



Hands-On Ethical Hacking and Network Defense

Chapter 4
Footprinting and Social Engineering

Updated 9-27-17

Objectives

- Use Web tools for footprinting
- Conduct competitive intelligence
- Describe DNS zone transfers
- Identify the types of social engineering

Using Web Tools for Footprinting

- “Case the joint”
 - Look over the location
 - Find weakness in security systems
 - Types of locks, alarms
- In computer jargon, this is called footprinting
 - Discover information about
 - The organization
 - Its network

Tool	Function
Google groups (http://groups.google.com)	Search for e-mail addresses in technical or nontechnical newsgroup postings
Whois (www.arin.net or www.whois.net)	Gather IP and domain information
SamSpade (www.samspade.org)	Gather IP and domain information; versions available for UNIX and Windows OSs
Web Data Extractor (www.rafasoft.com)	Extract contact data, such as e-mail, phone, and fax information, from a selected target
FOCA (www.informatica64.com/FOCA)	Extract metadata from documents on Web sites to reveal the document creator's network logon and e-mail address, information on IP addresses of internal devices, and more

Table 4-1 Summary of Web tools

Tool	Function
Necrosoft NScan (www.nscan.org)	Windows scanning, DNS lookup, and advanced Dig tools (see Dig command later in this table)
Google search engine (www.google.com)	Search for Web sites and company data
Namedroppers (www.namedroppers.com)	Run a domain name search; more than 30 million domain names updated daily
White Pages (www.whitepages.com)	Conduct reverse phone number lookups and retrieve address information
Metis (www.severus.org/sacha/metis)	Gather competitive intelligence from Web sites
Dig (command available on all *nix systems; can be downloaded from http://members.shaw.ca/nicholas.fong.dig/ for Windows platforms)	Perform DNS zone transfers; replaces the Nslookup command
Netcat (command available on all *nix systems; can be downloaded from www.securityfocus.com/tools/139 for Windows platforms)	Read and write data to ports over a network
Wget (command available on all *nix systems; can be downloaded from http://gnu.org/software/wget/wget.html for Windows platforms)	Retrieve HTTP, HTTPS, and FTP files over the Internet
Paros (www.parosproxy.org)	Capture Web server information and possible vulnerabilities in a Web site's pages that could allow exploits such as SQL injection and buffer overflow attacks
Maltego (www.paterva.com/web4/index.php/maltego ; also on the book's DVD)	Gather competitive intelligence and represent in graphical form previously unknown relationships between personal identities, companies, and Internet networks

Table 4-1 Summary of Web tools (cont'd.)

Conducting Competitive Intelligence

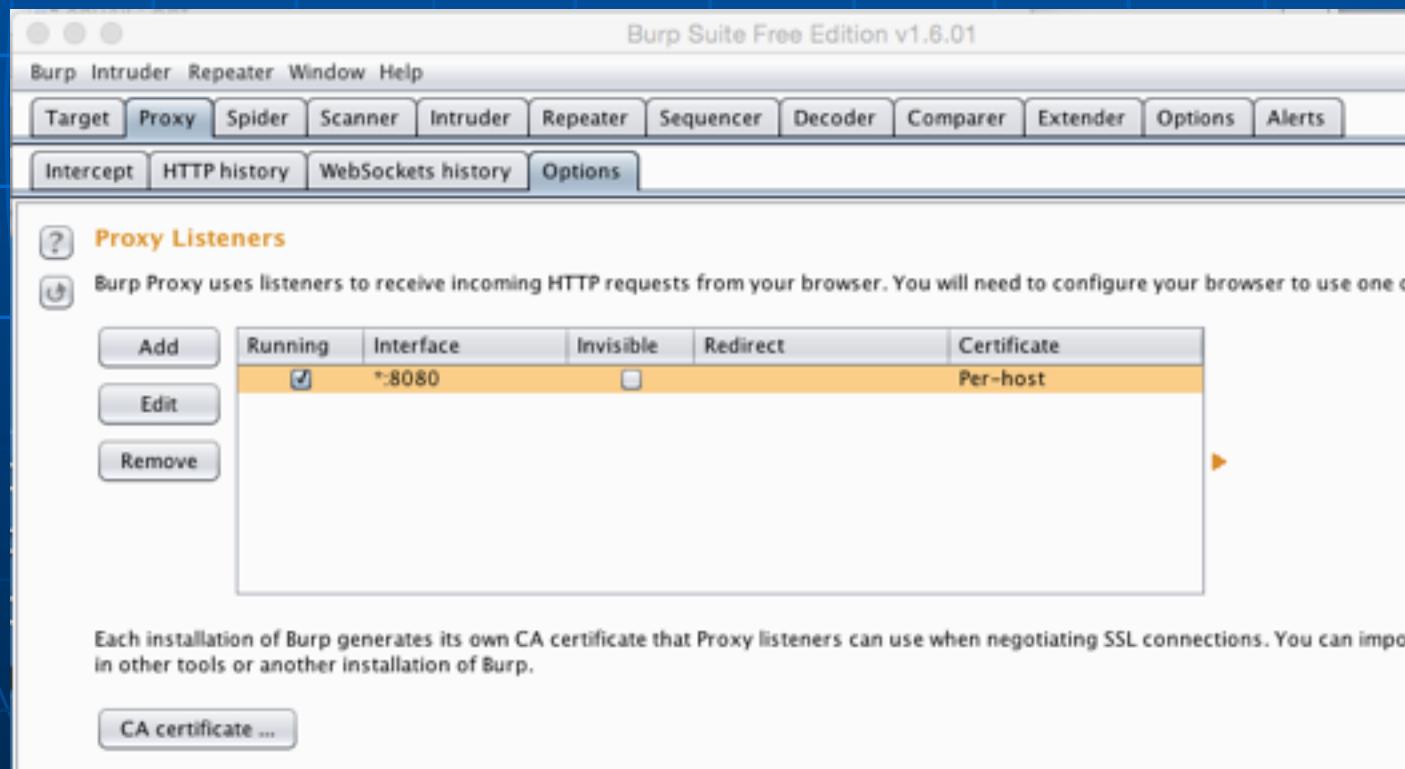
- Numerous resources to find information legally
- Competitive Intelligence
 - Gathering information using technology
- Identify methods others can use to find information about your organization
- Limit amount of information company makes public

Analyzing a Company's Web Site

- Web pages are an easy source of information
- Many tools available
- BurpSuite
 - Powerful proxy for all platforms (uses Java)
 - <https://portswigger.net/burp/>

