@FSLabsAdvisor wrote an interesting Tweet :

it turns out, by heading to https://www.facebook.com/directory, you can get a list of every searchable user on all of Facebook!

My first idea was simple: spider the lists, generate first-initial-last-name (and similar) lists, then hand them over to @Ithilgore to use in Nmap's awesome new bruteforce tool he's working on, Ncrack
.

But as I thought more about it, and talked to other people, I realized that this is a scary privacy issue. I can find the name of pretty much every person on Facebook. Facebook helpfully informs you that "[a]nyone can opt out of appearing here by changing their Search privacy settings" -- but that doesn't help much anymore considering I already have them all (and you will too, when you download the torrent). Suckers!

Once I have the name and URL of a user, I can view, by default, their picture, friends, information about them, and some other details. If the user has set their privacy higher, at the very least I can view their name and picture. So, if any searchable user has friends that are non-searchable, those friends just opted into being searched, like it or not! Oops :)

The lists

Which brings me to the next topic: the list! I wrote a quick Ruby script (which has since become a more involved
Nmap Script

that I haven't used for harvesting yet) that I used to download the full directory. I should warn you that it isn't exactly the most user friendly interface -- I wrote it for myself, primarily, I'm only linking to it for reference. I don't really suggest you try to recreate my spidering. It's a waste of several hundred gigs of bandwidth.

The results were spectacular. **171 million** names (**100 million** unique). My original plan was to use this list to generate a list of the top usernames (based on first initial last name)...

Read more:

https://www.skullsecurity.org/blog/?p=887