OSINT, CYBERSTALKING, FOOTPRINTING AND RECON: GETTING TO KNOW YOU

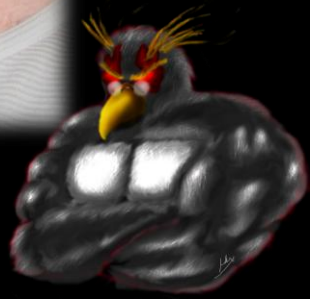
Adrian Crenshaw

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything - I'm just a geek with time on my hands
- (ir)Regular on the ISDPodcast
  http://www.isd-podcast.com/

Sometimes my presentations are like this.

And sometimes my presentations are like this.



Class Structure

- Mile wide, 2.5 feet deep
- Feel free to ask questions at any time
- There will (hopefully) be many long breaks to play with the tools mentioned
- I'll try not to drop anyone's docs but my own, but volunteers for "victims" will help

So, what info is out there?

Other names and related concepts:

- OSInt (Open Source Intelligence)
- Scoping
- Footprinting
- Discovery
- Recon
- Cyberstalking

Subtopics

- DNS, Whois and Domain Tools
- Finding general Information about an organization via the web
- Anti-social networks
- Google Hacking
- Metadata
- Other odds and ends

Why?

For Pen-testers and attackers:

- Precursor to attack
- Social Engineering
- Disgruntled Employees
- User names and passwords
- Web vulnerabilities
- Internal IT structure (software, servers, IP layout)
- Spearphishing

For everyone else:

- You want to keep attackers from finding this info and using this against you. ☺

Dropping Docs

- All these techniques are legal as far as I know, but IANAL
- Sorry if I “drop someone’s docs” other than my own
- Please don’t misuse this information

Backtrack 5

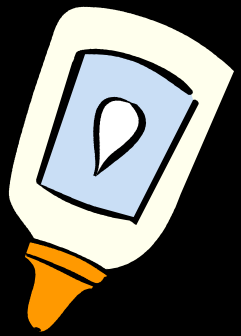
- Tons of fun tools to play with http://www.backtrack-linux.org/
- Username: root
  Password: toor
- Many of the DNS tools are in /pentest/enumeration/dns/

DNS, WHOIS AND DOMAIN TOOLS

Who-do the voodoo that you do so well

DNS

- Glue of the Internet
- Think of it as a phone book of sorts
- Maps names to IPs, and IPs to names (and other odds and ends)
- Organization information is also kept



www.irongeek.com 69.163.177.249

Simple DNS Lookups

- Host name to IP lookup:
  nslookup www.irongeek.com

- Reverse lookup:
  nslookup 208.97.169.250

DNS Record Types

Just a few record types cribbed from: http://en.wikipedia.org/wiki/List_of_DNS_record_types

Code	Number	Defining RFC	Description	Function
A	1	RFC 1035	**address record**	Returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host, but also used for DNSBLs, storing subnet masks in RFC 1101, etc.
AAAA	28	RFC 3596	**IPv6 address record**	Returns a 128-bit IPv6 address, most commonly used to map hostnames to an IP address of the host.
MX	15	RFC 1035	mail exchange record	Maps a domain name to a list of mail exchange servers for that domain
CNAME	5	RFC 1035	**Canonical name record**	Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name.
PTR	12	RFC 1035	**pointer record**	Pointer to a canonical name. Unlike a CNAME, DNS processing does *NOT* proceed, just the name is returned. The most common use is for implementing reverse DNS lookups, but other uses include such things as DNS-SD.
AXFR	252	RFC 1035	**Full Zone Transfer**	Transfer entire zone file from the master name server to secondary name servers.

Getting a list of host names

- Zonetransfers
- Bruteforcing from a dictionary
- Nmap –sL <some-IP-range>

DIGing for data

dig irongeek.com any

dig @ns1.dreamhost.com irongeek.com any

Zone Transfer:Give me all your records!

