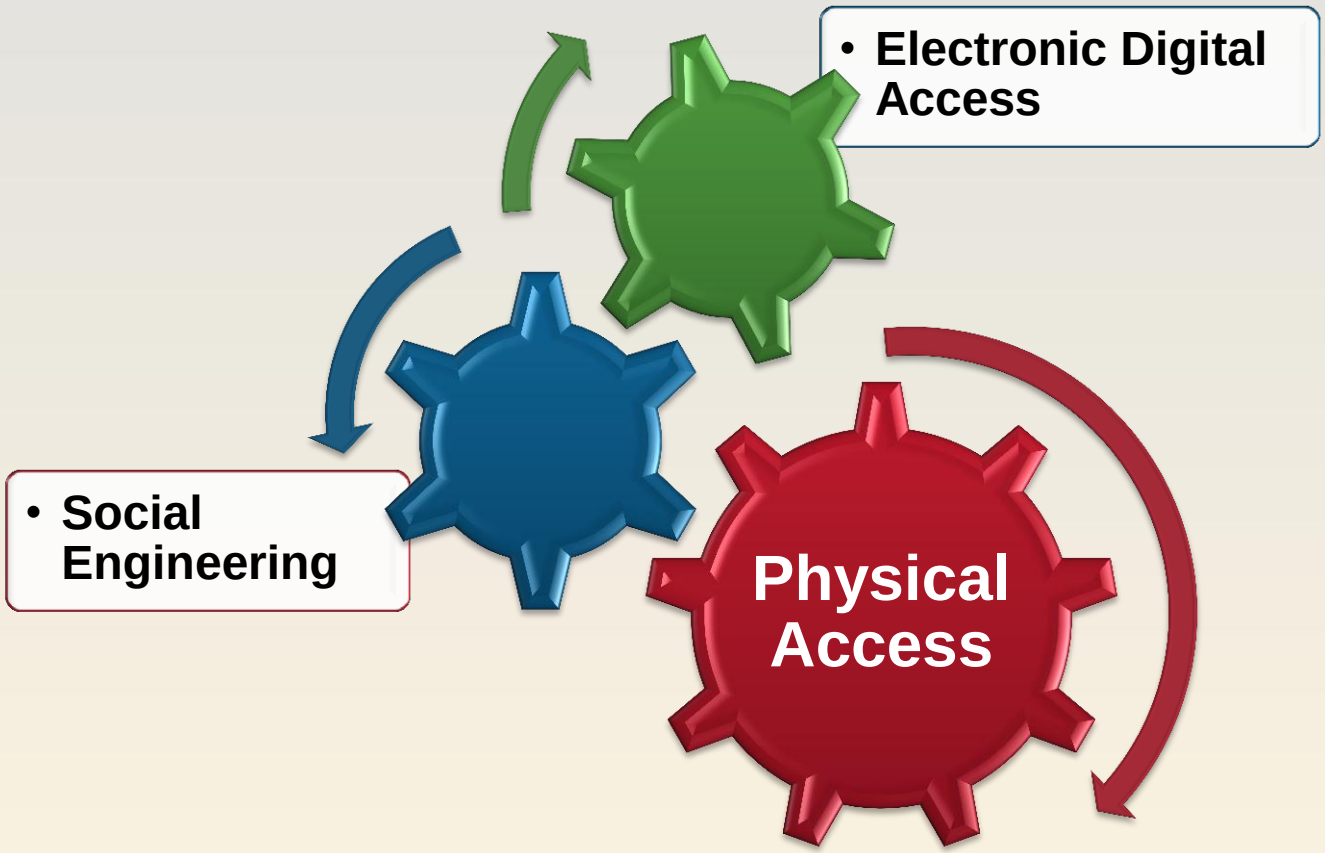


http://freemind.sourceforge.net/

IHMC CmapTools



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.

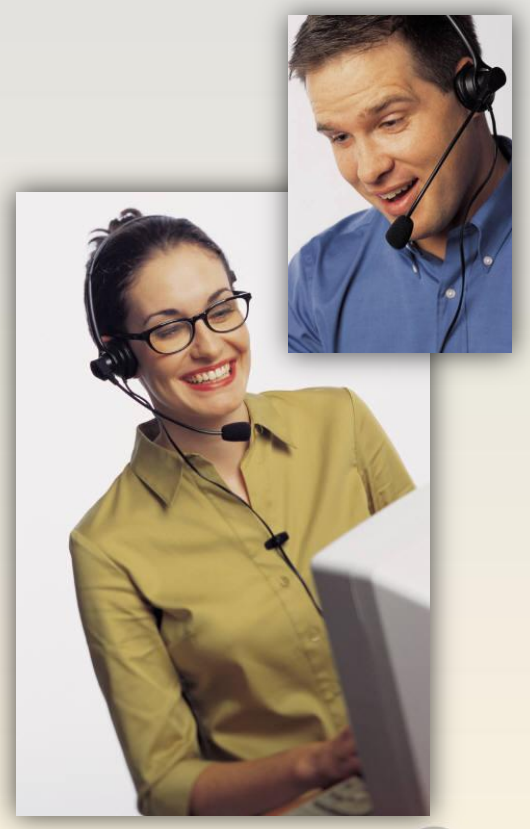
They could pose as a Pest control man, fire inspector, or an employee from another office to gain access to the facility.

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.

Social Engineering Techniques

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

myspace.com a place for music

facebook

classmates.com

LinkedIn

twitter

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.