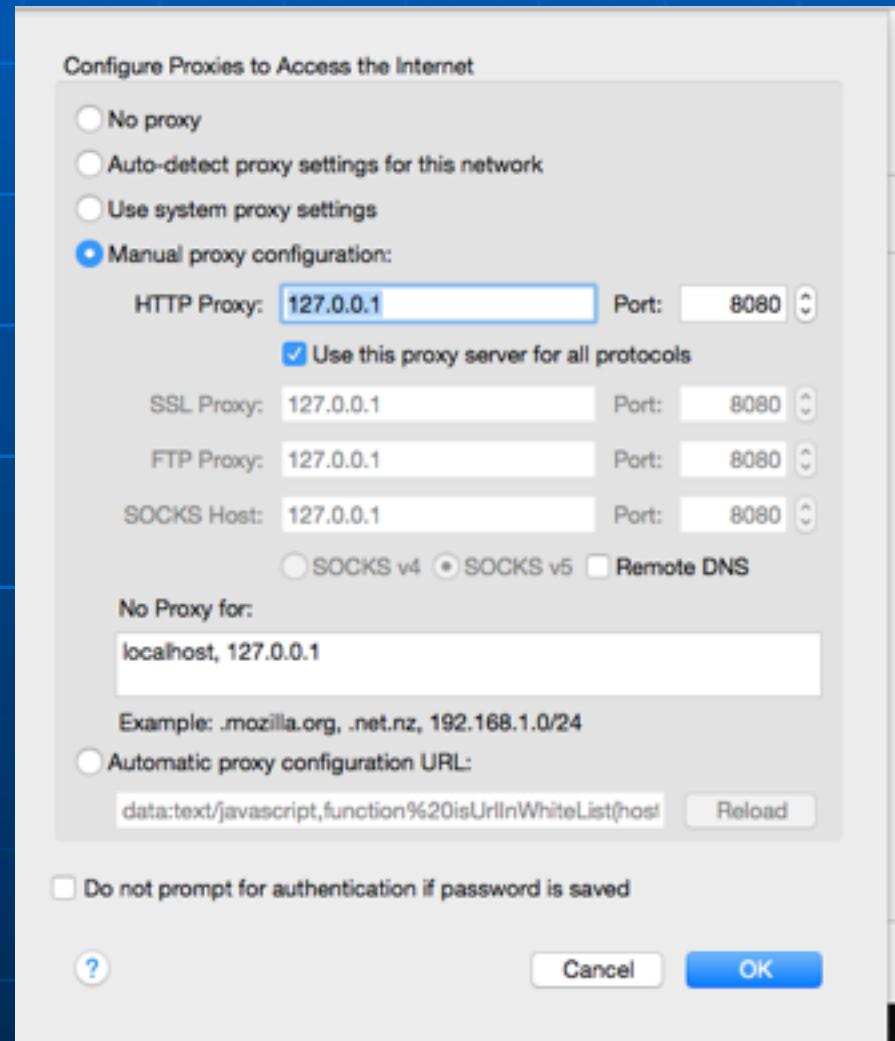
Burp Configuration

- "Proxy" tab, "Intercept" sub-tab
 - Adjust to "Intercept is off"
- "Proxy" tab, "Options" sub-tab
 - Start running on port 8080



Proxy Settings in Firefox

- At top right, click "3 bars" icon, then the Gear icon
- In "Advanced", on the "Network" tab, click "Settings"



Surf an Insecure Site like ietf.org

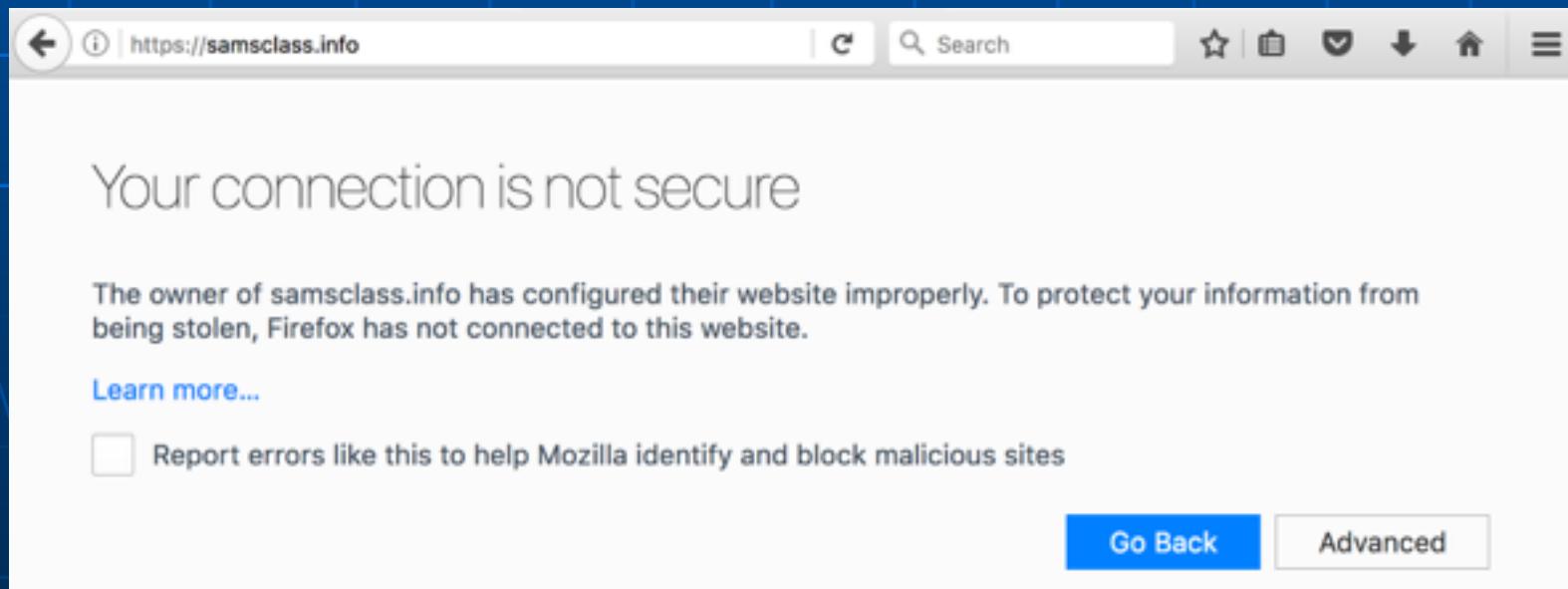
- "HTTP History" tab shows each request and response

The screenshot shows the NetworkMiner interface with the "HTTP history" tab selected. The table displays three network requests:

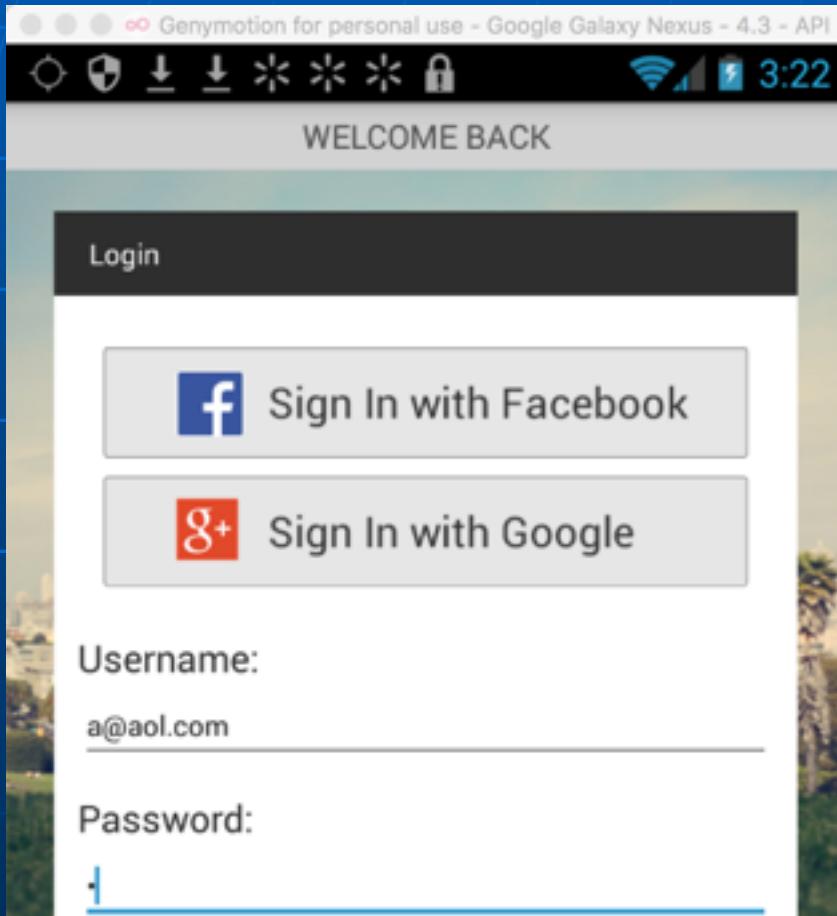
#	Host	Method	URL
1	http://ietf.org	GET	/
2	http://ietf.org	GET	/css/ietf.js
11	http://detectportal.firefox.c...	GET	/success.txt

Surf a Secure Site like samsclass.info

- Browser detects Burp's MITM attack and warns you



Demo: Stitcher



Intercept HTTP history WebSockets history Options

Filter: Showing all items

#	Host	Method	URL
620	https://stitcher.com	GET	/Service/CheckAuthentication.php?

Request Response

Raw Params Headers Hex

GET request to /Service/CheckAuthentication.php

Type	Name	Value
URL	version	4.04
URL	uid	0
URL	os	18
URL	mode	android-Google Galaxy Nexus - 4.3 - A
URL	deviceType	phone
URL	hiRes	1
URL	udid	0000000000000000
URL	androidId	ee854fc116d1238c
URL	timezone	0
URL	connectionType	NONE
URL	markStartup	1
URL	email	test@aol.com
URL	epx	2x2x2x2x2x

Installing the Burp Certificate

- On computer, in Firefox, using the proxy, visit <http://burp>
 - Click the "CA Certificate" link
 - Change file extension to .cer
 - Drag file onto Genymotion phone
- On phone, settings, Security, "Install from SD card"

Demo: Posting a Long Tweet

The screenshot shows a web browser window with a blue grid background. The address bar at the top is secure, indicated by a green lock icon and the URL <https://samsclass.info/124/proj14/longtweet.htm>. Below the address bar, the main content area features a large, bold, black heading: "How to Post Long Tweets". Underneath the heading, there is a paragraph of text: "I got this from @ErrataRob, who got it from @dildog." At the bottom left of the content area, there is another line of text: "Use Chrome.".

How to Post Long Tweets

I got this from @ErrataRob, who got it from @dildog.

Use Chrome.

Other Proxy Functions

- Intercept & Modify Requests
 - Can exploit poorly-made shopping sites
- Spider
 - Finds all the pages in a site
 - Saves a local copy of them
- Scan for vulnerabilities
 - Get authorization first

Other Proxies

- Zed Attack Proxy from OWASP
 - Can scan for vulnerabilities
- Tamper Data
 - Firefox plug-in for easy interception and alteration of requests
- Chrome Developer Tools
 - Click 3-bars, "More Tools", "Developer Tools"
 - Allows you to examine requests and responses

Timeline

- Shows requests & responses even for secure sites

Developer Tools - https://samsclass.info/

Elements Network Sources Timeline Profiles Resources Audits Console EditThisCookie ⚠ 10 > ⚙️ 🖥

Filter Hide data URLs All XHR JS CSS Img Media Font Doc WS Other

Name	Meth...	Status	Type	Initiator	Size	Time	Timeline - Start Time
samsclass.info	GET	200	document	Other	4.9 KB	152 ...	
trophy.png	GET	200	png	(index):103	166 KB	41 ms	
CSAW15LOGO_CO...	GET	200	png	(index):199	6.1 KB	14 ms	
ja.jpg	GET	200	jpeg	(index):209	6.2 KB	75 ms	

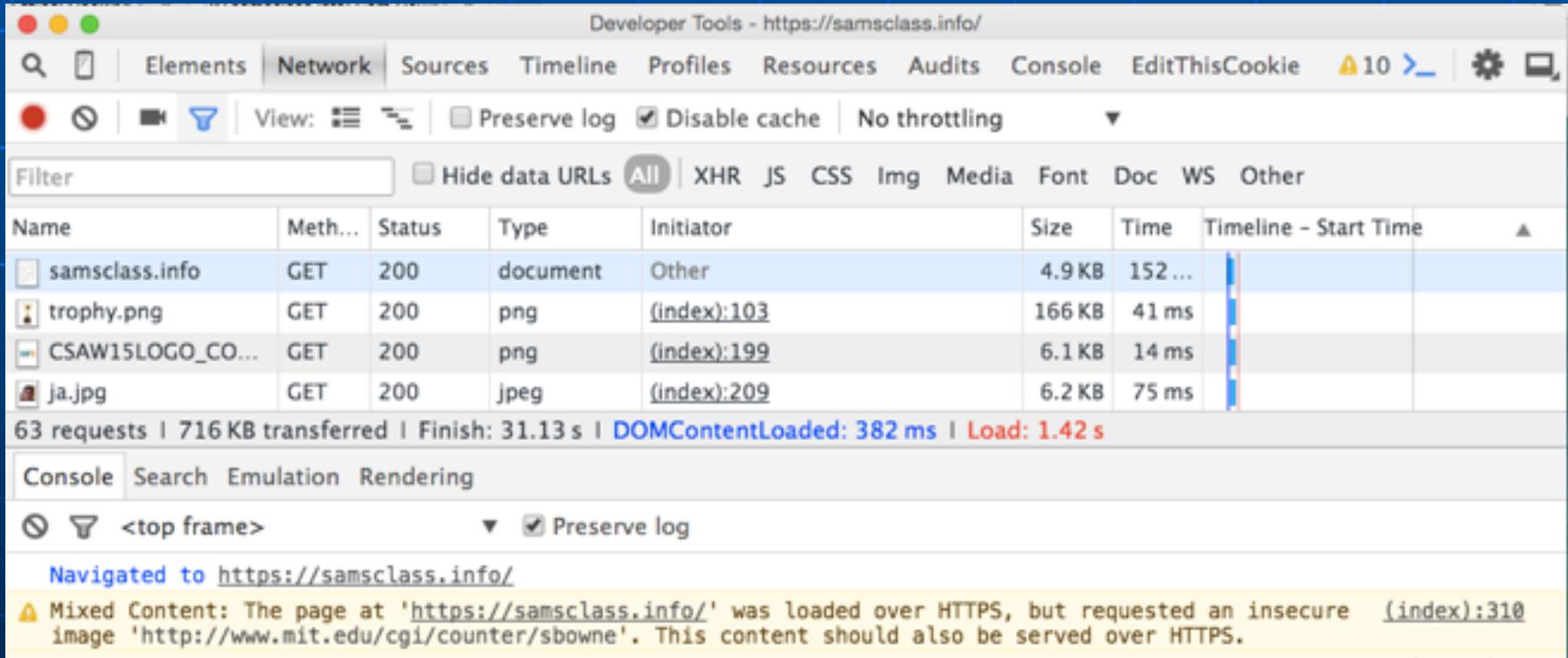
63 requests | 716 KB transferred | Finish: 31.13 s | DOMContentLoaded: 382 ms | Load: 1.42 s