Zone Transfer: NSLOOKUP

(Windows version)

```
C:\Documents and Settings\Adrian>nslookup
Default Server:  resolver1.opendns.com
Address:  208.67.222.222

> set type=ns
> irongeek.com
Server:  resolver1.opendns.com
Address:  208.67.222.222

Non-authoritative answer:
irongeek.com    nameserver = ns1.dreamhost.com
irongeek.com    nameserver = ns2.dreamhost.com
irongeek.com    nameserver = ns3.dreamhost.com
> server ns1.dreamhost.com
Default Server:  ns1.dreamhost.com
Address:  66.33.206.206

> ls irongeek.com
[ns1.dreamhost.com]
*** Can't list domain irongeek.com: Query refused
> exit
```

Zone Transfer: Can you DIG it?

- Domain Internet Groper
  dig ugent.be ns
  dig @ugdns1.ugent.be ugent.be axfr

Zone Transfer: Others

- Other tools in BackTrack
  ./dnsrecon.py -d ugent.be –x
  ./dnsenum.pl ugent.be

- ServerSniff:
  http://serversniff.net/nsreport.php
  http://serversniff.net/content.php?do=subdomains

- GUI Dig for Windows
  http://nscan.org/dig.html

Bruteforcing

- Fierce
  http://ha.ckers.org/fierce/
  ./fierce.pl -threads 100 -dns irongeek.com
  ./fierce.pl -dns irongeek.com -wordlist dictionary.txt

Nmap Demo

nmap -sL <some-IP-range>
nmap -sL 192.0.32.1-10

Whois: Whooo, are you? Who-who-who-who.

- Great for troubleshooting, bad for privacy
- Who owns a domain name or IP
- E-mail contacts
- Physical addresses
- Name server
- IP ranges

- Who is by proxy?

Whois Demo

apt-get install whois

whois example.com

whois 208.97.169.250

Whois Tools

*nix Command line

Nirsoft's

http://www.nirsoft.net/utils/whois_this_domain.html

http://www.nirsoft.net/utils/ipnetinfo.html

Pretty much any network tools collection

Whois and domain tools sites

- RobTex
  http://www.robtex.com

- ServerSniff
  http://www.serversniff.net

Traceroute

(ok, not really a DNS tool, but I was too lazy to make another section)

- Windows (ICMP):
  tracert irongeek.com

- *nix (UDP by default, change with –I or -T):
  traceroute irongeek.com

- Just for fun:
  http://www.nabber.org/projects/geotrace/

FINDING GENERAL INFORMATION ABOUT AN ORGANIZATION VIA THE WEB

So, you have a job posting for an
Ethical Hacker huh?

Sites about the organization

- The organization's website (duh!)
- Corp Info
  http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines#Corporate
- Wayback Machine
  http://www.archive.org
- Monster (and other job sites)
  http://www.monster.com/
- Zoominfo
  http://www.zoominfo.com/
- Google Groups (News groups, Google Groups and forums)
  http://groups.google.com/
- Boards
  http://boardreader.com
  http://omgili.com
  http://groups.google.com
- LinkedIn
  http://www.linkedin.com/

ANTI-SOCIAL NETWORKS

It’s all about how this links to that links to some other thing…

Let's get to know Ester

- Fake profile I made up to use for class
- Dropped some Dox at a few places
- May sound creepy, but you can practice with names from dating sites
- Remember what you learned from 4chan:

RULE 30

There are no girls on the internet.

Cyberstalking Sites

Large list at:

- http://www.irongeek.com/i.php?page=security/doxing-footprinting-cyberstalking

Useful:

- http://com.lullar.com
- http://www.peekyou.com
- http://www.checkusernames.com / http://knowem.com
- http://www.isearch.com
- http://www.whitepages.com

Not quite related, but cool:

- http://tineye.com
- http://pipes.yahoo.com/pipes/

Crap:

- Most of them

Other

General

- http://youropenbook.org

Geolocation

- http://www.bing.com/maps
- http://twittermap.appspot.com
- http://www.fourwhere.com/
- http://icanstalku.com
- http://ip2geolocation.com