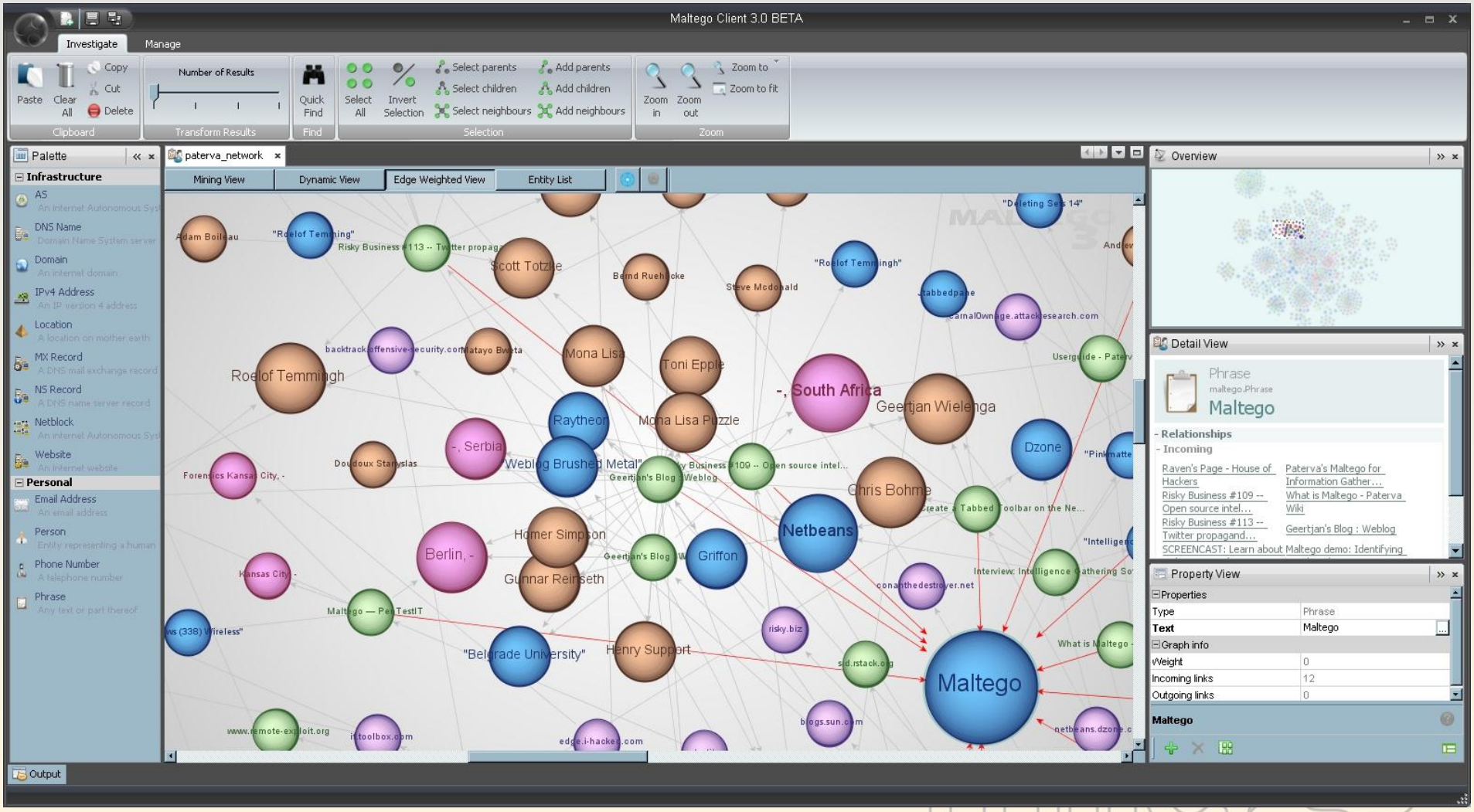
Then finally creating a network diagram and/or a company blueprint for later attack analysis.

Maltego

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.

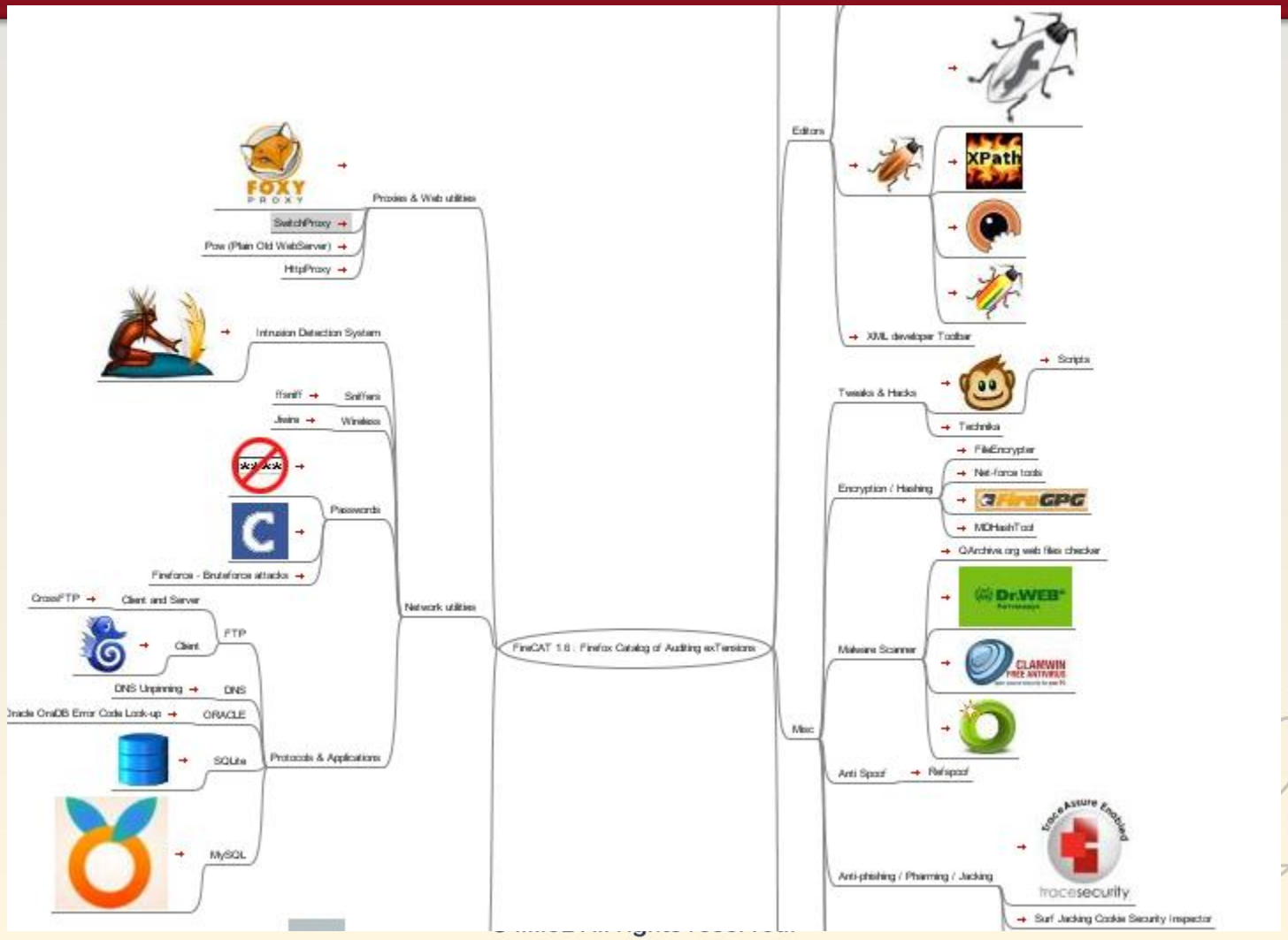
Coupled with its graphing libraries, Maltego, allows you to identify key relationships between information and identify previously unknown relationships between them. It is a must-have tool in the forensics, security and intelligence fields!

Maltego GUI



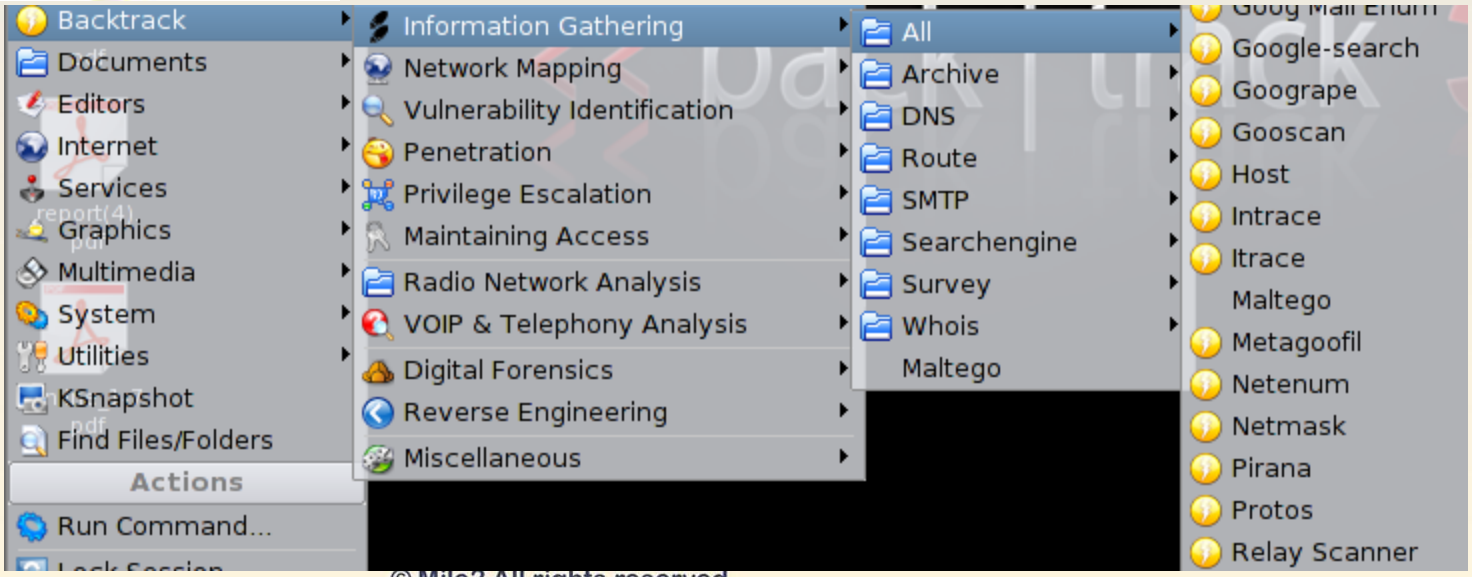
FireCAT

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.

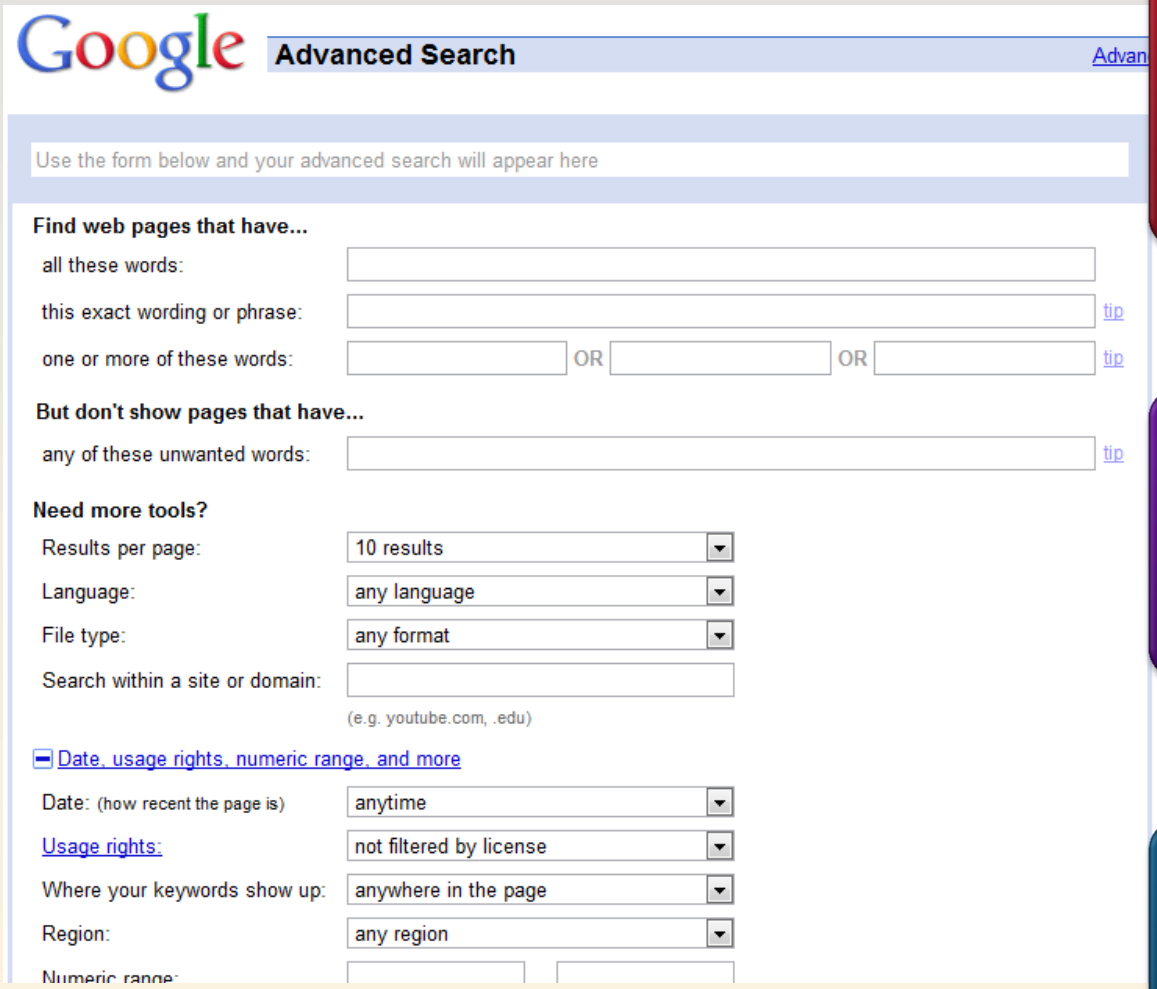
Files containing passwords (135 entries)
PASSWORDS, for the LOVE OF GOD!!! Google found PASSWORDS!

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 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.

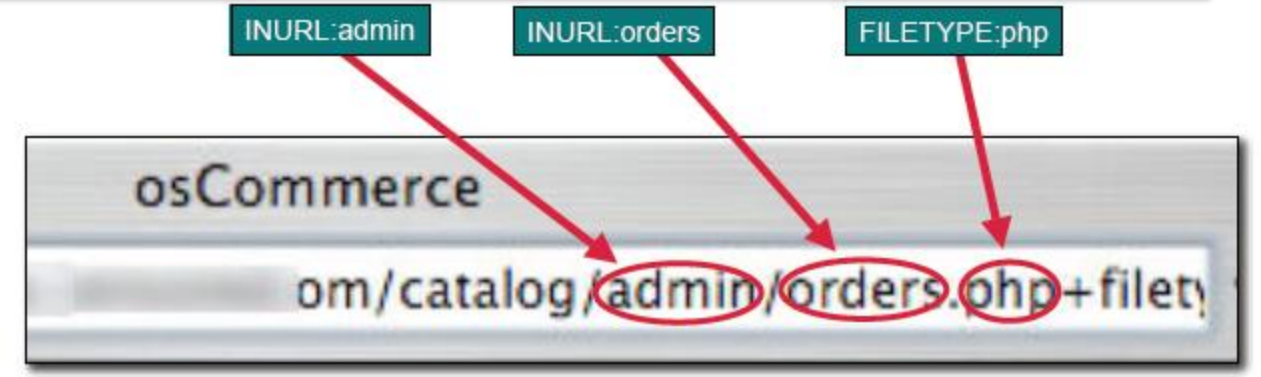
allinurl: restricts the results to those with all of the query words in the url.

