CENGAGE Learning

Ethical Hacking and Countermeasures: Attack Phases, Second Edition

Chapter 2
Footprinting

Objectives

After completing this chapter, you should be able to:

- Define footprinting in terms of the reconnaissance phase
- Gather publicly accessible information from a company’s Web site
- Understand both passive and competitive intelligence gathering
- Complete a WHOIS query

Objectives

After completing this chapter, you should be able to (cont'd):

- Trace an Internet connection
- Track a personal e-mail

Introduction to Footprinting

- Footprinting
  - The act of gathering information about the security profile of a computer system or organization, undertaken in a methodological manner
  - First of the three preattack phases: footprinting, scanning, and enumeration
  - Describes the structure and topology of a given system
- Information gathered during this phase can be used to narrow the attack methodology to be used
  - As well as a guide to assess an attack’s merit

Why is Footprinting Necessary?

- Technologies employed in a given system and their organization is key to their vulnerability
- Footprinting can be a difficult task when identifying security postures
- Areas and information that attackers seek
  - Internet
  - Remote Access
  - Intranet
  - Extranet

Revisiting Reconnaissance

- Footprinting, scanning, and enumeration are all essential parts of the reconnaissance phase
- Exact methodology that a hacker adopts while approaching a target can vary
  - Some may randomly select a target based on a vulnerability that can be exploited
  - Others may try their hand at a new technology or skill level
  - Others may be methodologically preparing to attack a particular target for any number of reasons

Information-Gathering Methodology

- Information-gathering activity can be broadly divided into seven phases:
  1. Unearth initial information
  2. Locate the network range
  3. Ascertain active machines
  4. Discover open ports/access points
  5. Detect operating systems
  6. Uncover services on ports
  7. Map the network

Unearthing Initial Information

- Open source footprinting
  - The act of footprinting basic, usually freely available, information about a target
- Attacker may choose to source the information from:
  - A Web page
  - Multiple-search engines
  - Using an advanced search in Web sites
  - Searching on publicly traded companies
- Attackers can look up the domain name with a WHOIS client and also do an Nslookup

Unearthing Initial Information

- A WHOIS query gives additional information such as:
  - Server type, number of DMOZ listings, Web site status, and how many sites the Web server is hosting
- Some WHOIS clients also provide a reverse query
  - Allows a known IP address to be traced back to its domain
- There are five Regional Internet Registries (RIRs)
  - Maintain a WHOIS database with details of IP address registrations in their regions