Neighbors

- http://www.whitepages.com/find_neighbors

Tools

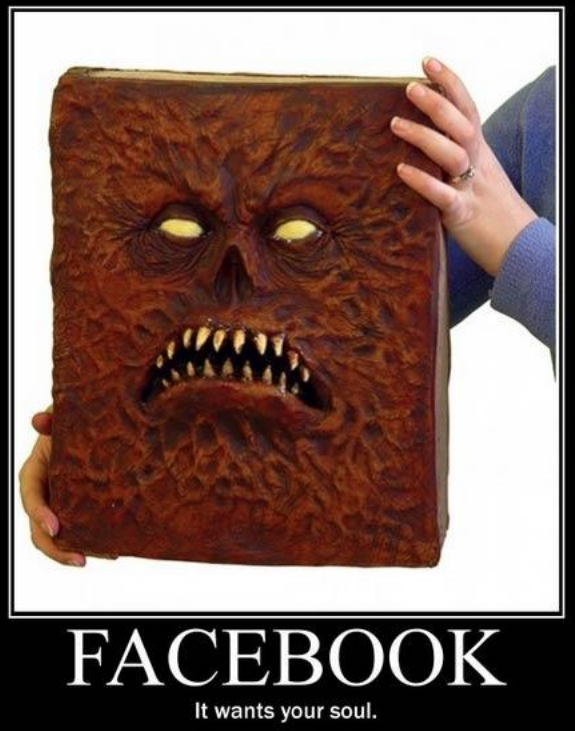
- Maltego
  http://www.paterva.com/web5/
- See differences:
  http://www.paterva.com/web5/client/difference.php
- Covers a large cross section of what this class is about

Story Time

- George Bronk
- Found info on women's Facebook profiles
- Used information to answer security question at mail providers
- Found nudes
- Posted some, sent them to contacts lists, asked for more

To be social or anti-social

- Should you have a profile?
- What if you don’t?
- Impersonators
- Robin Sage (by Thomas Ryan)
  - Get in peoples friends list to probe their connections



GOOGLE HACKING

More than just turning off safe search
(though that's fun too)

So, do you really know what's shared online about your organization?

- PII (Personally identifiable information)
- Email address
- User names
- Vulnerable web services
- Web based admin interfaces for hardware
- Much more……..
- YOU HAVE TO USE YOUR IMAGINATION

Google Advance Operators

Operators	Description
site:	Restrict results to only one domain, or server
inurl:/allinurl:	All terms must appear in URL
intitle:/allintitle:	All terms must appear in title
cache:	Display Google's cache of a page
ext:/filetype:	Return files with a given extension/file type
info:	Convenient way to get to other information about a page
link:	Find pages that link to the given page
inanchor:	Page is linked to by someone using the term

http://www.googleguide.com/advanced_operators.html

More Operators

Operators	Description
-	Inverse search operator (hide results)
~	synonyms
[#]..[#]	Number range
*	Wildcard to put something between something when searching with “quotes”
+	Used to force stop words
OR	Boolean operator, must be uppercase
|	Same as OR

General Examples

- inurl:nph-proxy site:edu
- intitle:index.of.etc
- intitle:index.of site:irongeek.com
- filetype:pptx site:irongeek.com
- "vnc desktop" inurl:5800
- adrian crenshaw -site:irongeek.com

More General Examples

- SSN filetype:xls | filetype:xlsx
- "dig @* * axfr”
- inurl:admin
- inurl:indexFrame.shtml Axis
- inurl:hp/device/this.LCDispatcher
- “192.168.*.*” (but replace with your IP range)

Facebook Images

195608_100002238375103_5292346_n.jpg

inurl:100002238375103

Google Hacking For People

- inurl:ester.pent
- inurl:ester1337
- intitle:ester1337
- inurl:user inurl:irongeek -site:irongeek.com
- inurl:account "irongeek“
- site:facebook.com inurl:group (ISSA | Information Systems Security Association)
- site:linkedin.com inurl:company (NSA | National Security Agency)