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

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

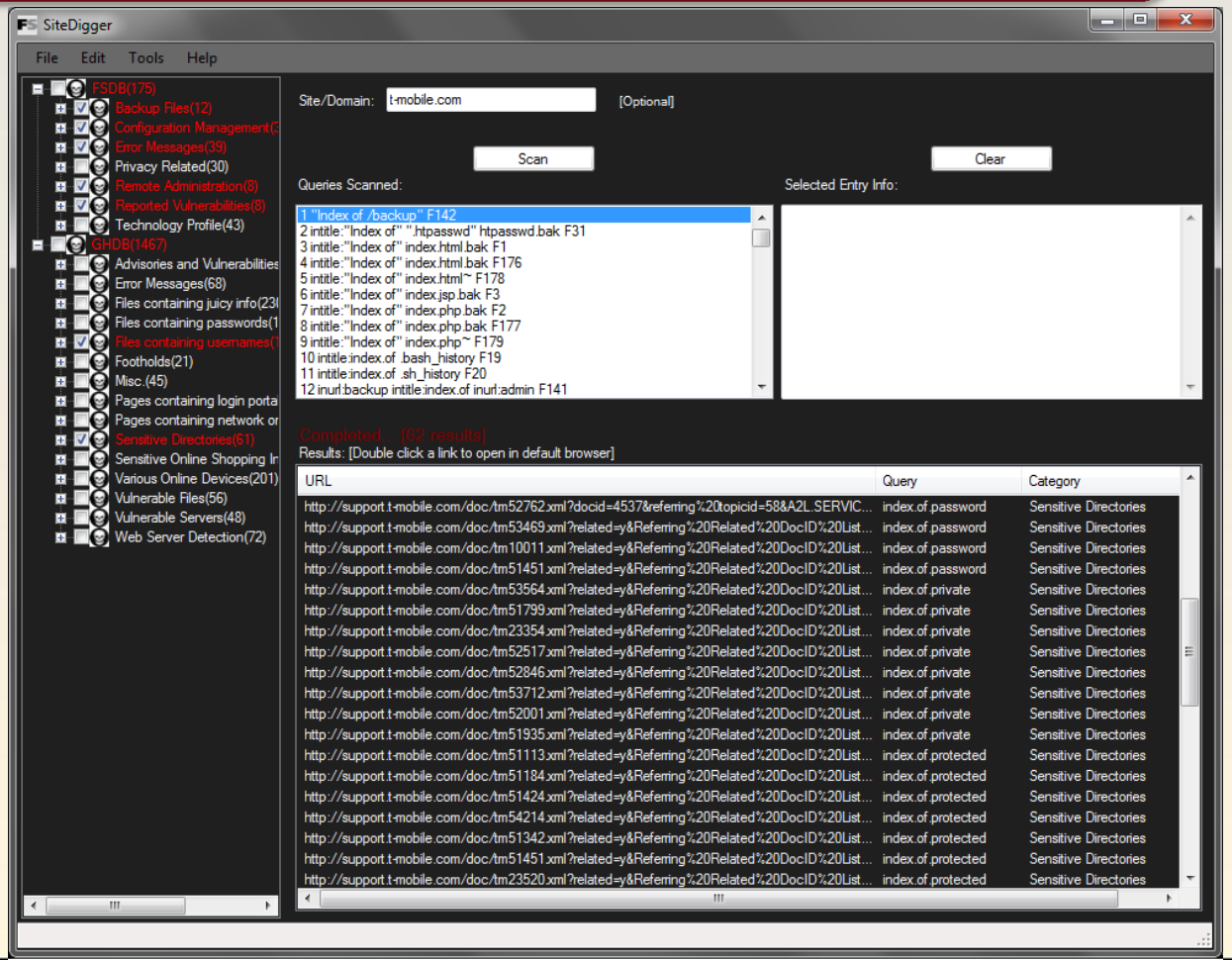
filetype: restricts results to only those containing that filetype.

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

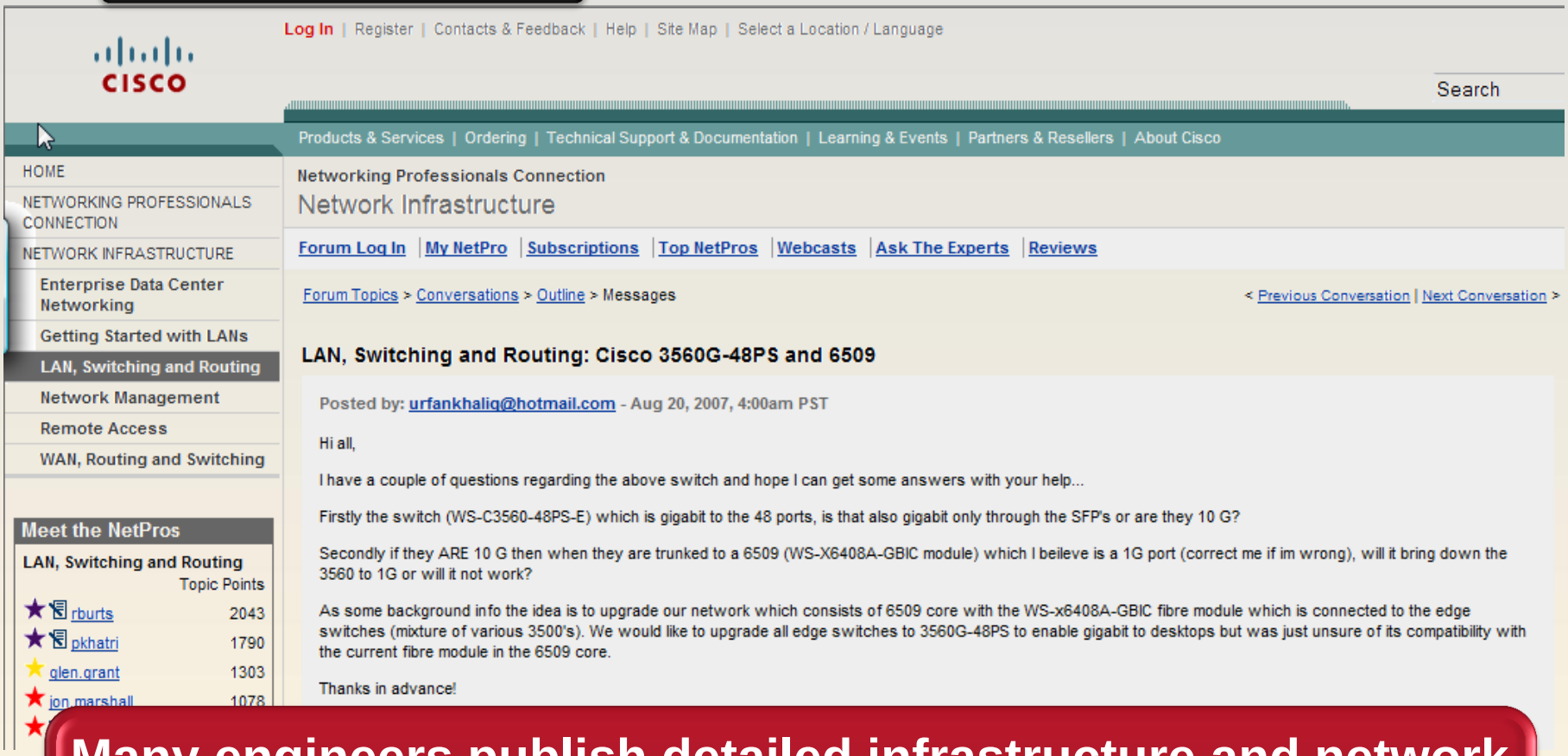
Visit job posting sites:

- 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



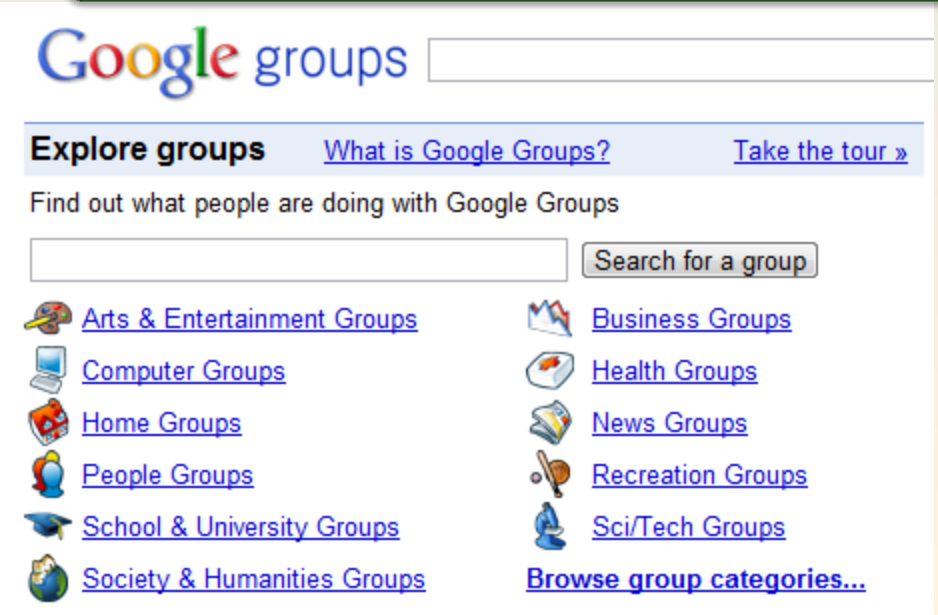
Many engineers publish detailed infrastructure and network device information, such as IP address's, firewall rules and even access passwords.

Google Groups / USENET

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

groups.google.com

“cisco password 7”



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

mile2.com

mile2 IT Security Training & Consulting

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.

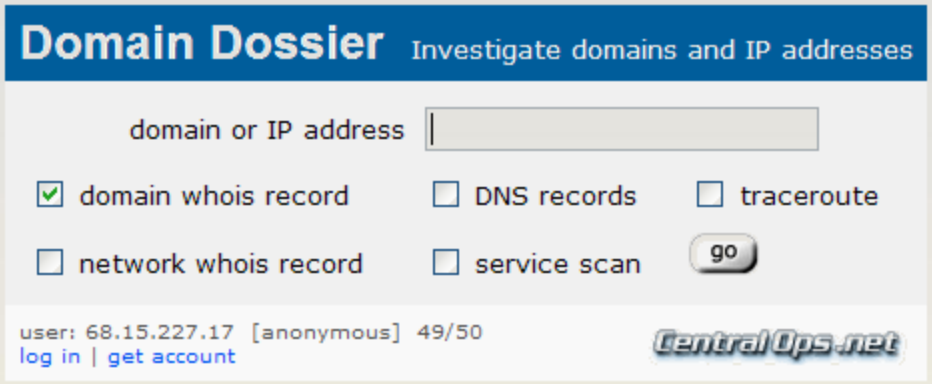
WHOIS information is public information, so anyone can retrieve it….at anytime.

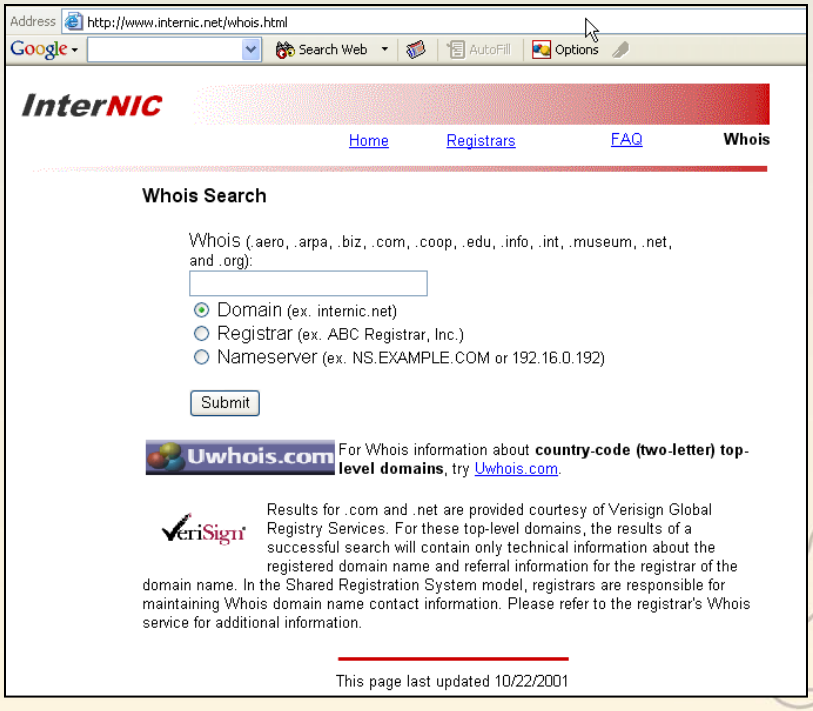
Here's a few sites that do WHOIS queries:

- 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:    [redacted].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
```





DNS Databases

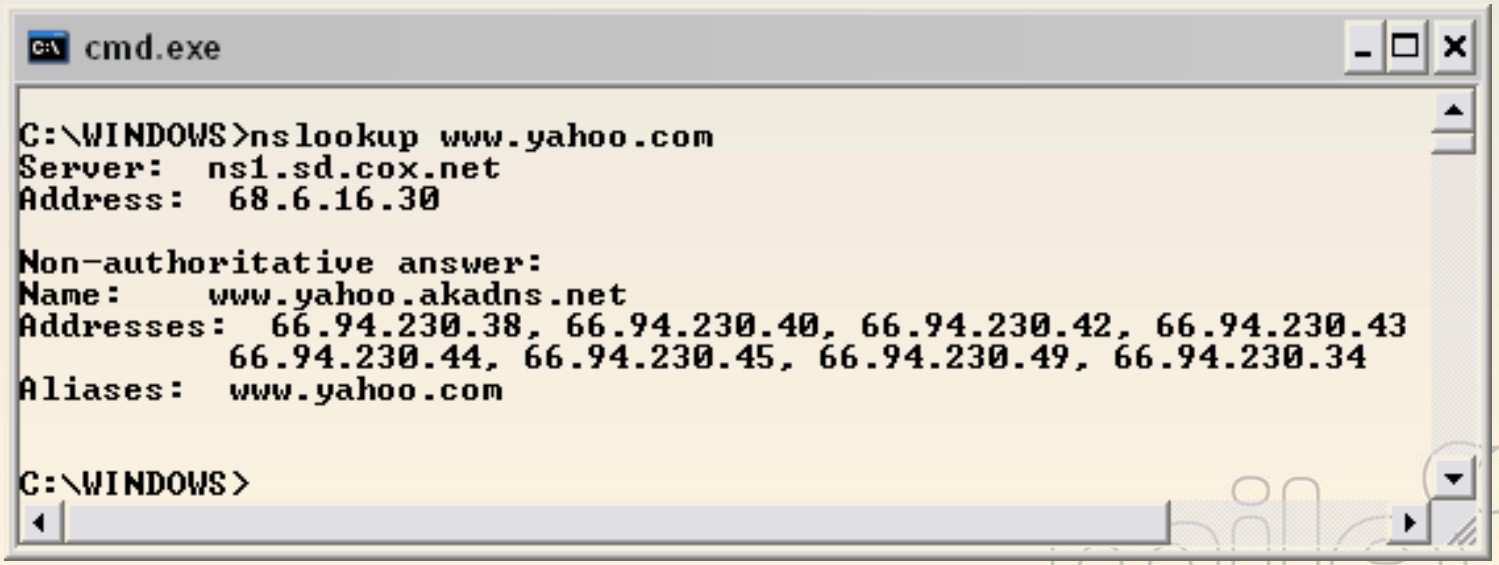
DNS databases contain information about FQDNs and IP addresses. They also contain information such as which servers are the Mail servers and Active Directory servers.

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.



Dig for Unix / Linux

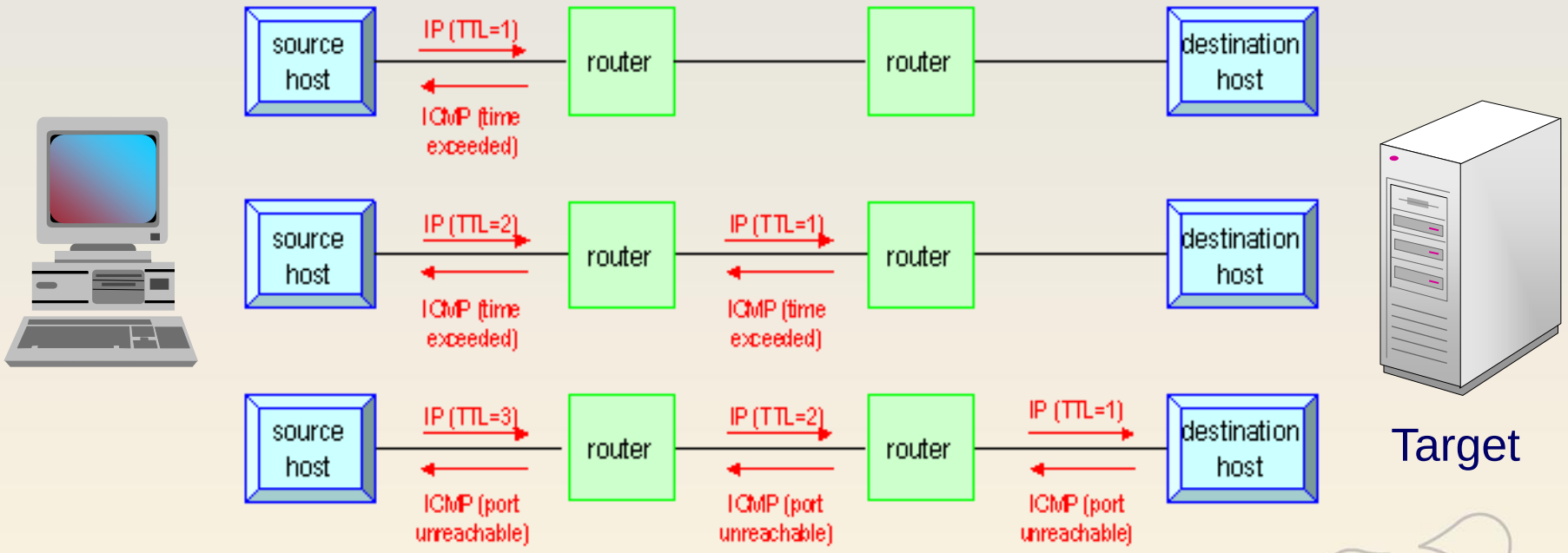
Dig is a Unix utility that performs DNS queries, similar to Nslookup. The syntax of dig is:

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.
```