Unearthing Initial Information

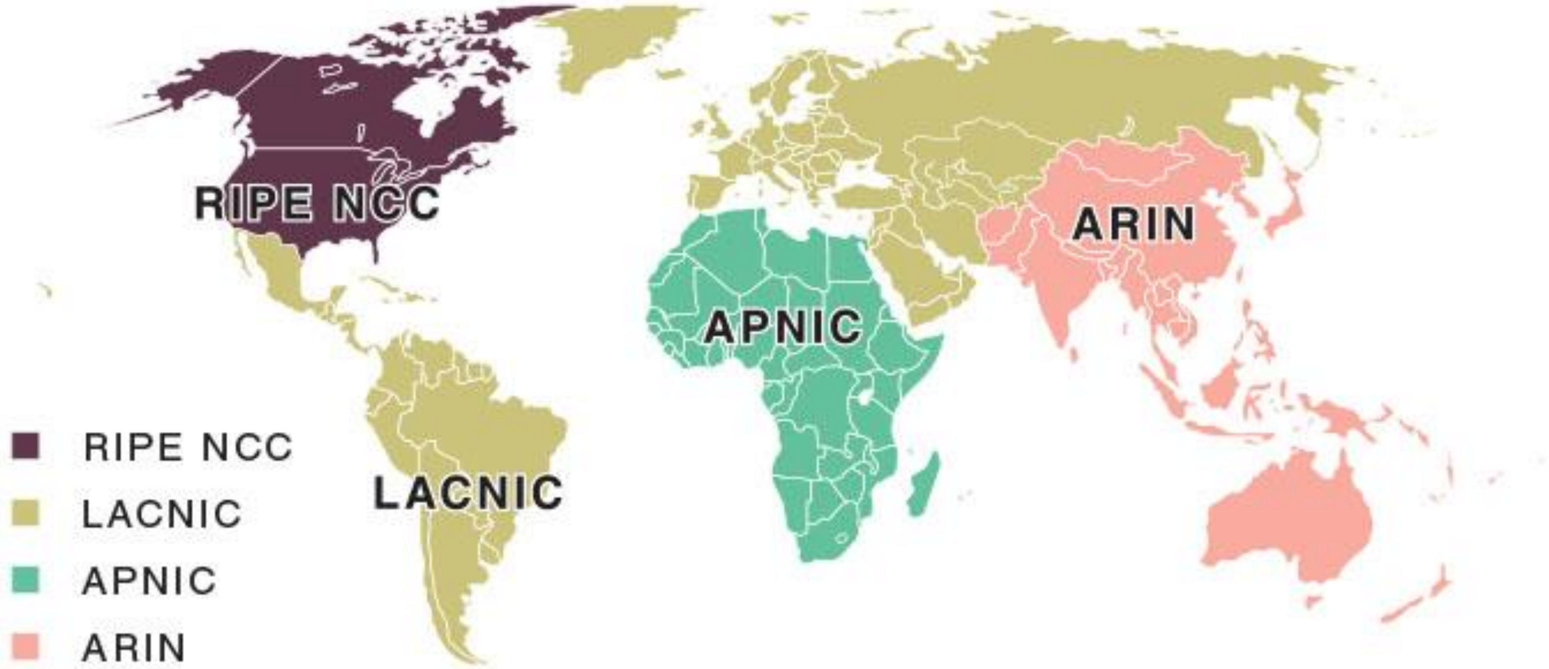


Figure 2-1 RIR coverage map

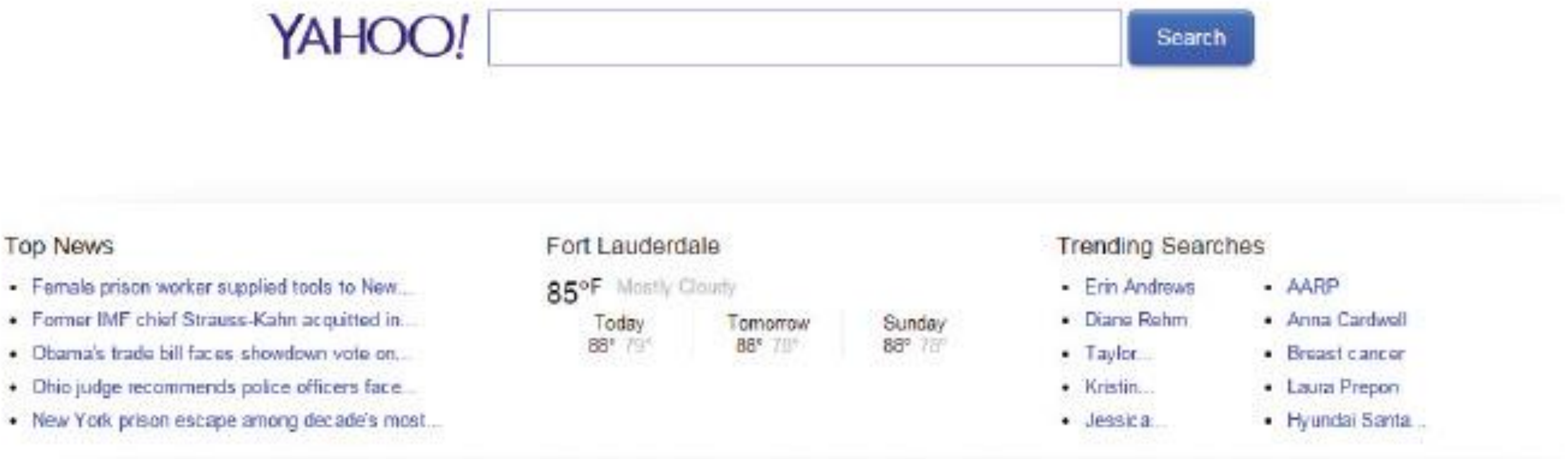
What Is an IP Address?

- IP address (Internet Protocol address)
  - Unique number that devices use in order to identify and communicate with each other on a network
- Any participating device must have its own unique address
  - Allows information passed onward on behalf of the sender to indicate where to send it next
  - For the receiver of the information to know that it is the intended destination
- The numbers currently used in IPv4 addresses range from 1.0.0.0 to 255.255.255.255

Finding a Company’s URL

- Perform a search engine query with the company’s name
  - Search engine will display a list of URLs related to the company
- Internal URLs, or intranets
  - Private links that only company’s employees use
  - Hacker can gain access to internal resources by typing an internal URL
- Extracting an archive of a Web site
  - Archive Web sites can be used to gather information on a company’s Web pages since their creation

People Searching



Top News

- Female prison worker supplied tools to New...
- Former IMF chief Strauss-Kahn acquitted in...
- Obama's trade bill faces showdown vote on...
- Ohio judge recommends police officers face...
- New York prison escape among decade's most...

Fort Lauderdale

85°F Mostly Cloudy

Today	Tomorrow	Sunday
88° 79°	88° 78°	88° 78°

Trending Searches

- Erin Andrews
- Diane Rehm
- Taylor...
- Kristin...
- Jessica...
- AARP
- Anna Cardwell
- Breast cancer
- Laura Prepon
- Hyundai Santa...

Figure 2-2 Yahoo! People Search allows a user to search for people based on set criteria

People Searching

- Information collection and use practices
  - You can choose whether or not to include an e-mail address in a People Search e-mail directory while registering for Yahoo! Mail
- Information sharing and disclosure practices
  - When a person posts personal information online, that person may receive unwanted e-mails or messages from other parties in return
- People search services include:
  - Best People Search, People-Search-America.com, Switchboard, Google Finance, and Yahoo! Finance

Footprinting Through Job Sites

- Job sites may reveal information about a company’s infrastructure
- Depending upon the posted requirements for job openings
  - Attackers may be able to learn about the software, hardware, and network-related information that the company use
- Many strategies of Google Inc. have been leaked through analysis of the company’s job openings

Information Gathering Stances

- **Passive Information Gathering**
  - Carried out by obtaining details that are freely available
  - Every Internet-connected system leaks information in one way or another
- **Competitive Intelligence Gathering**
  - Process of accumulating information from resources such as the Internet that can later be analyzed as business intelligence
  - Noninterfering and subtle in nature compared to the direct intellectual property theft carried out through hacking or industrial espionage

Information Gathering Stances

- Issues involved in competitive intelligence:
  - Data gathering
  - Data analysis
  - Information verification
  - Information security
- Cognitive hacking
  - Information verification and security
- Two types of cognitive hacking:
  - Single-source cognitive hacking
  - Multiple-source cognitive hacking

Information Gathering Services

- Why do hackers need competitive intelligence?
  - It is important in comparing the hacker's product with their competitors' offerings
- Competitive intelligence tools
  - Carratu International
  - CI Centre
  - Trellian
  - Web Investigator
  - RelevantNoise
  - Reputation.COM

Information Gathering Services

- Public and Private Web Sites
  - Public Web sites look like standard URLs:
    - *www.xsecurity.com*
    - *www.xsecurity.net*
    - *www.xsecurity.org*
  - Subdomain URLs or private URLs are not revealed to outsiders and look like the following”
    - *http://intranet.xsecurity.com*
    - *http://partner.xsecurity.com*

Footprinting Tools

- This section covers some possible footprinting tools
- Each tool has unique offerings as well as disadvantages

