Links for Doxing, Personal OSInt, Profiling, Footprinting, Cyberstalking

Maybe you are doing a pen-test and need information before you carry out a social engineering attack. Maybe you just want to see if someone who contacted you online is legit, or know what data of yours is out there for others to find.

Here are a collection of sites I and others have found useful for finding data about a person or organization. I'm posting them mostly so I don't lose them, and so I have a place to point others to when they ask. If you have ideas for additions please contact me.

There are tools for automating some of these tasks, but there is something to be said for doing it "by hand". Computers are great at math and automation, but extracting context is a bit more difficult for my silicon friends (and also for my silicone friends). The human mind can be far better at these tasks, at least some minds. The way you have to think is in making connections. One bread crumb of data leads to another, which leads to another and then another. For example:

- Finding a user name leads to other profiles with more data, this leads to a full name, then this could lead to a physical address.
- A user name can lead to pics, which could lead to license plates or physical addresses.
- For common names like John Doe adding interests from a profile or a location can lead to narrowing down the results to a specific person.

It's all about making connections. Keep in mind, you will normally find more information on someone who is tech savy then someone who is not. My granny ain't on Facebook after all.

Please note there a quite a few common problems with these sorts of social network aggregation sites:

1. Some sites start out free, then go paid. When this happens you get a lot of info teases that lead to companies wanting your credit card. Sucky!
2. People like to create mashups, but then abandon them after the fun is over. Then the back end API changes, and the site no longer works. What sites are good for a task changes over time.
3. Some may ask for social network credentials. You may want to make some throw-away accounts just for the purposes of using these tools.

This page will need t be updated over time, so please send me suggestions.

General Search:

Google
Duh. Make sure you know your operators to get he most out of it however.
http://www.google.com

Bing
Ok, Bing gets made fun of a lot as an "also ran" next to Google, but it has a few awesome features. Many of the same operators from Google work here, but one I really dig that only Bing has is IP: to find other websites on the same IP (shared host cross referencing fun).
http://www.bing.com/

Networking, Domain and Routing Information

Most of this page will cover finding out information on people from social networks, not network networks. However, sometimes knowing who owns a network/domain/IP is a great place so start, and people leave things in their Whois records that may reveal a lot of useful leads. There are so many sites that offer these types of services, but I'll only cover my favorites.

RobTex
While the interface is a bit weird in my opinion, this is a great site for doing reverse DNS look-ups on IPs, grabbing Whois

contacts, and finding other general information about an IP or domain name.
http://www.robtex.com

ServerSniff
This one is sort of an odd ball. Lots of sites offer Whois info, this one goes for more exotic tools. You really have to just play with it to find all of its features. It's sometimes hard to remember which option is where. Just some of the tools are: ICMP & TCP traceroutes, SSL Info, DNS reports and Hostnames on a shared IP. It's nice to have them do some of the recon for you if you don't want to use a proxy and don't wish for your IP to show up in the target's logs.
http://serversniff.net

Looking for profiles on a person

OSINT BOOKMARKLETS v0.2
http://illmob.org/bookmark.html
Cool page from Will Genovese where you can lookup Phone, IP, Host, Email, S/N, Name, and Address info in an automated fashion.

True People Search
https://www.truepeoplesearch.com
Awesome site for finding addresses and mapping out family relations.

Family Tree Now
http://www.familytreenow.com
Awesome site for finding addresses and mapping out family relations.

Moose Roots
http://www.mooseroots.com
Awesome site, especially for these sub-sites
http://birth-records.mooseroots.com/
http://marriage-divorce-records.mooseroots.com/
which are great for mapping out family relations for password reset questions.

Advanced Background Checks
For finding street addresses and relatives this is the bomb. So far, it has not failed me on finding street addresses if I have a vague idea where someone lives
http://www.advancedbackgroundchecks.com

Peek You
The interface is clean, and while it links off to pay sites it at least gives you real information first. I seem to recall it being better in the past.
http://www.peekyou.com

Lullar

Search for a person using Email|Name|user name. There are not as many results returned as other sites, but what it gives you is nice an clean, with out all of the paid sites in the way.
http://com.lullar.com/

Check Usernames
Ok, got to say I love this site. It may not have been meant as a site for profiling, but it works well for that task. We all talk about password reuse being a problem, but for profiling someone user name reuse is where it is at. This site lets you search 160 social network sites to see if a screen name is taken. From there, you can go see what is in a persons profile on those sites by hand. Saves some time verses checking for an account on each site yourself, but there is still lots of work for you to do afterwards.
http://www.checkusernames.com/

KnowEm
Similar to Check Usernames above, but claims to check over 500 sites to see if a given user name is taken.
http://knowem.com

iSearch
This use to be Spock ("Single Point Of Contact (by) Keyword"). Not sure when it changed, my guess is after Intelius bought them. You can search on Name|Phone|Email|lScreen Name. Good for finding relatives I suppose. Once you find a name from a user name you should step back and search for it as well, as the results vary a lot. Seems to mostly drive people to paying money to Intelius.
http://www.isearch.com