Console Search Emulation Rendering

✖️ ⚡ <top frame> ▾ Preserve log

Navigated to https://samsclass.info/

⚠️ Mixed Content: The page at '<https://samsclass.info/>' was loaded over HTTPS, but requested an insecure image '<http://www.mit.edu/cgi/counter/sbowne>'. This content should also be served over HTTPS. (index):310



Using Other Footprinting Tools

- Whois
 - Commonly used tool
 - Gathers IP address and domain information
 - Attackers can also use it
- Host command
 - Can look up one IP address, or the whole DNS Zone file
 - All the servers in the domain

ARIN Whois from Linux

- host mit.edu
- nc whois.arin.net
- 18.7.22.69
- This shows registration information for the domain

```
yourname@S214-01u:~$ nc whois.arin.net 43
18.7.22.69

OrgName: Massachusetts Institute of Techn
OrgID: MIT-2
Address: Room W92-190
Address: 77 Massachusetts Avenue
City: Cambridge
StateProv: MA
PostalCode: 02139-4307
Country: US

NetRange: 18.0.0.0 - 18.255.255.255
CIDR: 18.0.0.0/8
NetName: MIT
NetHandle: NET-18-0-0-0-1
Parent:
NetType: Direct Assignment
NameServer: STRAWB.MIT.EDU
NameServer: W20NS.MIT.EDU
NameServer: BITSY.MIT.EDU
Comment:
RegDate:
Updated: 1998-09-26

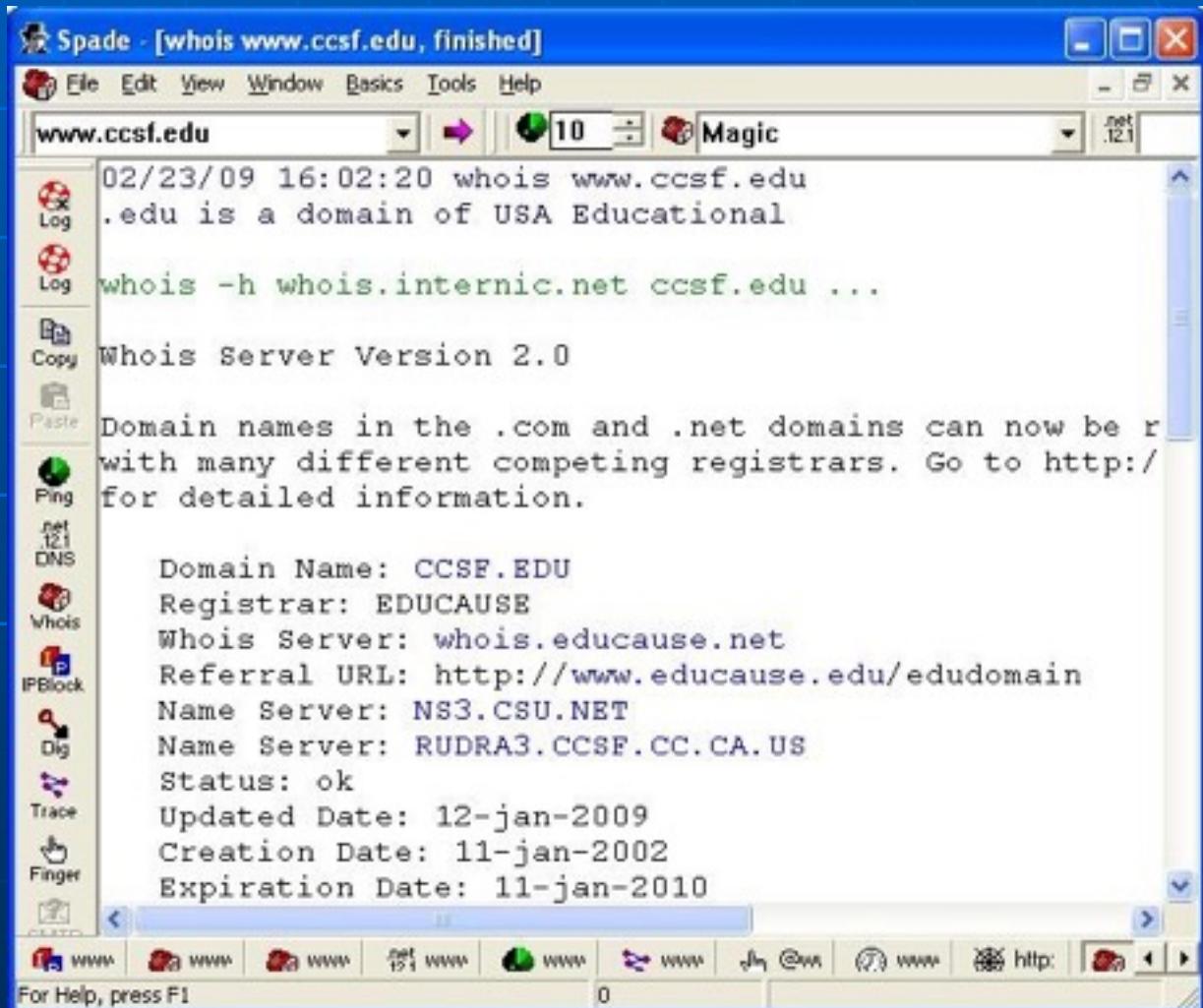
RTechHandle: JIS-ARIN
RTechName: Schiller, Jeffrey
RTechPhone: +1-617-253-8400
RTechEmail: jis@mit.edu

OrgTechHandle: JIS-ARIN
OrgTechName: Schiller, Jeffrey
OrgTechPhone: +1-617-253-8400
OrgTechEmail: jis@mit.edu

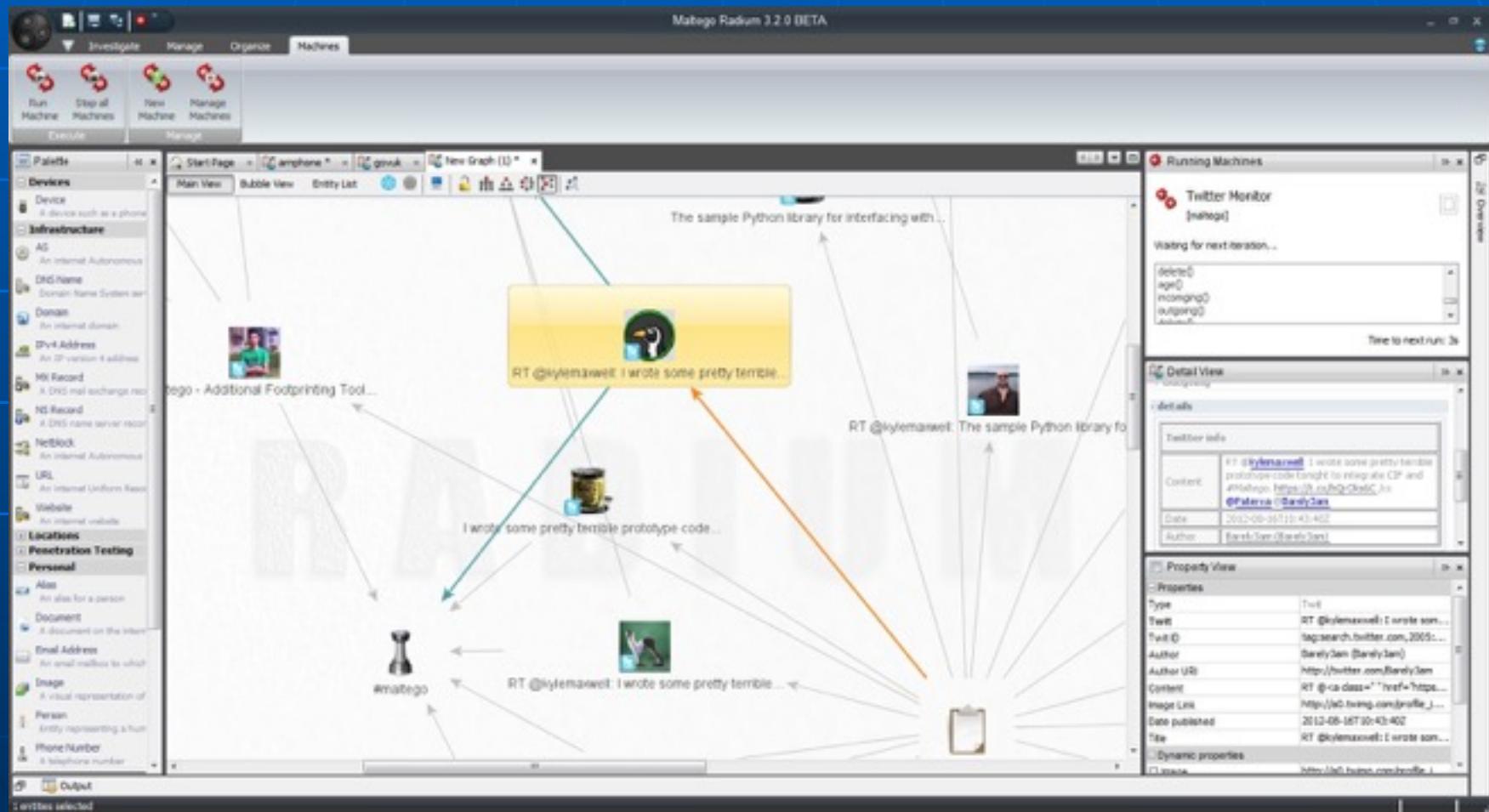
# ARIN WHOIS database, last updated 2007-02-
# Enter ? for additional hints on searching
```