Sensepost Footprint Tools 3

- Sensepost offers security assessment, training, and consulting services
  - Developed a tool named BiDiBLAH
- System requirements for BiDiBLAH:
  - Microsoft .NET framework
  - Nessus server or login for Nessus functionality
  - A valid Google API key for subdomain discovery
  - MetaSploit Framework for MetaSploit functionality

XYMon

- XYMon is a Web-based system and network monitoring solution
  - Provides a highly scalable, customizable, and easy to maintain system with a small footprint for monitoring the real-time availability of:
    - Network devices
    - Server (Windows, UNIX, and Linux)
    - All network-related services in any IT infrastructure

Advanced Administrative Tools

- Includes the following features:
  - Port scanner
  - Proxy analyzer
  - RBL locator
  - CGI analyzer
  - E-mail verifier
  - Links analyzer
  - Network monitor
  - Process monitor
  - WHOIS
  - System information
  - Resource viewer

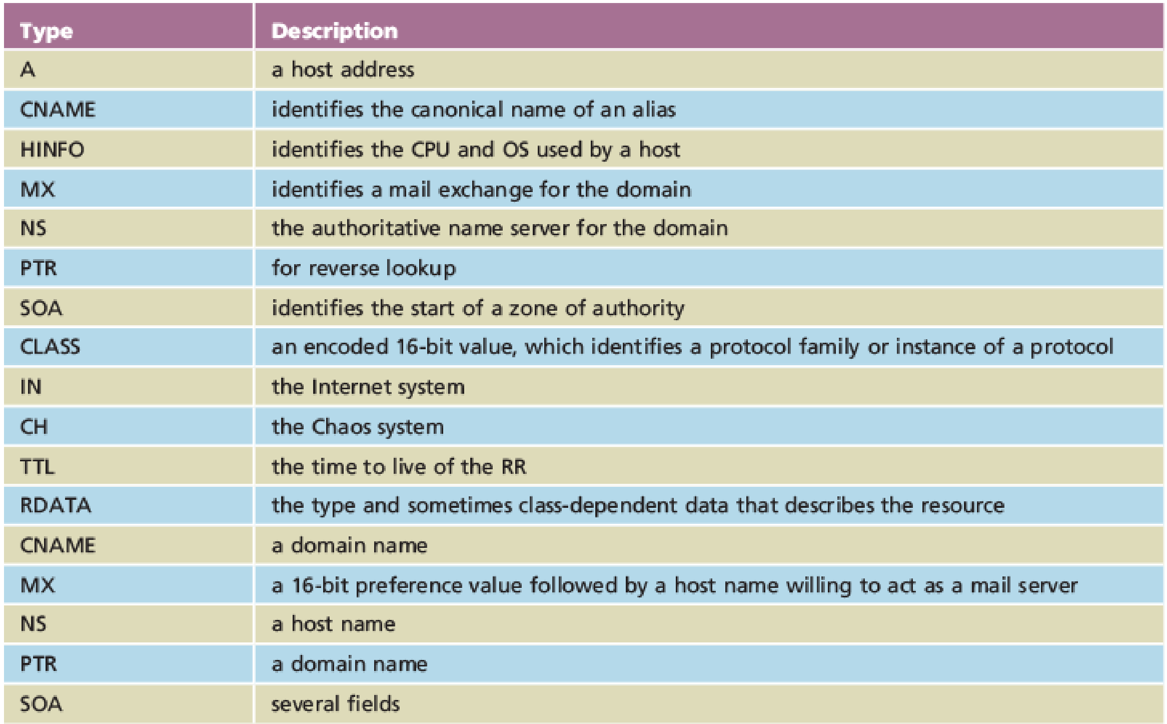
Wikto

- Features of the Wikto footprinting tool:
  - Web server fingerprinting using Net-Square’s HTTPrint
  - Directory and link extraction from mirrors using HTTrack
  - Indexable director detection in BackEnd
  - One-click updates of both Nikto and Google Hack databases
  - Built-in SSL support for Wikto and BackEnd miner

WHOIS Tools

- WHOIS
  - Several operating systems provide a WHOIS utility
  - Syntax: **whois -h hostname identifier**
  - Normal query will result in contact information, name of registrar and name servers, which can be resolved further into specific IP addresses
- A specific RR (resource record) is assumed to have the following:
  - *Owner*
  - *Type*

WHOIS Tools



Type	Description
A	a host address
CNAME	identifies the canonical name of an alias
HINFO	identifies the CPU and OS used by a host
MX	identifies a mail exchange for the domain
NS	the authoritative name server for the domain
PTR	for reverse lookup
SOA	identifies the start of a zone of authority
CLASS	an encoded 16-bit value, which identifies a protocol family or instance of a protocol
IN	the Internet system
CH	the Chaos system
TTL	the time to live of the RR
RDATA	the type and sometimes class-dependent data that describes the resource
CNAME	a domain name
MX	a 16-bit preference value followed by a host name willing to act as a mail server
NS	a host name
PTR	a domain name
SOA	several fields

