ONLINE SELF FINGERPRINTING 101

Between OSINT & OPSEC – Tips & Tricks

Whoami ?

- Former ENSIBS (Graduated 2019)
- Cybersecurity Consultant / Pentester (Rennes, FR)
- Interested in :
  - *Offensive Security (Active Directory, Phishings..)*
  - *OSINT related topics*
- Twitter : Haax9_
- Discord : Haax#2683
- Posts :
  - *haax.fr*
  - *cheatsheet.haax.fr*

What ?

- ■ OSINT = Open Source Intelligence
  - – *Online publicly available information*

- ■ OPSEC = Operations Security
  - – *Process that identifies risks and information about [insert entity] if these informations are collected by the ennemy intelligence*

- ■ Online Self Fingerprinting
  - – *All data that can lead to your real identity or give information about you*
  - – *Your « online presence »*

Why ?

- To control what is publicly available about you
  - *And to choose what*

- To prevent data leaks and clean some old data

- To limit your online presence and to avoid as much as possible being tracked

- To protect yourself or people around you

How ?

- Identify and gather
- Verify information
- Delete or update what you can
- In-depth research
- PS C:> Invoke-GDPR
- De-indexing the world !
- Bonus : picture filtering
- And what now ?

- <u>Disclaimer</u> : I'm clearly not expert here. Just giving some tips and methods that everyone can appply

Identify and gather

■ List online assets where you have accounts

– *Start by writing down everything you can*

■ Remember your old e-mail addresses ? ☺

– *They can be usefull !*

– *Take them back (before really deleting it)*

– *And search through your 2k e-mails...*

■ You can't get all your accounts in oneshot

– *So, keep your list and everytime you remember something, append !*

Identify and gather

Verify information

- Take these accounts back and look settings
  - *What's your username ?*
  - *Your public name ?*
  - *Does it have more infos (birth, address…) ?*
  - *Does it have MORE infos (credit card, official documents) ?*

- Report it to your list
  - *You can choose what data matter to you !*

Verify information

Delete or update what you can

Delete or update what you can

- First thing first, do you want to keep this account ?
  - *No ? Delete it*

- Are these data necessary ?
  - *If no, you can also delete*

- The service X needs some kind of personal data to work ?
  - *Is it official ?*
  - *If no, just set up fake ones (or online dedicated ones)*

- Once again, you can choose what you want to keep online

#SocialNetworkEdition

- Social Network are a big part, and an important one

- For each one :
  - *Check your settings (what data you gave and privacy settings)*
  - *Browse your entire profile, back to the past*
  - *You can delete all the old stuff you don't want anymore*
  - *Old tweets, old facebook pictures, etc.*
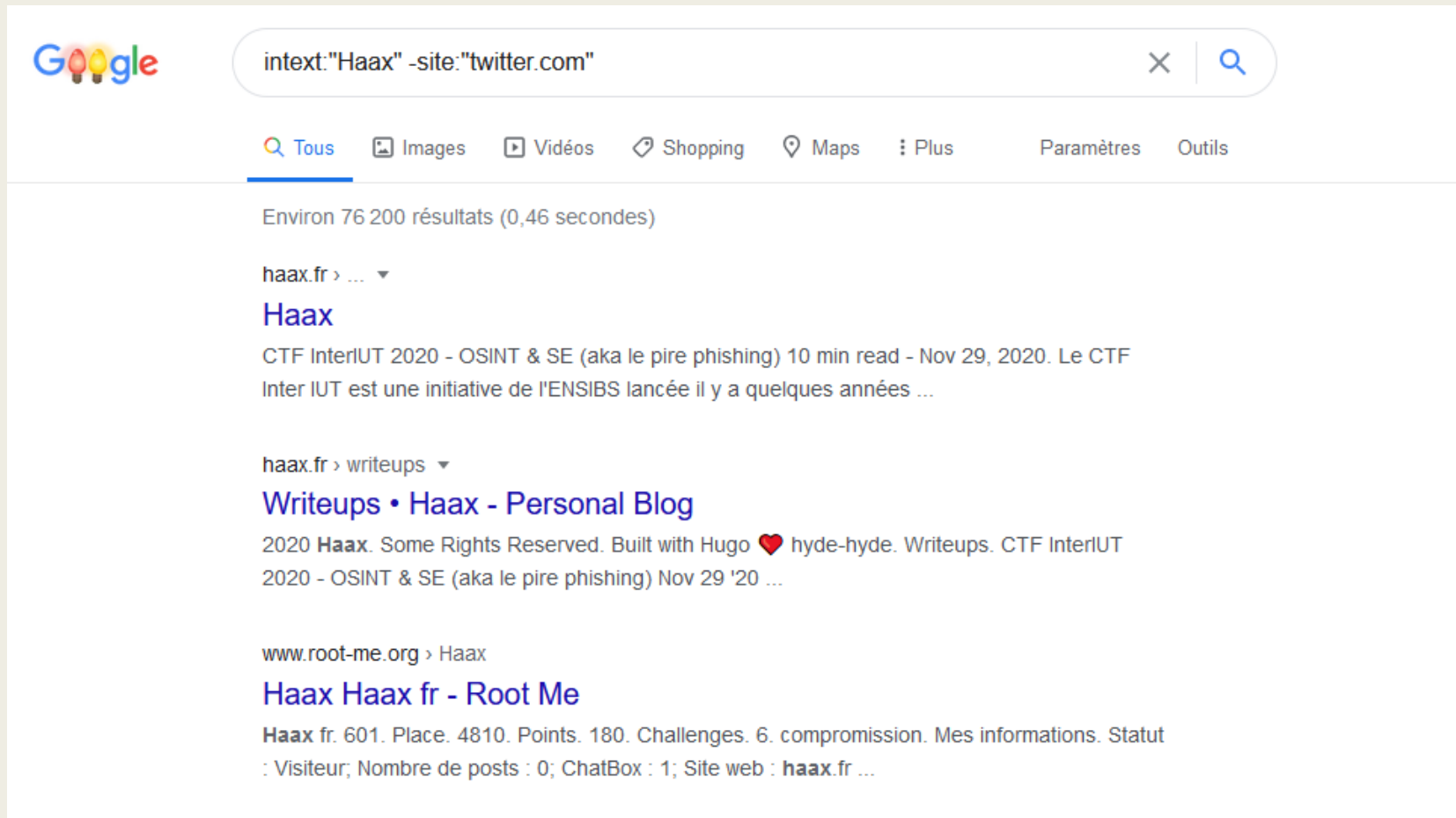
In-depth research
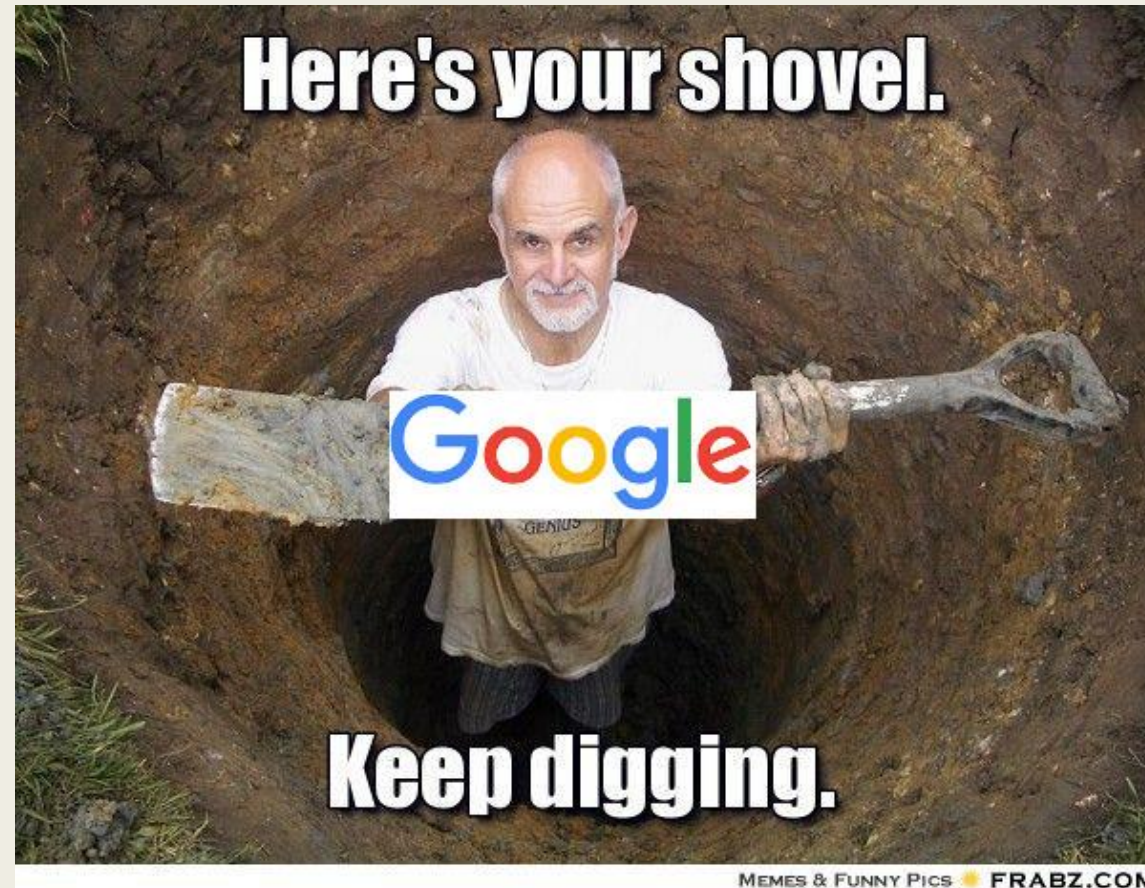
In-depth research