Sam Spade

- GUI tool
- Available for UNIX and Windows
- Easy to use



Maltego



What does Maltego do?

- 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
 - Web sites
 - Internet infrastructure such as:
 - Domains
 - DNS names
 - Netblocks
 - IP addresses
 - Phrases
 - Affiliations
 - Documents and files
- These entities are linked using open source intelligence.
- Maltego is easy and quick to install - it uses Java, so it runs on Windows, Mac and Linux.
- Maltego provides you with a graphical interface that makes seeing these relationships instant and accurate - making it possible to see hidden connections.
- Using the graphical user interface (GUI) you can see relationships easily - even if they are three or four degrees of separation away.
- Maltego is unique because it uses a powerful, flexible framework that makes customizing possible. As such, Maltego can be adapted to your own, unique requirements.

Using E-mail Addresses

- E-mail addresses help you retrieve even more information than the previous commands
- Find e-mail address format
 - Guess other employees' e-mail accounts
- Tool to find corporate employee information
 - *Groups.google.com*

Using HTTP Basics

- HTTP operates on port 80
- Use HTTP language to pull information from a Web server
- Basic understanding of HTTP is beneficial for security testers
- Return codes
 - Reveal information about server OS

Table 4-2 HTTP client errors

Error	Description
400 Bad Request	Request not understood by server
401 Unauthorized	Request requires authentication
402 Payment Required	Reserved for future use
403 Forbidden	Server understands request but refuses to comply
404 Not Found	Unable to match request
405 Method Not Allowed (methods are covered later in this section)	Request not allowed for the resource
406 Not Acceptable	Resource does not accept your request
407 Proxy Authentication Required	Client must authenticate with proxy
408 Request Timeout	Request not made by client in allotted time
409 Conflict	Request could not be completed due to an inconsistency
410 Gone	Resource is no longer available
411 Length Required	Content length not defined
412 Precondition Failed	Request header fields evaluated as false
413 Request Entity Too Large	Request larger than server is able to process
414 Request-URI (Uniform Resource Identifier) Too Long	Request-URI is longer than the server is willing to accept

Table 4-3 HTTP server errors

Error	Description
500 Internal Server Error	Request could not be fulfilled by server
501 Not Implemented	Server does not support request
502 Bad Gateway	Server received invalid response from upstream server
503 Service Unavailable	Server is unavailable due to maintenance or overload
504 Gateway Timeout	Server did not receive a timely response
505 HTTP Version Not Supported	HTTP version not supported by server

