FOOTPRINTING, SCOPING AND RECON WITH DNS, GOOGLE AND METADATA

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

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 be many long breaks to play with the tools mentioned

So, what info is out there?

Other names:

- 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
- 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
- Sorry if I “drop someone’s docs” other than my own
- Please don’t misuse this information

Backtrack 4 Prep

Enable the interface:

ifconfig eth0 up

Get an IP:

dhclient

Start up the GUI/WIMP:

startx

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

Simple DNS Lookups

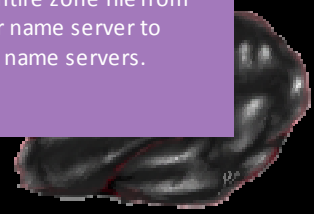
- Host name to IP lookup:
  nslookup www.irongeek.com

- 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
- Nmap –sL <some-IP-range>
- Serversniff
  http://serversniff.net/subdomains.php

DIGing for data

dig irongeek.com any

dig @ns1.dreamhost.com irongeek.com any

Zone Transfer:Give me all your records!

http://Irongeek.com

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?

dig issa-kentuckiana.org ns

dig @dns3.doteasy.com issa-kentuckiana.org axfr

dig louisvilleinfosec.com ns

dig @dns3.doteasy.com louisvilleinfosec.com axfr

dig ugent.be ns

dig @ugdns1.ugent.be ugent.be axfr

Zone Transfer: Others

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

- Fierce
  http://ha.ckers.org/fierce/
  ./fierce.pl -dns irongeek.com

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

Nmap Demo

nmap –sL <some-IP-range>

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

whois irongeek.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

Windows Mobile:

http://www.cam.com/vxutil_pers.html

Whois and domain tools sites

- http://www.domaintools.com/
- http://samspade.org
- 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?

http://Irongeek.com

Sites about the organization

- The organization's website (duh!)
- 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/
- Board reader
  http://boardreader.com
- LinkedIn
  http://www.linkedin.com/

ANTI-SOCIAL NETWORKS

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

http://Irongeek.com

Cyberstalking Sites

Useful:

- http://www.pipl.com
- http://www.peekyou.com
- http://yoname.com

Not quite related, but cool:

- http://tineye.com

Crap:

- http://www.spock.com
- http://wink.com
- http://Rapleaf.com (not very useful anymore)

Tools

- Maltego
  http://www.paterva.com/maltego/community-edition/

- Covers a large cross section of what this presentation is about.

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

Examples

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

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)

Google Hacking DB

- http://johnny.ihackstuff.com/ghdb.php

Google Hacking Tools

- Metagoofil
  ./metagoofil.py -d irongeek.com -l 1000 -f all -0 output.html -t temp

- 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.foundstone.com/us/resources/proddesc/sitedigger.htm
- BiLE
  http://www.sensepost.com/research_misc.html
- MSNPawn
  http://www.net-square.com/msnpawn/index.shtml

Google SOAP API Proxys

- EvilAPI
  http://evilapi.com/ (defunct?)

- Aura
  http://www.sensepost.com/research/aura/

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://Irongeek.com

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
- 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

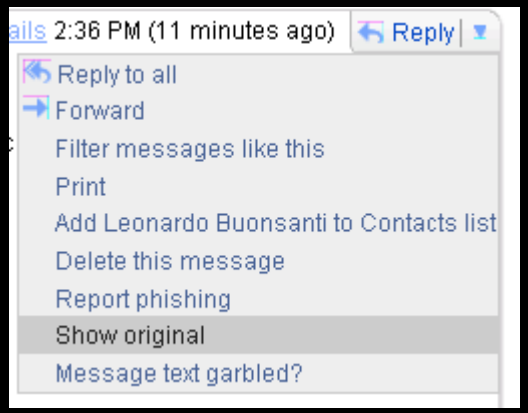
Metadata Tools

- EXIF Reader
  http://www.takenet.or.jp/~ryuuji/minisoft/exifread/english/
- Flickramio
  http://userscripts.org/scripts/show/27101
- 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