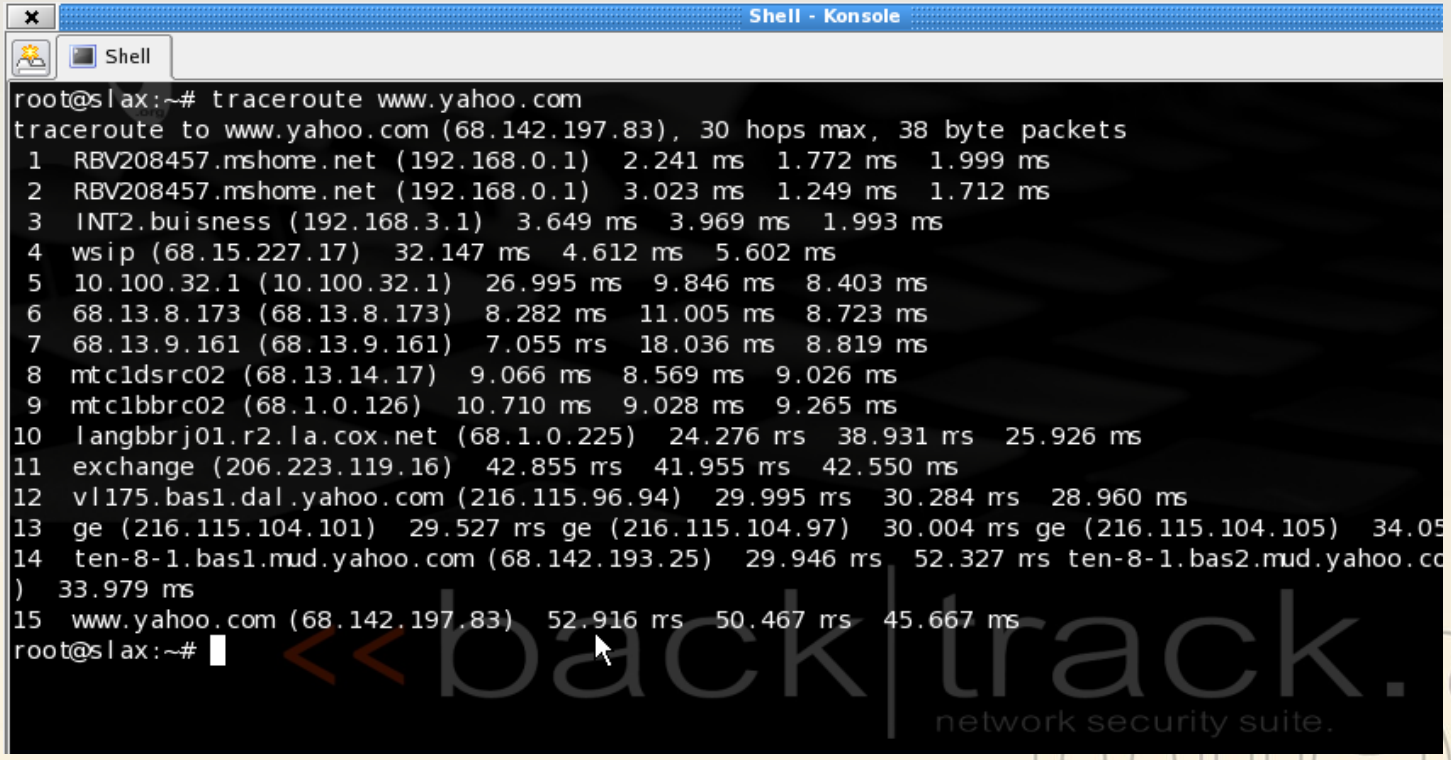
Traceroute Operation

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.

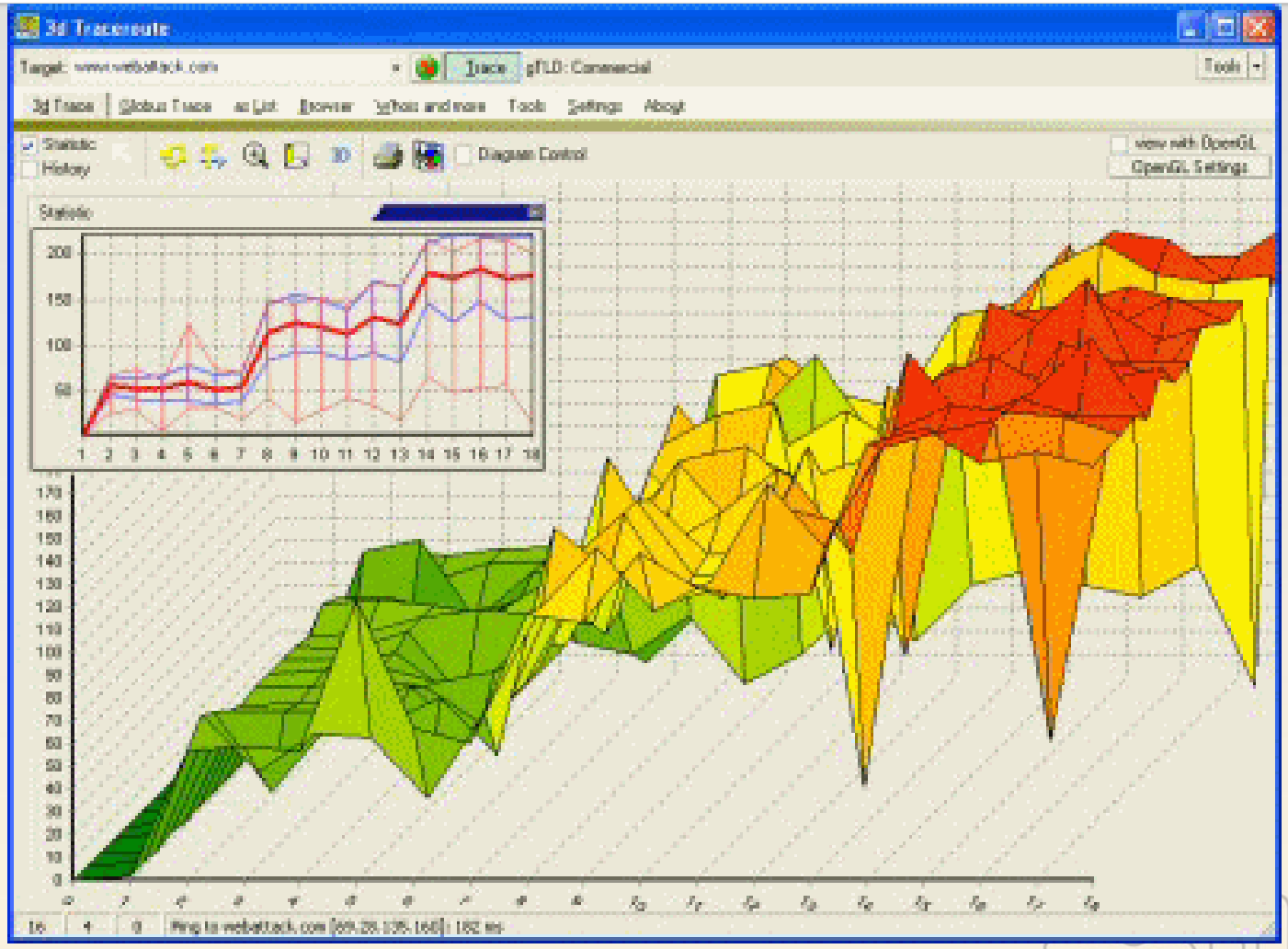


Traceroute (cont.)

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.



3D Traceroute



http://www.d3tr.de/

Opus online traceroute

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

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

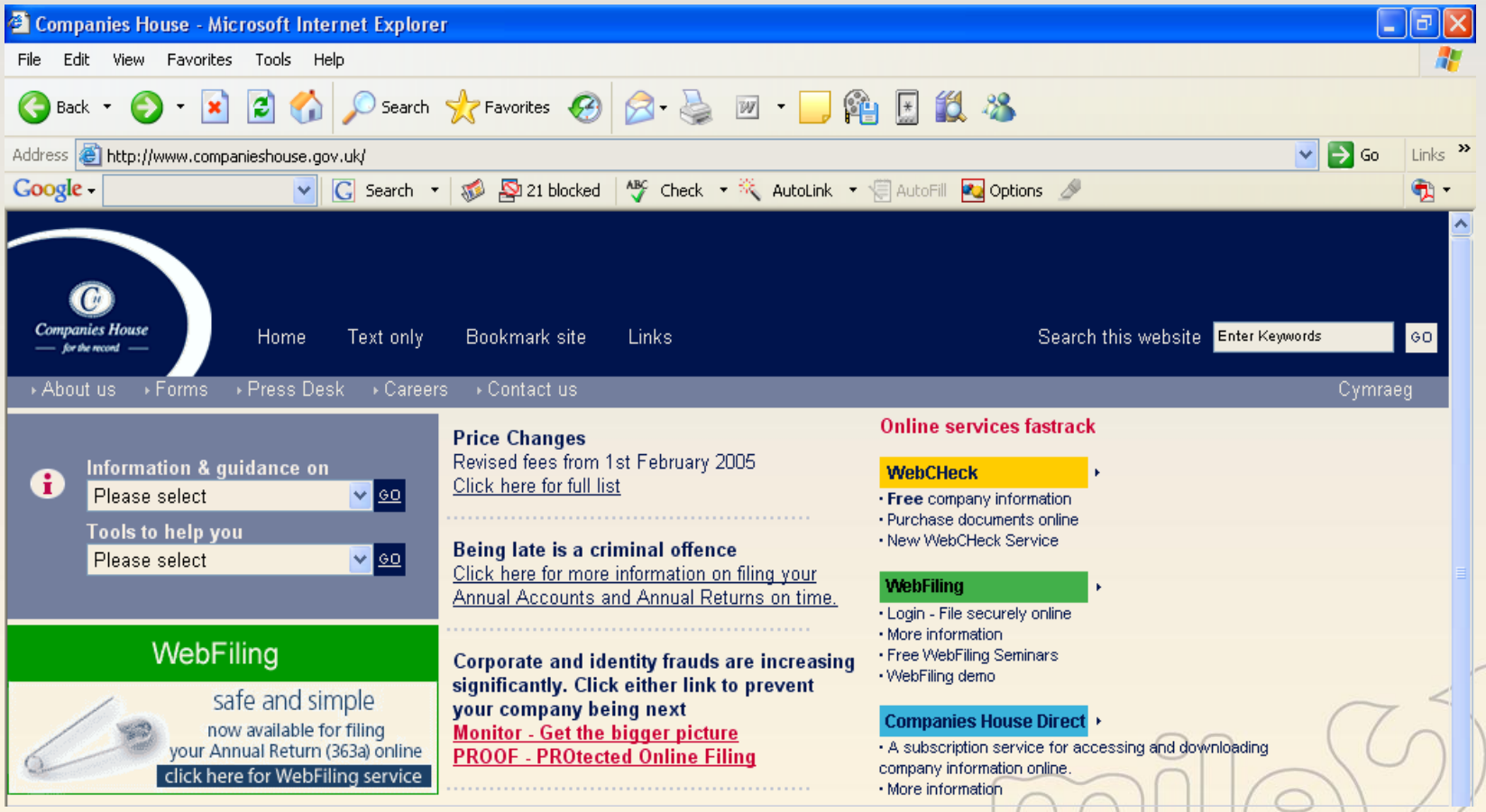
http://www.intelius.com

EDGAR For USA Company Info

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).

Company House For British Company Info

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



Client Email Reputation

WatchGuard ReputationAuthority

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

hsbc.com

Total IPs: 152

SPF record: Present

Learn more about Domain Reputation

Reputation:
- Good
- Suspect
- Bad

Reputation Range: All Show

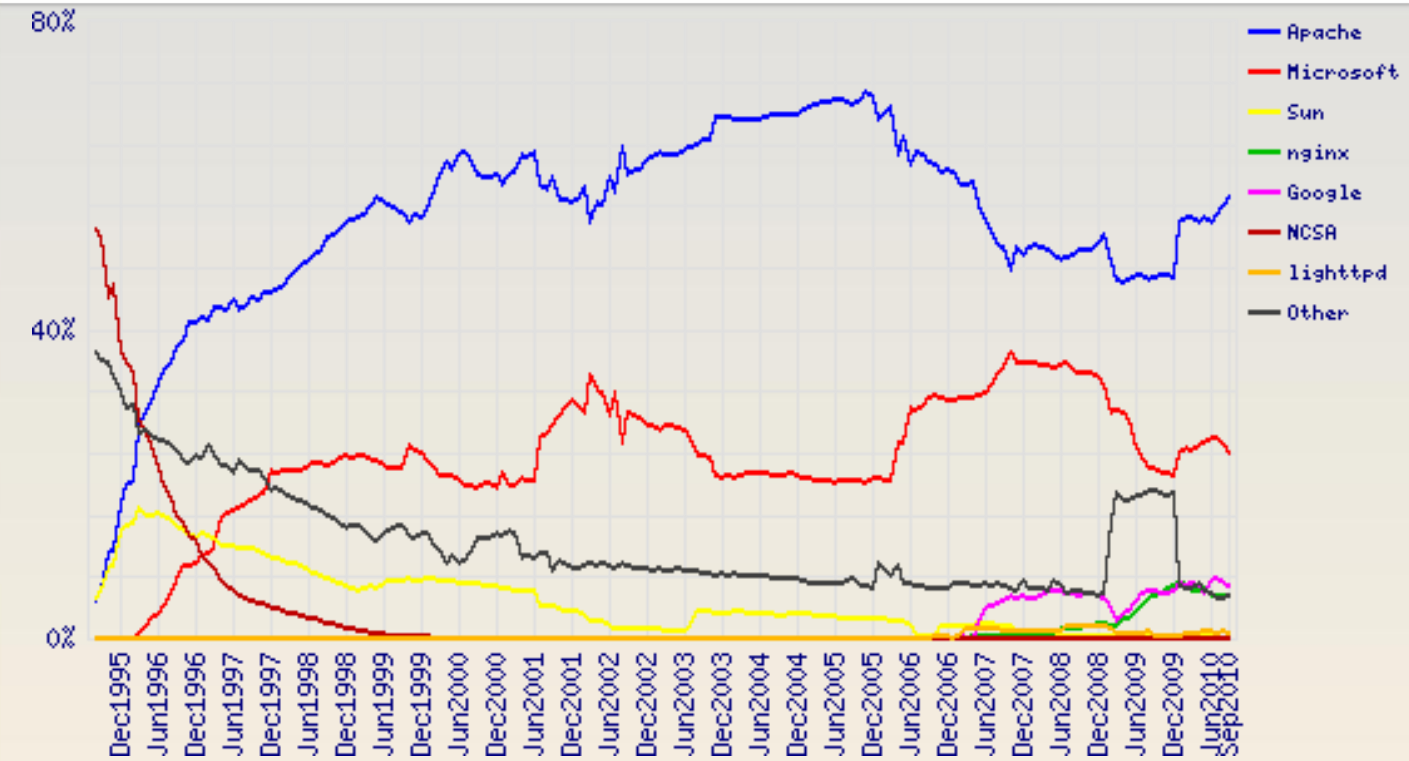
Showing page **1** of **7**

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		89%	11%		99%	1%
203.112.90.35	HSBC BANKING AN	HSBC.COM.H	HK		88%	12%		97%	3%
203.112.84.13	HSBC BANKING AN	HSBC.COM.H	HK		88%	12%		97%	3%
204.178.86.20	MCI COMMUNICATI	ALTER.NET	US		96%	4%		99%	1%
205.214.176.20	HSBC BANK USA	-	US		95%	5%		99%	1%
193.108.75.63	HSBC BANK PLC U	-	UK		64%	36%		99%	1%

http://www.reputationauthority.org/

Web Server Info Tool: Netcraft



NETCRAFT

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.

DOMAINSBYPROXY.COM

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

Google Search 1 blocked 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