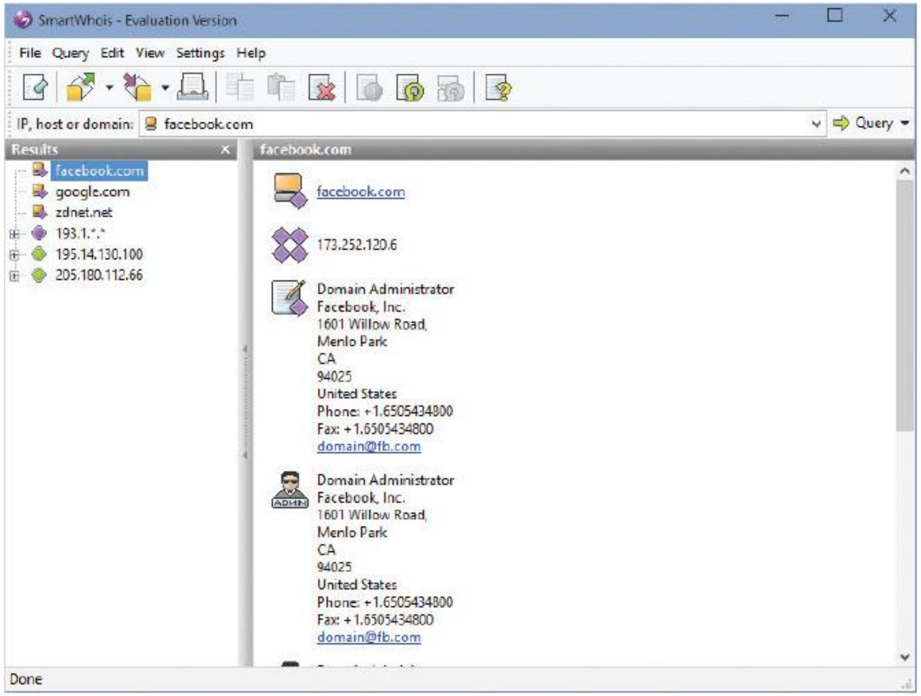
Table 2-1 The various types of information in a resource record

WHOIS Tools

- Types of queries for a WHOIS database:
  - *Registar*
  - *Organizational*
  - *Domain*
  - *Network*
  - *Point of contact (POC)*

WHOIS Tools

- SmartWhois
  - Allows users to find information about an IP address, host name, or domain



SmartWhois - Evaluation Version
File Query Edit View Settings Help
Query
Results
facebook.com

IP, host or domain: facebook.com

facebook.com
google.com
zdnet.net
193.1.*.*
195.14.130.100
205.180.112.66

facebook.com

173.252.120.6

Domain Administrator
Facebook, Inc.
1601 Willow Road,
Menlo Park
CA
94025
United States
Phone: +1.6505434800
Fax: +1.6505434800
domain@fb.com

Domain Administrator
Facebook, Inc.
1601 Willow Road,
Menlo Park
CA
94025
United States
Phone: +1.6505434800
Fax: +1.6505434800
domain@fb.com

Done

Figure 2-3 SmartWhois is a WHOIS utility that provides information about the registered owner of a Web site

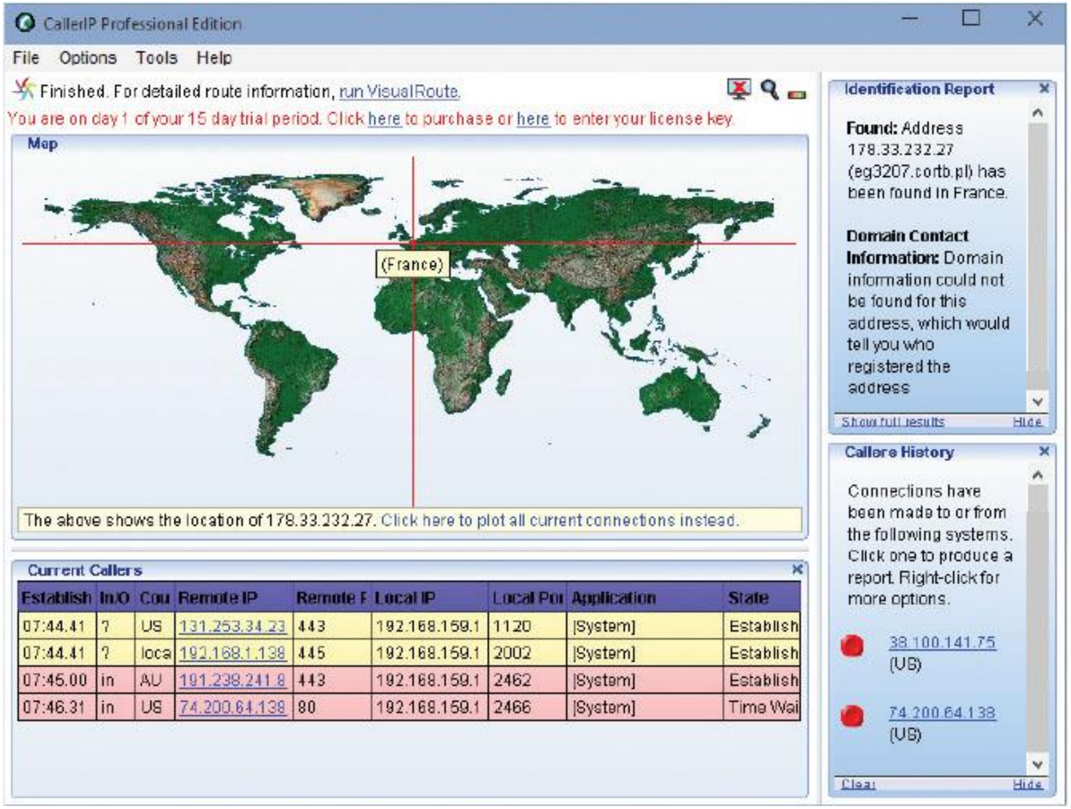
WHOIS Tools

- ActiveWhois
  - A network tool that retrieves information such as countries, e-mail addresses, and postal addresses of owners of IP addresses and Internet domains
  - Features of ActiveWhois:
    - Can work in offline mode (saved to disk and accessible without an Internet connection)
    - Can be used to check and register domains
    - Includes tools for investigating attacks, spam, suspicious Web sites, and IRC and IM screen names

WHOIS Tools

- LanWhoIs
  - Helps a user find out who registered a domain, and where and when that domain was registered
- CountryWhois
  - A user can make IP-to-country correlations
- CallerIP
  - Used to see when someone has connected to his or her computer (provides evidence of an invasion)
  - Determines IP address of the external system and runs a trace on that address

WHOIS Tools



Finished. For detailed route information, run VisualRoute.

You are on day 1 of your 15 day trial period. Click here to purchase or here to enter your license key.

The above shows the location of 178.33.232.27. Click here to plot all current connections instead.

Current Callers

Establish	In/O	Cou	Remote IP	Remote F	Local IP	Local Por	Application	State
07:44.41	?	US	131.253.34.23	443	192.168.159.1	1120	[System]	Establish
07:44.41	?	loca	192.168.1.138	445	192.168.159.1	2002	[System]	Establish
07:45.00	in	AU	191.238.241.8	443	192.168.159.1	2462	[System]	Establish
07:46.31	in	US	74.200.64.138	80	192.168.159.1	2466	[System]	Time Wai

Identification Report

Found: Address 178.33.232.27 (eg3207.cortb.pl) has been found in France.

Domain Contact Information: Domain information could not be found for this address, which would tell you who registered the address

Show full results Hide

Callers History

Connections have been made to or from the following systems. Click one to produce a report. Right-click for more options.

● 38.100.141.75 (US)

● 74.200.64.138 (US)

Clear Hide

Figure 2-4 CallerIP can show the IP addresses of computers that have connected to a particular system

WHOIS Tools

- Web Data Extractor
  - Extracts data from Web sites
  - Can extract:
    - Company contact data
    - URLs
    - Metadata stored in a Web page

DNS Information Tools

- DNS Enumerator
  - Perl script that uses Google to extract subdomains and DNS names
- SpiderFoot
  - Open-source domain footprinting tool that searches the Web sites on the given domain and also queries search engines, WHOIS, and DNS servers

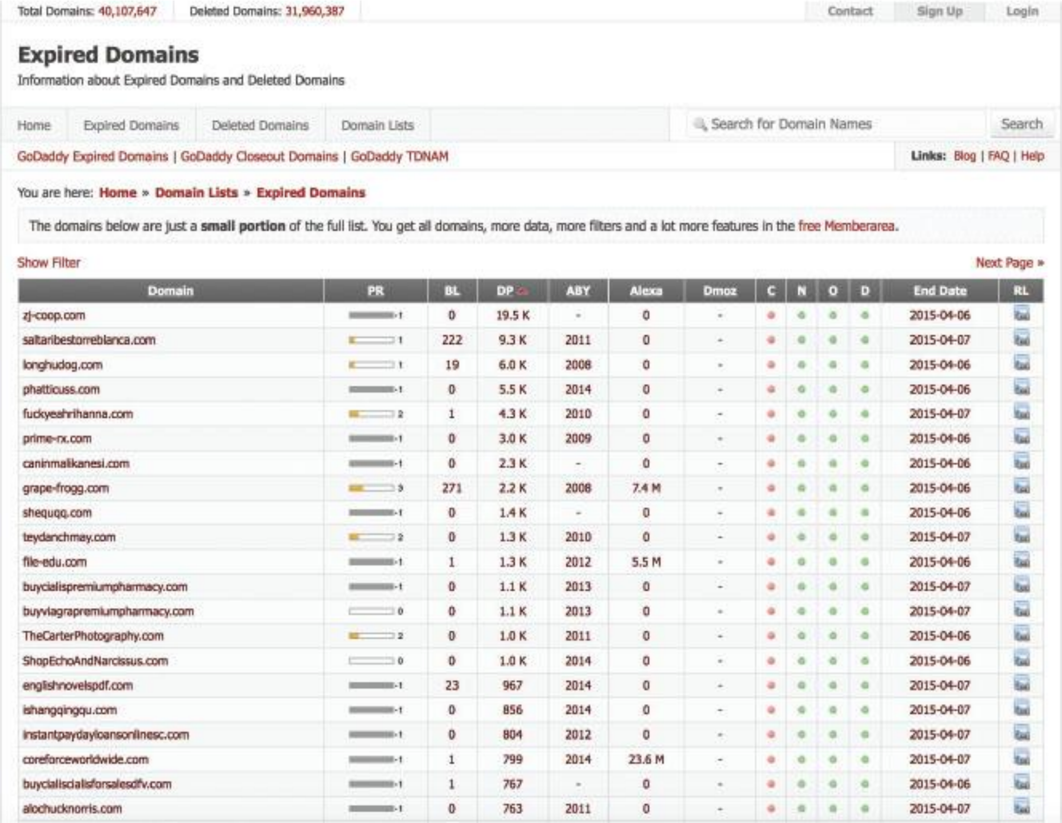
DNS Information Tools

- Nslookup
  - Tool for querying DNS information for host name resolution
  - Allows the local machine to focus on a DNS server that is different from the default one by invoking the server command
  - Employs the domain name delegation method when used on the local domain
  - Zone transfers
    - To stop unauthorized zone transfers, an administrator must specify exact IP addresses from where zone transfers may be allowed

DNS Information Tools

- DNSstuff.com
  - Users can extract DNS information about IP addresses and find information about mail server extensions
- Expired Domains
  - A web tool that allows a user to search through a list of expired and expiring domain names by keyword

DNS Information Tools



Total Domains: 40,107,647 | Deleted Domains: 31,960,387

Contact | Sign Up | Login

Expired Domains

Information about Expired Domains and Deleted Domains

Home | Expired Domains | Deleted Domains | Domain Lists

Search for Domain Names | Search

GoDaddy Expired Domains | GoDaddy Closeout Domains | GoDaddy TDNAM

Links: Blog | FAQ | Help

You are here: **Home** » **Domain Lists** » **Expired Domains**

The domains below are just a **small portion** of the full list. You get all domains, more data, more filters and a lot more features in the free Memberarea.

Show Filter

Next Page »

Domain	PR	BL	DP	ABY	Alexa	Dmoz	C	N	O	D	End Date	RL
zj-coop.com	-1	0	19.5 K	-	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
saltaribestorreblanca.com	1	222	9.3 K	2011	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
longhudog.com	1	19	6.0 K	2008	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
phatticuss.com	-1	0	5.5 K	2014	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
fuckyeahrihanna.com	2	1	4.3 K	2010	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
prime-rx.com	-1	0	3.0 K	2009	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
caninmalikanesi.com	-1	0	2.3 K	-	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
grape-frogg.com	3	271	2.2 K	2008	7.4 M	-	🔴	🟢	🟢	🟢	2015-04-06	▣
shequqq.com	-1	0	1.4 K	-	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
teydanchmay.com	2	0	1.3 K	2010	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
file-edu.com	-1	1	1.3 K	2012	5.5 M	-	🔴	🟢	🟢	🟢	2015-04-06	▣
buycialispremiumpharmacy.com	-1	0	1.1 K	2013	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
buyviagrapremiumpharmacy.com	0	0	1.1 K	2013	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
TheCarterPhotography.com	2	0	1.0 K	2011	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
ShopEchoAndNarcissus.com	0	0	1.0 K	2014	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
englishnovelspdf.com	-1	23	967	2014	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
ishangqingqu.com	-1	0	856	2014	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
instantpaydayloansonlinesc.com	-1	0	804	2012	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣
coreforceworldwide.com	-1	1	799	2014	23.6 M	-	🔴	🟢	🟢	🟢	2015-04-07	▣
buycialiscialisforsalesdfv.com	-1	1	767	-	0	-	🔴	🟢	🟢	🟢	2015-04-06	▣
alochucknorris.com	-1	0	763	2011	0	-	🔴	🟢	🟢	🟢	2015-04-07	▣

Figure 2-5 Expired Domains provides listings of expired and expiring domains

DNS Information Tools

- DomainKing
  - Software tool that searches WHOIS databases to find free, taken, and expired domain names
  - Can generate domains based on keywords, search the Web for domains, and generate misspelled domains
- MSR Strider URL Tracer
  - Allows a user to scan a domain name to see the third-party domains that it serves content from and whether the site is being redirected

Locating the Network Range

- Attacker can get more detailed information from the appropriate regional registry database regarding IP allocation and the nature of the allocation
- **Tracerouting**
  - Tracing the route between the attacker system and the target system
  - Popular traceroute tools: NeoTrace and Visual Route
- If the DNS servers are not set up correctly
  - Attacker has a good chance of obtaining a list of internal machines on the server

ARIN

- ARIN allows for a search of the WHOIS database in order to locate information about a network's autonomous system numbers (ASNs), network-related handles, and points of contact (POC)
  - Good starting point for information gathering because the information retrieved is more elaborate
- From an Nslookup query, an attacker can find name servers, mail exchange servers, and the classes to which these servers belong
  - Mail exchange servers can then be further resolved into IP addresses

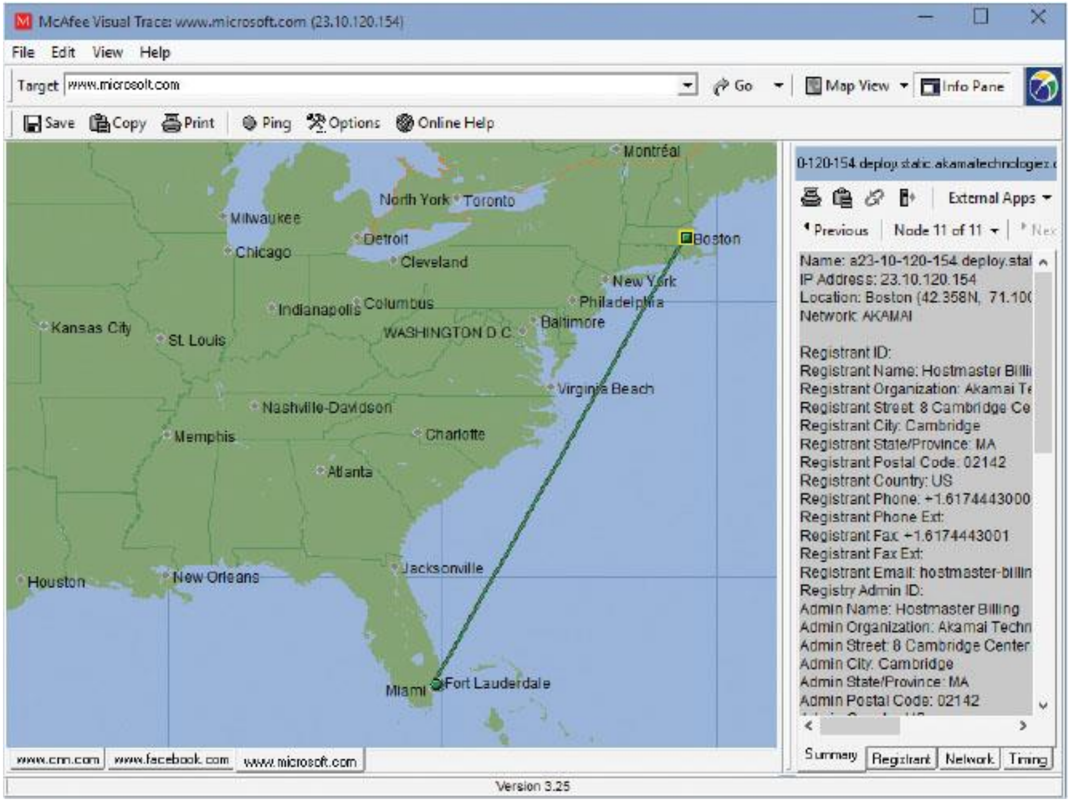
Traceroute

- Details the path that IP packets travel between two systems
- Tells a user:
  - How many routers packets travel through
  - How long it takes the packets to travel from one router to the next
  - Information about those routers, including their names and geographic locations
- Uses the Time To Live (TTL) field in an IP packet to determine how long it takes to reach a target host and whether that host is reachable and active

3D Traceroute

- 3D Traceroute
  - Three-dimensional program that allows a user to visually monitor Internet traces
  - Provides different graphing options and provides statistical information
  - Provides both a GUI and a command-line interface