Using HTTP Basics (continued)

- HTTP methods
 - GET / HTTP/1.1. is the most basic method
 - Can determine information about server OS from the server's generated output

Table 4-4 HTTP methods

Method	Description
GET	Retrieves data by URI (Uniform Resource Identifier)
HEAD	Same as the GET method, but retrieves only the header information of an HTML document, not the document body
OPTIONS	Requests information on available options
TRACE	Starts a remote application-layer loopback of the request message
CONNECT	Used with a proxy that can dynamically switch to a tunnel connection, such as Secure Socket Layer (SSL)
DELETE	Requests that the origin server delete the identified resource
PUT	Requests that the entity be stored under the Request-URI
POST	Allows data to be posted (that is, sent to a Web server)

Using the OPTIONS Method

```
[Sams-MacBook-Pro-3:platform-tools sambowne$ nc ad.samsclass.info 80
OPTIONS / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 27 Sep 2017 23:28:38 GMT
Server: Apache/2.4.18 (Ubuntu)
Allow: POST,OPTIONS,GET,HEAD
Content-Length: 0
Connection: close
Content-Type: text/html
```

Using the GET Method

```
[Sams-MacBook-Pro-3:platform-tools sambowne$ nc ad.samsclass.info 80
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Wed, 27 Sep 2017 23:29:35 GMT
Server: Apache/2.4.18 (Ubuntu)
Last-Modified: Mon, 03 Apr 2017 15:38:14 GMT
ETag: "c8c-54c44f2891c7d"
Accept-Ranges: bytes
Content-Length: 3212
Vary: Accept-Encoding
Connection: close
Content-Type: text/html

<html>
<head>
<title>Vulnerable Pages</title>
</head>
<body bgcolor= "#009900" text="#33ffff" link="#ffffff"
alink="#33ffcc" vlink="#ffff00" background="teal_leaf.gif">
```

Kahoot!

Other Methods of Gathering Information

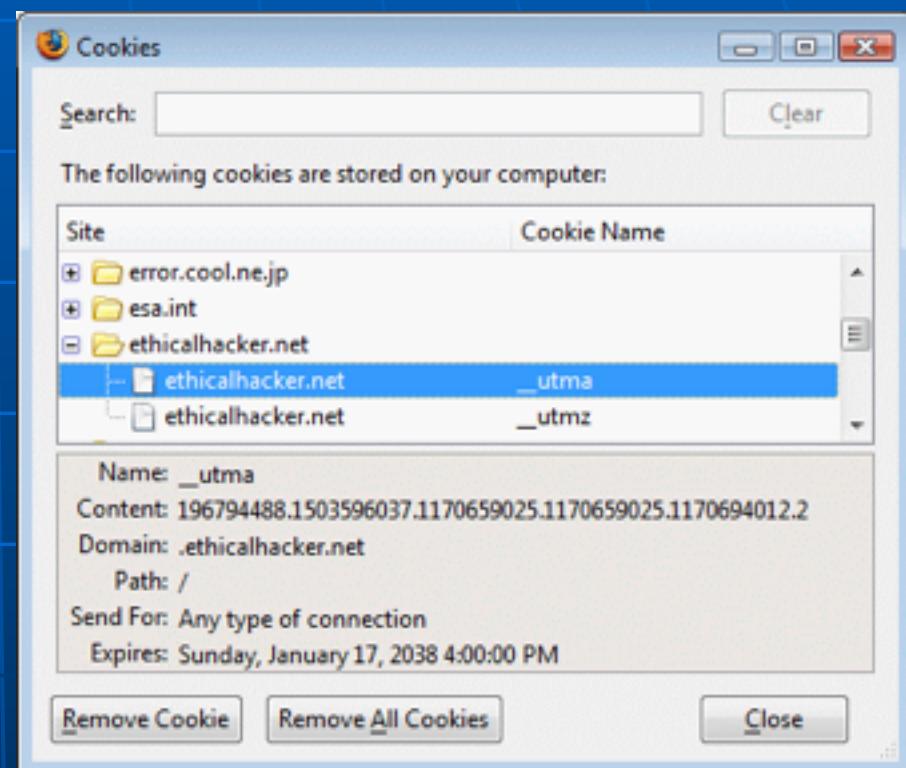
- Cookies
- Web bugs

Detecting Cookies and Web Bugs

- **Cookie**
 - Text file generated by a Web server
 - Stored on a user's browser
 - Information sent back to Web server when user returns
 - Used to customize Web pages
 - Some cookies store personal information
 - Security issue

Viewing Cookies

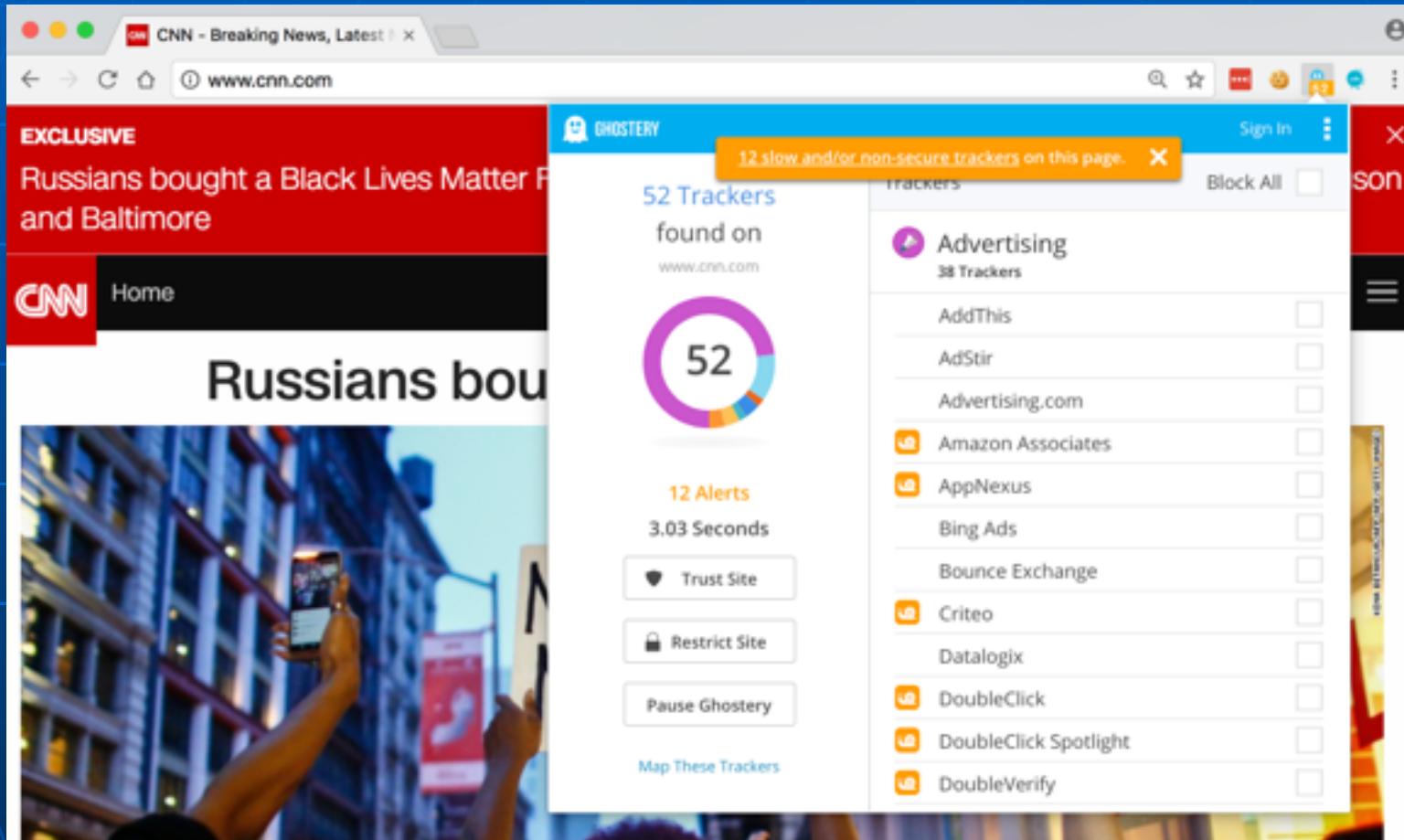
- In Firefox
- Tools, Options
- Privacy tab
- Show Cookies