Google Hacking DB

- Exploit DB Google Dorks
  http://www.exploit-db.com/google-dorks/

- Old School
  http://www.hackersforcharity.org/ghdb/

Google Hacking Tools

- Metagoofil
  http://www.edge-security.com/metagoofil.php
- The Harvester
  ./theHarvester.py -d irongeek.com -l 100 -b google
- Online Google Hacking Tool
  http://www.secapps.com/a/ghdb
- Spiderfoot
  http://www.binarypool.com/spiderfoot/
- Goolag
  http://goolag.org

More Google Hacking Tools

- Gooscan
  Should be on BackTrack CD/VM
- Wikto
  http://www.sensepost.com/research/wikto/
- SiteDigger
  http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx
- BiLE
  http://www.sensepost.com/research_misc.html
- MSNPawn
  http://www.net-square.com/msnpawn/index.shtml

Google APIs and proxies

- JSON/Atom
  http://code.google.com/apis/customsearch/v1/overview.html
- Old
  http://code.google.com/apis/websearch/
- Really Old SOAP:
- EvilAPI
  http://evilapi.com/ (defunct?)
- Spud
  http://www.sensepost.com/labs/tools/pentest/spud
- I can Haz API keyz?
  https://github.com/search

METADATA

Data about data

Pwned by Metadata

Cat Schwartz
Is that an unintended thumbnail in your EXIF data, or are you just happy to see me?

Dennis Rader (BTK Killer)
Metadata in a Word DOC he sent to police had the name of his church, and last modified by “Dennis” in it.

Darkanaku/Nephew chan
A user on 4chan posts a pic of his semi-nude aunt taken with an iPhone, Anonymous pulls the EXIF GPS info from the file and hilarity ensues.
More details can be on the following VNSFW site:
~~http://encyclopediadramatica.com/User:Darkanaku/Nephew_chan~~
http://web.archive.org/web/20090608214029/http://encyclopediadramatica.com/User:Darkanaku/Nephew_chan

Examples of file types that contain metadata

MAC addresses, user names, edits, GPS info. It all depends on the file format.

- JPG
  EXIF (Exchangeable image file format)
  IPTC (International Press Telecommunications Council)
- PDF
- DOC
- DOCX
- EXE
- XLS
- XLSX
- PNG
- Too many to name them all.

Metadata Tools

- Strings
- FOCA (use compatibility mode if needed)
  http://www.informatica64.com/DownloadFOCA/
- Metagoofil
  http://www.edge-security.com/metagoofil.php
- EXIF Tool
  http://www.sno.phy.queensu.ca/~phil/exiftool/
- EXIF Viewer Plugin
  https://addons.mozilla.org/en-US/firefox/addon/3905
- Jeffrey's Exif Viewer
  http://regex.info/exif.cgi

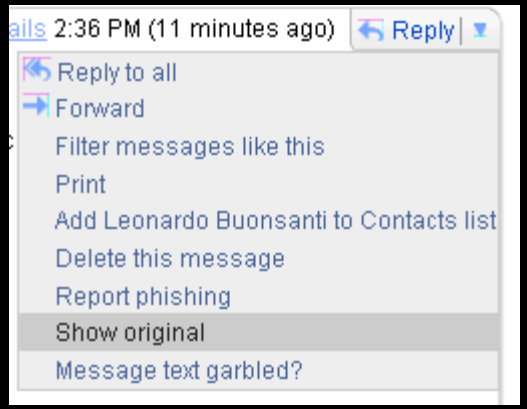
Metadata Tools

- EXIF Reader
  http://www.takenet.or.jp/~ryuuji/minisoft/exifread/english/
- Flickramio
  http://userscripts.org/scripts/show/27101
- Cree.py
  http://ilektrojohn.github.com/creepy/
- Pauldotcom
  http://www.google.com/search?hl=en&q=metadata+site%3Apauldotcom.com&btnG=Search

OTHER ODDS AND ENDS

Stuff that does not quite fit anywhere else

Off with their Headers



http://www.irongeek.com/i.php?page=security/how-to-cyberstalk-potential-employers