Mail Header Fun



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

Robots.txt

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

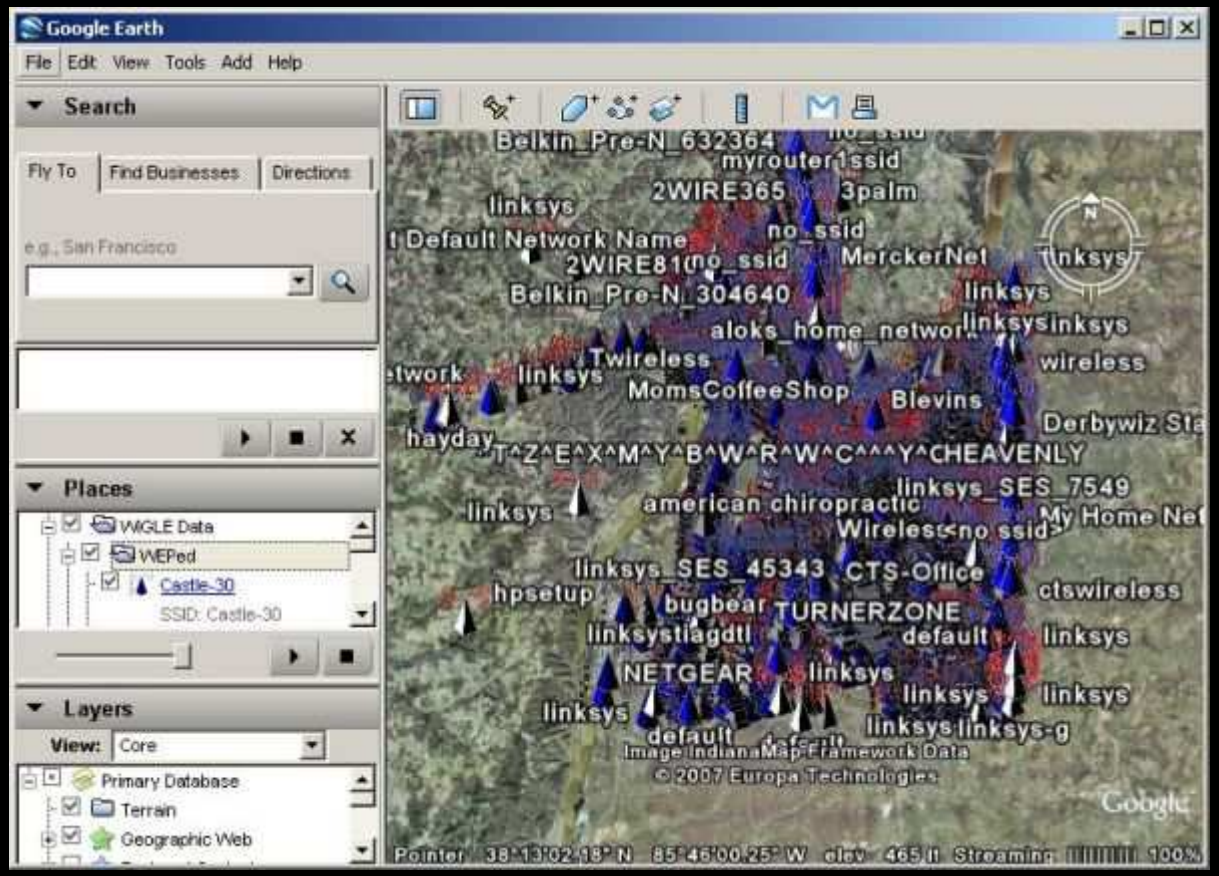
User-agent: *

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

http://Irongeek.com

More Links

- Recon Sites and Tools
  http://www.binrev.com/forums/index.php?showtopic=40526

- Pauldotcom
  http://mail.pauldotcom.com/pipermail/pauldotcom/2009-March/000960.html

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

Events

- Free ISSA classes
- ISSA Meeting
  http://issa-kentuckiana.org/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Phreaknic/Notacon/Outerz0ne
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

Thanks

- Brian
  http://www.pocodoy.com/blog/
- Kelly for getting us the room and organizing things
- Jonathan Cran
  http://hexesec.wordpress.com/
  http://www.0x0e.net/ghg/
- Folks at Binrev and Pauldotcom
- Louisville ISSA
- Russ Mcree
  http://holisticinfosec.org
- iamnowonmai for helping me “zone out”
- Larry “metadata” Pesce
  http://pauldotcom.com
- John for the extra camera

QUESTIONS?

42

http://Irongeek.com