Detecting Cookies and Web Bugs (continued)

- Web bug
 - 1-pixel x 1-pixel image file (usually transparent)
 - Referenced in an tag
 - Usually works with a cookie
 - Purpose similar to that of spyware and adware
 - Comes from third-party companies specializing in data collection

Ghostery



- Firefox & Chrome extension to reveal Web bugs

Using Domain Name Service (DNS)

Zone Transfers

- DNS
 - Resolves host names to IP addresses
 - People prefer using URLs to IP addresses
- Zone Transfer tools
 - Dig
 - Host

Primary DNS Server

- Determining company's primary DNS server
 - Look for the Start of Authority (SOA) record
 - Shows zones or IP addresses

Using dig to find the SOA

- dig soa mit.edu
- Shows three servers, with IP addresses
- This is a start at mapping the MIT network

```
yourname@S214-0lu:~$ dig soa mit.edu

; <>> DiG 9.3.2 <>> soa mit.edu
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60742
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;mit.edu.                      IN      SOA

;; ANSWER SECTION:
mit.edu.           4539    IN      SOA      BITSY.mit.edu. NETWOR
it.edu. 4349 3600 900 3600000 21600

;; AUTHORITY SECTION:
mit.edu.           4539    IN      NS       STRAWB.mit.edu.
mit.edu.           4539    IN      NS       BITSY.mit.edu.
mit.edu.           4539    IN      NS       W20NS.mit.edu.

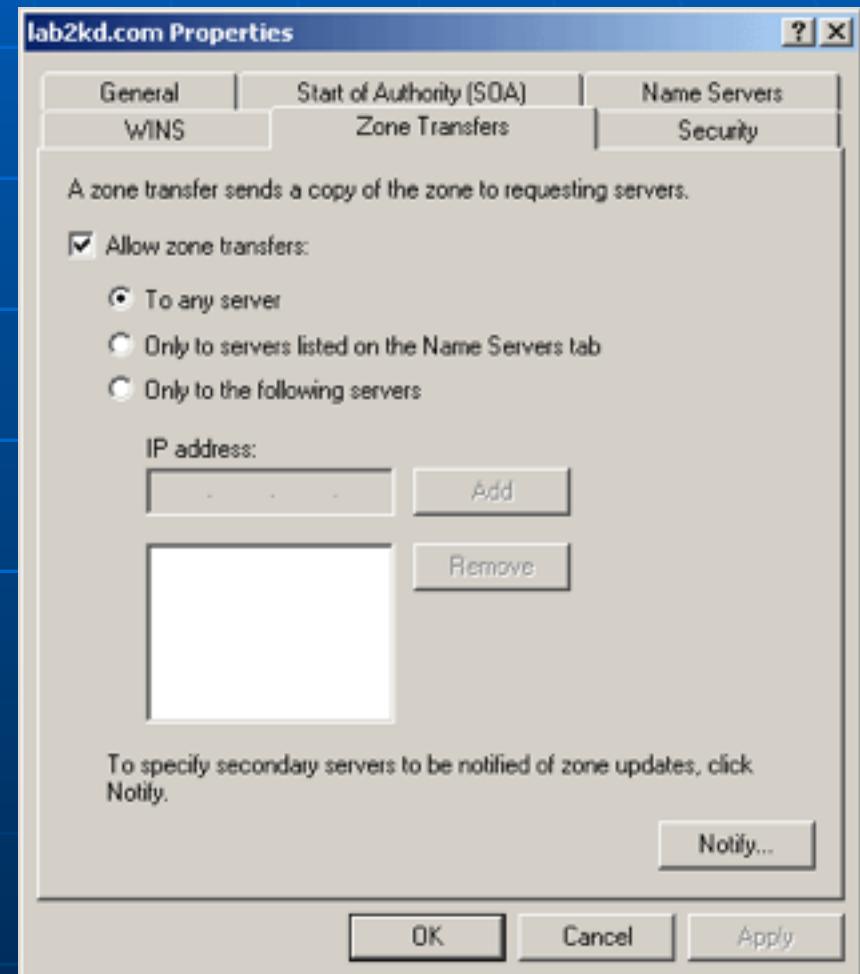
;; ADDITIONAL SECTION:
BITSY.mit.edu.     14362   IN      A        18.72.0.3
W20NS.mit.edu.    16061   IN      A        18.70.0.160
STRAWB.mit.edu.   12793   IN      A        18.71.0.151
```

Using (DNS) Zone Transfers

- Zone Transfer
 - Enables you to see all hosts on a network
 - Gives you organization's network diagram
 - MIT has protected their network – zone transfers no longer work
 - dig @BITSY.mit.edu mit.edu axfr
 - Command fails now

Blocking Zone Transfers

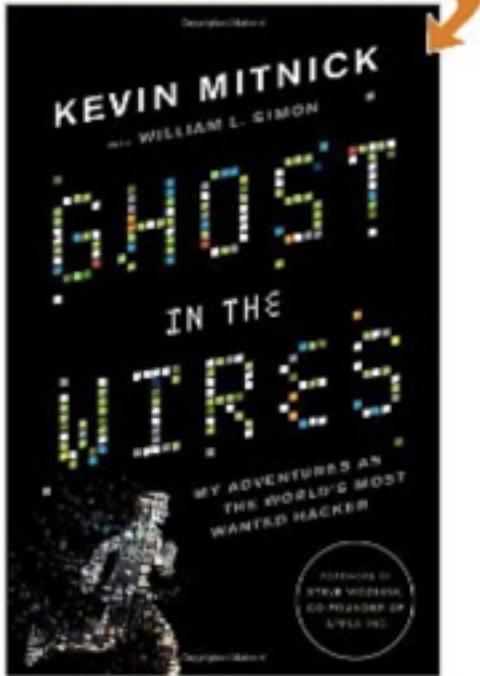
- See link Ch 4e



Introduction to Social Engineering

- Older than computers
- Targets the human component of a network
- Goals
 - Obtain confidential information (passwords)
 - Obtain personal information

[Click to LOOK INSIDE!](#)



Ghost in the Wires: My Adventures as the World's Most Wanted Hacker [Hardcover]

[Kevin Mitnick \(Author\)](#), [Steve Wozniak \(Foreword\)](#), [William L. Simon](#) (Contributor)

(99 customer reviews) | (77)

List Price: \$25.99

Price: **\$15.17** & eligible for **FREE Super Saver Shipping** on orders over \$25. [Details](#)

You Save: **\$10.82 (42%)**

In Stock.

Ships from and sold by **Amazon.com**. Gift-wrap available.

Want it delivered Thursday, September 8? Order it in the next 0 hours and 18 minutes, and choose **One-Day Shipping** at checkout. [Details](#)

[22 new](#) from \$14.79 [9 used](#) from \$16.86

- Link Ch 4!

Mitnick fakes way into LA Telco Central Office

elinormills

10 videos



Subscribe



- Link Ch 4m

HB Gary Federal Hacked

Anonymous speaks: the inside story of the HBGary hack

By Peter Bright | Published 12 months ago



- Link Ch 4n

From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to
88Scr3am3r88 ?
thanks

From: Jussi
To: Greg
Subject: Re: need to ssh into rootkit
hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg
To: Jussi
Subject: Re: need to ssh into rootkit
no i dont have the public ip with me at the moment because im ready
for a small meeting and im in a rush.
if anything just reset my password to changeme123 and give me publi-
ip and ill ssh in and reset my pw.

Tactics

- Persuasion
- Intimidation
- Coercion
- Extortion/blackmailing

Introduction to Social Engineering (continued)

- The biggest security threat to networks
- Most difficult to protect against
- Main idea:
 - “Why to crack a password when you can simply ask for it?”
 - Users divulge their passwords to IT personnel

Social Engineer Studies Human Behavior

- Recognize personality traits
- Understand how to read body language

Introduction to Social Engineering (continued)

- Techniques
 - Urgency
 - Quid pro quo
 - Status quo
 - Kindness
 - Position

Preventing Social Engineering

- Train user not to reveal any information to outsiders
- Verify caller identity
 - Ask questions
 - Call back to confirm
- Security drills

OSSTMM Social Engineering Template

Company	
Company Name	
Company Address	
Company Telephone	
Company Fax	
Company Web Page	
Products and Services	
Primary Contacts	
Departments and Responsibilities	
Company Facilities Location	
Company History	
Partners	
Resellers	
Company Regulations	
Company Info Security Policy	
Company Traditions	
Company Job Postings	
Temporary Employment Availability	
Typical IT Threats	

People	
Employee Information	
Employee Names and Positions	
Employee Place in Hierarchy	
Employee Personal Pages	
Employee Best Contact Methods	
Employee Hobbies	
Employee Internet Traces (SENET, Forums)	
Employee Opinions Expressed	
Employee Friends and Relatives	
Employee History (Including Work History)	
Employee Character Traits	
Employee Values and Priorities	
Employee Social Habits	
Employee Speech and Speaking Patterns	
Employee Gestures and Manners	

Figure 4-17 Social Engineering Template

OSSTMM Social Engineering Telephone Attack Template

Attack Scenario	
Telephone #	
Person	
Description	
Results	

Figure 4-18 Social Engineering Telephone Attack Template

DEF CON Social Engineering Contest

Only 5 (all women) of 135 pass Defcon social engineering test

Contest results will be published next week, organizers say

By [Robert McMillan](#), IDG News Service

September 03, 2010 03:40 AM ET



Share/Email



Tweet This



Comment



Print



Newsletter Sign-Up

Of the 135 Fortune 500 employees targeted by social engineering hackers in a recent contest only five of them refused to give up any corporate information whatsoever. And guess what? All five were women.

- Link Ch 4k

The Art of Shoulder Surfing

- Shoulder surfer
 - Reads what users enter on keyboards
 - Logon names
 - Passwords
 - PINs

Tools for Shoulder Surfing

- Binoculars or telescopes or cameras in cell phones
- Knowledge of key positions and typing techniques
- Knowledge of popular letter substitutions
 - s equals \$, a equals @

The Art of Shoulder Surfing (continued)

- Prevention
 - Avoid typing when someone is nearby
 - Avoid typing when someone nearby is talking on cell phone
 - Computer monitors should face away from door or cubicle entryway
 - Immediately change password if you suspect someone is observing you

Dumpster Diving

- Attacker finds information in victim's trash
 - Discarded computer manuals
 - Notes or passwords written in them
 - Telephone directories
 - Calendars with schedules
 - Financial reports
 - Interoffice memos
 - Company policy
 - Utility bills
 - Resumes of employees

The Art of Dumpster Diving (continued)

- Prevention
 - Educate your users about dumpster diving
 - Proper trash disposal
 - Use “disk shredder” software to erase disks before discarding them
 - Software writes random bits
 - Done at least seven times
 - Discard computer manuals offsite
 - Shred documents before disposal

Piggybacking

- Trailing closely behind an employee cleared to enter restricted areas
- How it works:
 - Watch authorized personnel enter an area
 - Quickly join them at security entrance
 - Exploit the desire of other to be polite and helpful
 - Attacker wears a fake badge or security card

Piggybacking Prevention

- Use turnstiles
- Train personnel to notify the presence of strangers
- Do not hold secured doors for anyone
 - Even for people you know
- All employees must use secure cards

Phishing

- Deceptive emails or text messages
- Can take money, passwords, or install malware on your computer

PLEASE HELP. Spam | X

My name is Stephney Zizi to me [show details](#) Feb 12 [Reply](#) ▾

My name is Stephney Zizi, I am seeking for a help, My parents with my two younger once was involved in the earth quake that happened in my country Haiti and I thank God that I was in school when the earth quake happened in my country Haiti.

Please dear sir/madam I need your help as a girl of 21 years old I can not do anything to help my fathers fund that was deposited in a Bank so I wish to present you as the family member so that you can have the deposited fund to claim from the Bank which I will make available the information of my fathers Attorney so he can put you through on what to do to claim the fund.

Kahoot!