Also let us not forget HTTP headers

HTTP/1.1 200 OK
Content-Type: text/javascript; charset=UTF-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Wed, 18 May 2011 15:34:03 GMT
Content-Encoding: gzip
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Content-Length: 1269
Server: GSE

LiveHeaders Plugin

http://www.shodanhq.com/

https://panopticlick.eff.org/

Robots.txt

http://www.irongeek.com/robots.txt

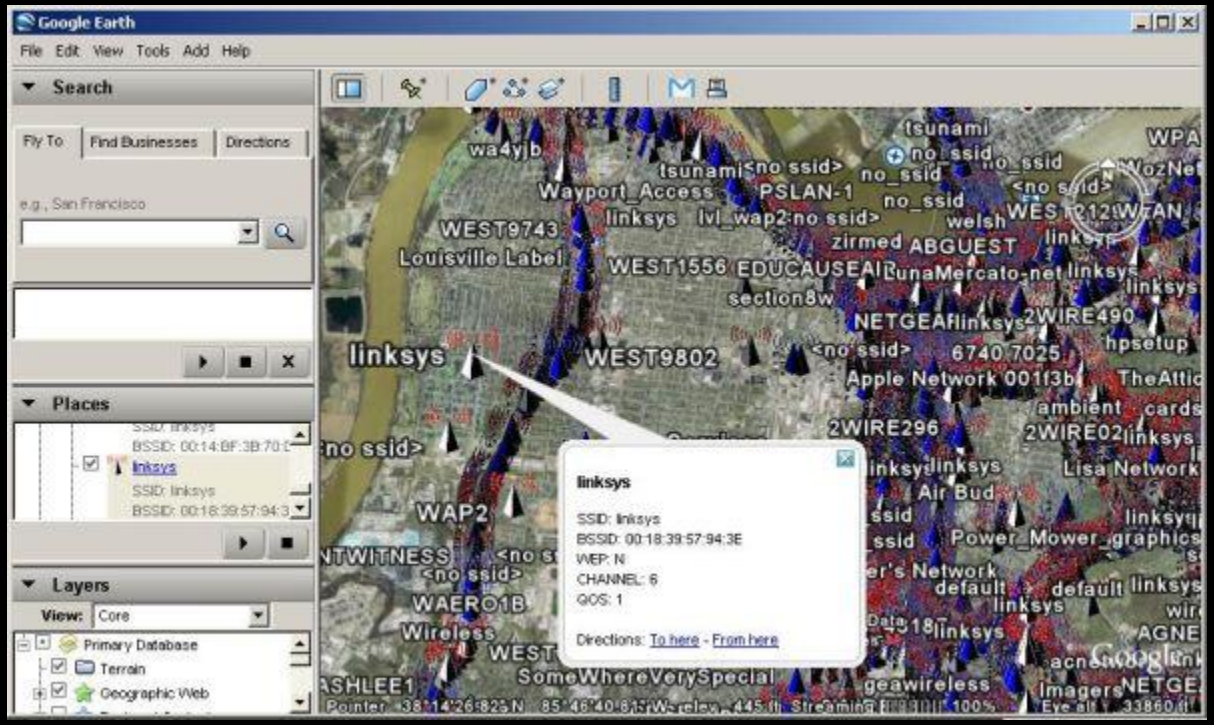
User-agent: *

Disallow: /private

Disallow: /secret

THIS IS MY ROBOTS.TXT FILE. FOR THE LOVE OF CTHULHU, DON'T GO THERE!

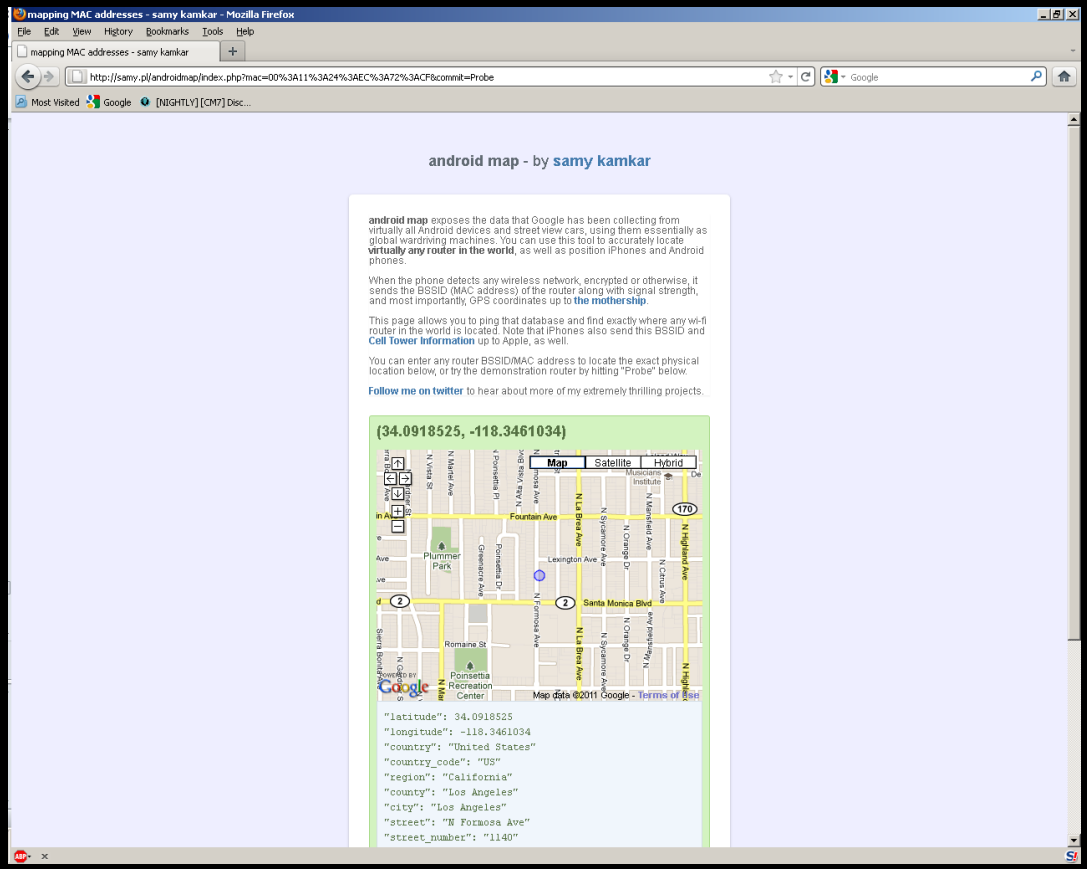
IGiGLE and WiGLE



http://www.irongeek.com/i.php?page=security/igigle-wigle-wifi-to-google-earth-client-for-wardrive-mapping

Android Location?

- http://samy.pl/androidmap



More Links

- Links for Doxing, Personal OSInt, Profiling, Footprinting, Cyberstalking
  http://www.irongeek.com/i.php?page=security/doxing-footprinting-cyberstalking

- PTES Technical Guidelines
  http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

- VulnerabilityAssessment.co.uk - An information portal for Vulnerability Analysts and Penetration Testers
  http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html

Videos/Talks/Presentations

- Social Zombies - Kevin Johnson and Tom Eston
  http://www.youtube.com/watch?v=l79q2G3E8HY
  http://www.youtube.com/view_play_list?p=C591646E9B0CF33B
  http://vimeo.com/18827316

- Satan is on my Friends List - Shawn Moyer and Nathan Hamiel
  http://www.youtube.com/watch?v=asj8yzXihcc

- Using Social Networks To Profile, Find and 0wn Your Victims - Dave Marcus
  http://www.irongeek.com/i.php?page=videos/dojocon-2010-videos#Using%20Social%20Networks%20To%20Profile,%20Find%20and%200wn%20Your%20Victims

Events

- DerbyCon 2011, Louisville Ky
  Sept 30 - Oct 2
  http://derbycon.com/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Other Cons:
  http://www.skydogcon.com/
  http://www.dojocon.org/
  http://www.hack3rcon.org/
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

QUESTIONS?

42