NeoTrace (now McAfee Visual Trace)



Target: www.microsoft.com

0-120-154.deploy.static.akamaitechnologies.c

```
Name: a23-10-120-154.deploy.stat
IP Address: 23.10.120.154
Location: Boston (42.358N, 71.10(
Network: AKAMAI

Registrant ID:
Registrant Name: Hostmaster Billi
Registrant Organization: Akamai Te
Registrant Street: 8 Cambridge Ce
Registrant City: Cambridge
Registrant State/Province: MA
Registrant Postal Code: 02142
Registrant Country: US
Registrant Phone: +1.6174443000
Registrant Phone Ext:
Registrant Fax: +1.6174443001
Registrant Fax Ext:
Registrant Email: hostmaster-billin
Registry Admin ID:
Admin Name: Hostmaster Billing
Admin Organization: Akamai Techn
Admin Street: 8 Cambridge Center
Admin City: Cambridge
Admin State/Province: MA
Admin Postal Code: 02142
```

Figure 2-6 NeoTrace traces the path from the host system to any target system on the Internet

VisualRoute

- Graphical tool that determines where and how network traffic is flowing on the route between the desired destination and the location from which the user is trying to access it
- Provides three types of data:
  - An overall analysis
  - A data table
  - A geographical view of the routing

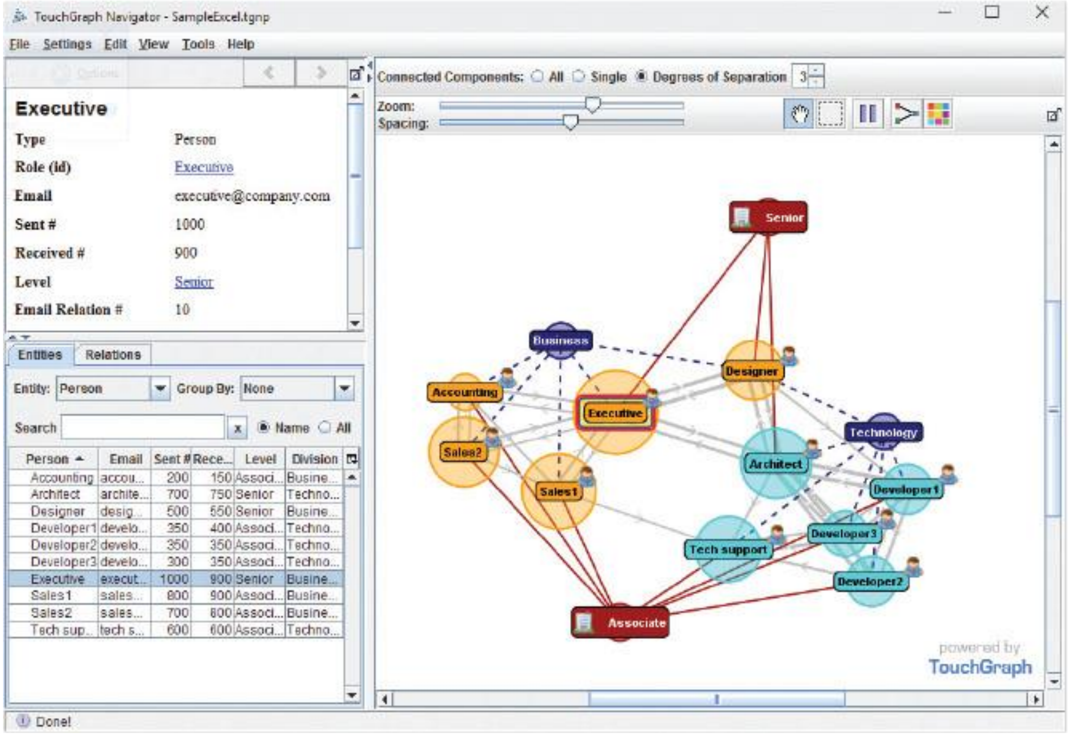
Path Analyzer Pro

- Traces network paths to determine where problems are occurring along the route
  - Whether the problems are being caused by a fault network device or a firewall blocking communication

Maltego

- An online tool for carrying out initial footprinting of a target network
- Can be used to unearth information related to:
  - People
  - Groups of people (social networks)
  - Companies
  - Organizations
  - Web sites
  - Internet infrastructure

TouchGraph



Connected Components: ○ All ○ Single ● Degrees of Separation 3

Executive

Type Person

Role (id) Executive

Email executive@company.com

Sent # 1000

Received # 900

Level Senior

Email Relation # 10

Entities | Relations

Entity: Person Group By: None

Search ● Name ○ All

Person	Email	Sent #	Rece...	Level	Division
Accounting	accou...	200	150	Associ...	Busine...
Architect	archite...	700	750	Senior	Techno...
Designer	desig...	500	550	Senior	Busine...
Developer1	develo...	350	400	Associ...	Techno...
Developer2	develo...	350	350	Associ...	Techno...
Developer3	develo...	300	350	Associ...	Techno...
Executive	execut...	1000	900	Senior	Busine...
Sales1	sales...	800	900	Associ...	Busine...
Sales2	sales...	700	800	Associ...	Busine...
Tech sup...	tech s...	600	600	Associ...	Techno...