Pipl
You can search for Name|Email|user name|Phone and find related results. The results can be very noisy, with links to a bunch of paid sites (Spokeo, Intellus, etc.), but if you are willing to sort though the crap it's pretty nice. I like what it shows from public records, Amazon profiles, and social networks.
http://www.pipl.com

123 People
Much like all of the above. Links off to a bunch of other resources, some paid and some not.
http://www.123people.com

Spokeo
Ok, Spokeo has some nice layout features but it's an info tease. It reports "hey I found something" a lot, but you have to pay for the results. Much like crime, I don't pay. Still, it can be nice as a starting point to lead you elsewhere. For example, once you know someone has a Facebook profile, you can just go to Facebook.

http://www.spokeo.com

WebMii
Lets you looks up people by name or keyword (try user name as a keyword).
http://webmii.com/

Zoom Info
Seems pretty good for finding where someone works. I wonder how much of the information is just from LinkedIn, and how much from other sources? Looking at them side by side, Zoom Info does seem to augment the details with other sources.
http://www.zoominfo.com

Geo Location

Android Map
If you have the MAC address of a router (it happens) Samy has a tool to try to geolocate it base on what Google knows. Seems likely that Google is using Android phone to do a distributed wardrive to supplement their street view car data.
http://samy.pl/androidmap

Bing Map Apps
The map apps are a nice extra to have, but you will need SilverLight and they don't seem stable unless you are using Internet Explorer (go figure). Look at the Twitter map app.
http://www.bing.com/maps/

Twitter Map
Also nice to see where people are tweeting from, but not as slick or as comprehensive as the Bing app.
http://twittermap.appspot.com/

Other Oddities

411
I've had good luck with using this to find addresses and neighbors.
http://www.411.com/

Google Images
I imagine most folks know about Google Images, but did you know who can upload images (or drag and drop them) to find similar results? Good for finding profiles under different names. Tin Eye is similar, but does not seem to cover as much.
http://images.google.com/

Tin Eye
Ever found a picture of someone, and wondered if it existed elsewhere? Tin Eye, and it's browser plugin, let you choose a picture and find similar ones online, even ones that have been seriously shopped. Unfortunately, the database seems small. My hope would be to go to a social network profile, right click on an image I only know the user name of, then find other profiles with a real name and better information. So far, it's mostly been useful for finding out "who is this actor/model", but perhaps in the future it will be better.
http://tineye.com

Open Book
Got to love people that leave Facebook comments open to the world. Even if one person is privacy aware, a friend of theirs may not be and could make comments about them.
~~http://youropenbook.org/~~

Open Status Search
Open Book seems to be gone, and Open Status Search seems to be the next best thing.
http://openstatussearch.com/

Pic Fog
May find something good, may find something that scars you for life.
http://picfog.com

White Pages Find Neighbors
Might be useful if you need to SE someone close by.
http://www.whitepages.com/find_neighbors

Yasni
I've had some pretty good luck using this to scrape info on people.
http://www.yasni.com

Archive.org Wayback Machine
Sometimes someone drops their docs, but removes them. The Wayback Machine may help you find the deleted info.
http://www.archive.org/web/web.php

Board Reader
Maybe the person posts on some forums with a given user name? Could lead to useful info.
http://boardreader.com

OMGili

Another board search, like the above.
http://omgili.com

Tools

Ok, these are not websites, but damn useful tools that pull from web resources.

Maltego
Nifty tool, and I like the way it draws connections between entities like name, domain, email addresses, etc., good for building a mind map of how things are related. I still prefer to do things by hand to clear up false positives and interpret data. You will likely have to register for API keys to get the most use out of it.
http://www.paterva.com

NetGlub
This could someday be an open source replacement for Maltego, but right now it seems next to impossible to get working.
http://www.netglub.org/

Foca
I really dig this tools. It can do searches for common document formats using Google and other search engines, then download them to extract metadata. Lovely.
~~http://www.informatica64.com/DownloadFOCA/~~
https://www.elevenpaths.com/labstools/foca/index.html

Cree.py
Great tool for geolocating/tracking Twitter/Foursquare users. Not only pulls coordinates from the posts directly, but can grab them from the EXIF data in pictures they link to.
http://ilektrojohn.github.com/creepy/

Sites I've found so useless...

... that I won't even link to them, but I want to keep people from asking "why isn't X listed?" Mostly you get on this list for having little to no free information, and only leading to questionable for pay information.

zabasearch
yoname (use to like it, now the results seem pretty bad)
wink
mylife

freeality
infospace

Thanks to @davemarcus, @ukfully, @digininja, @CiphersSon, @b4seb4nd, @xillwillx and pentest-standard.org.

Changelong:

5/15/2017: Added True People Search.
1/12/2017: Added Family Tree Now.
6/04/2016: Update Foca link
4/29/2015: Added "OSINT BOOKMARKLETS v0.2" and "Moose Roots".
2/26/2013: Added "Advanced Background Checks", "Yasni", "411", "Google Images" and "Open Status Search".


Printable version of this article

15 most recent posts on Irongeek.com: