

Recon: The social side

I got friends on the other side

The background of the slide is white with two large, solid pink triangles. One triangle is in the top-left corner, and the other is in the bottom-right corner. They meet at a diagonal line running from the top-left towards the bottom-right.

The aims of Social Intelligence

Humans are often the weak link

- ▶ Humans don't like difficult things
 - ▶ They will often choose simplicity over personal safety
 - ▶ They will make quick assumptions
- ▶ Humans like to be social
 - ▶ They like to help
- ▶ Humans will avoid confrontation
 - ▶ They will prefer not to confront you if they risk seeming “silly”

Phishing

- ▶ Using bait to try and snag a target
- ▶ Aims to be non-confrontational
 - ▶ Ideally the target won't even know they've been hit
- ▶ Spear Phishing
 - ▶ Designed to target a very specific target
- ▶ Whale Phishing
 - ▶ Going after high value targets
 - ▶ The term "whale" comes from the gambling industry

Blackmail

- ▶ If you can dig up juicy information you may be able to blackmail them into doing what you want
- ▶ Highly confrontational
 - ▶ More likely to go to the police

The background of the slide is white with two large, solid pink triangles. One triangle is in the top-left corner, pointing towards the center. The other is in the bottom-right corner, also pointing towards the center. They meet at a diagonal line that runs from the top-left towards the bottom-right.

How do we get information?

Google Dorks





- ▶ Just google a name if it's unique enough.
- ▶ `inurl:linkedin intitle:"<companyName>"`
- ▶ `Inurl:facebook intitle:"<name>"`

Recon-ng

- ▶ The “*-contacts” modules will help us pull names and addresses.
- ▶ Not quite as good since WHOIS turned off
- ▶ Possibly good if you add in the API keys
 - ▶ I haven't tried this yet.

SocialMapper – SpiderLabs

- ▶ Facial recognition across social media sites
- ▶ https://github.com/SpiderLabs/social_mapper
- ▶ It works by automating an actual browser, via selenium, to grab images

Photo	Name	LinkedIn	Facebook	Twitter	Instagram
		GooglePlus	Vkontakte	Weibo	Douban
	Jacob Wilkin				

targets-facebook					
A1					
1	Jacob Wilkin	Jacob Wilkin	jwilkin@trustwave.com	https://www.facebook.com/jacobwilkin123?ref=br_rs	https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/p320x320/
2	Lawrence Munro	Lawrence Munro	lmunro@trustwave.com	https://www.facebook.com/lawrence.munro?ref=br_rs	https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/c0.0.320.32
3	Hans Boshoff	Hans Boshoff	hboshoff@trustwave.com	https://www.facebook.com/johannes.boshoff.16?ref=br_rs	https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/p320x320/
4	Michael Gianarakis	Michael Gianarakis	mgianarakis@trustwave.com	https://www.facebook.com/mgianarakis?ref=br_rs	https://scontent-waw1-1.xx.fbcdn.net/v/t1.0-1/p320x320/
5					

Maltego

- ▶ Pre-installed on Kali
- ▶ Available in a Community Edition
 - ▶ Requires signing up on maltego site for login
- ▶ A multitude of data expanders
 - ▶ Take one datapoint and map to other relevant pieces.
 - ▶ Can be used for network mapping too.