Figure 2-7 Touchgraph shows relationships between people, organizations, and ideas

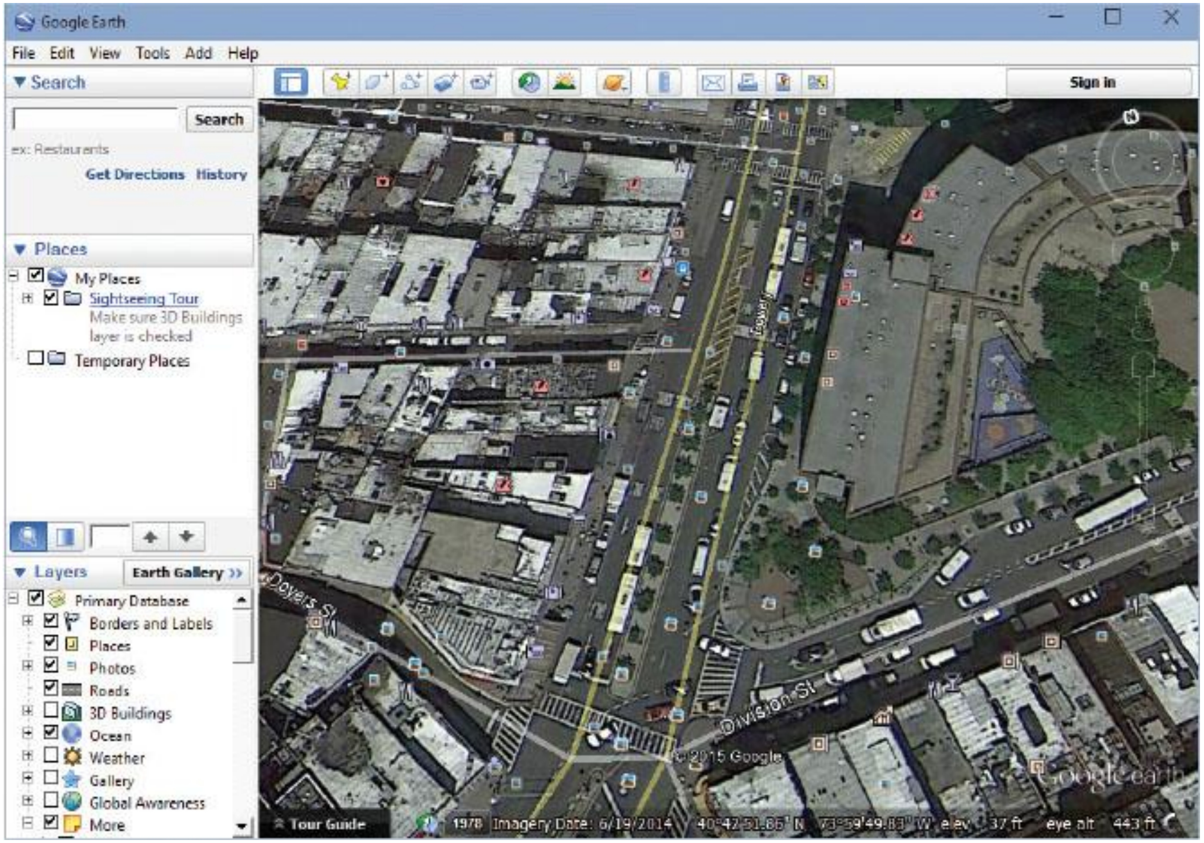
E-Mail Spiders

- 1st Email Address Spider
  - E-mail extractor tool that a spammer can use to set up mailing lists based on his or her preferences
  - User can type in keywords and gain numerous e-mail addresses that match specified criteria.
- Power Email Collector
  - E-mail address harvesting program
  - Can collect up to 750,000 unique valid e-mail addresses per hour with a broadband connection

Locating Network Activity

- GEO Spider
  - Allows a user to monitor his or her network activity by plotting this activity on a world map
  - Can also trace a hacker, investigate a Web site, and trace a domain name
- Google Earth
  - Provides imagery and geographic information for many locations
  - A user can footprint a location using Google Earth

Locating Network Activity



- ☑ My Places
  - ☑ Sightseeing Tour
    Make sure 3D Buildings layer is checked
- □ Temporary Places

- ☑ Primary Database
  - ☑ Borders and Labels
  - ☑ Places
  - ☑ Photos
  - ☑ Roads
  - □ 3D Buildings
  - ☑ Ocean
  - □ Weather
  - □ Gallery
  - □ Global Awareness
  - ☑ More

Figure 2-8 Google Earth provides satellite images of geographic locations around the globe

Meta Search Engines

- Dogpile
  - Meta search engine that fetches results from Google, Yahoo!, Live Search, Ask.com, About.com, MIVA, LookSmart, and other popular search engines
- WebFerret
  - Allows a user to search the Web quickly by submitting search queries to multiple search engines
- robots.txt
  - Holds a list of directories and other resources on a site that the owner does not want to be indexed by search engines

Meta Search Engines

- WTR – Web The Ripper 2
  - Allows a user to select and download files that are linked from a specified Web page
- Web Site Watcher
  - Keeps track of a user's favorite Web sites for updates and automatic changes
  - Benefits:
    - Can scan competitor's Web sites
    - Can keep track of when new software versions or driver updates are released
    - Can highlight changes in Web pages that are modified

Faking Web Sites Using Man-in-the-Middle Phishing Kit

- An attacker can use this kit to import pages from any target Web site
- Malicious users can use this kit to do phishing attacks
  - Can intercept any type of credentials submitted to a target site
- Fraudsters use the Universal Man-in-the-Middle Phishing Kit to create a fake URL via a simple online interface
  - This fake URL communicates with the legitimate Web site of the targeted organization in real time

Summary

- Footprinting is the blueprint of the security profile of an organization, undertaken in a methodological manner
- Footprinting is necessary to systematically and methodically ensure that all pieces of information related to an organization’s technologies are identified
- The information-gathering activity can be categorized into seven phases
- Passive information gathering is done without coming into contact with the organization’s servers

Summary

- Competitive intelligence gathering is the process of gathering information about a company’s competitors from resources such as the Internet
- WHOIS and ARIN, APNIC, LACNIC, and AFRINIC can be used to reveal public information about a domain
- Traceroute and mail tracking can be used to target specific IP addresses that can later be used for attacks
- Nslookup can reveal specific users that can compromise DNS security

Summary

- Using Universal Man-in-the-Middle Phishing Kit, an attack can be launched to import pages from any target Web site