- You want to know **everything** that has been indexed about you

- You can search for pseudo, real name, e-mail address
  - *Photos too*

- One tool to rule them all : DORKS
  - *« Haax »*
  - *Intext:«Haax »*
  - *Filtering site using –site:*
  - *…*

In-depth research

In-depth research

- Loop and search several times, for each identity, old pseudos etc.

- Depending on your online activity, you can collect TONS of data

- Store them all ! You can use them for :
  - *Gather other accounts you forgot ;*
  - *Collect old links or pages mentioning you (to delete them later) ;*
  - *Map your online fingerprint*

PS C:> Invoke-GDPR

PS C:> Invoke-GDPR

- In some (many) cases, you won't have a golden button allowing you to delete your own account
  - *GDPR to the rescue !*
  - *You'll need to contact the service and ask for deletion*

- You will also need :
  - *Patience*
  - *Time*

- Be ready to start for few weeks of e-mails ping pong

De-indexing the world !

De-indexing the world !

- Now that you have
    - *Collected all (or many) data and links to you*
    - *Stored them in your little list*

- The magical tool : « Remove Outdated Content »
    - *Even if accounts and posts might be removed, they remain in the Google Cache*
    - *But you can force (well, ask) Google to remove it*

De-indexing the world !

Bonus : picture filtering

■ Pictures are an important part

– *Good to (try to) know where your face appears*

– *They can be used for tons of things*

– *i.e: facial recognition, machine learning*

■ You can add noise to your pictures !

– *Fawkes tool :* *https://sandlab.cs.uchicago.edu/fawkes/*

– *It can helps protecting yourself*

And what now ?

- Now that you spent dozens of hour trying to collect and remove content about yourself, what can you do ?

- Go deeper by learning how tracking works on Internet
  - *Partition your online browsing (by using profiles for example)*
  - *Setup a dedicated browser for different types of online behavior*
  - *Work on your password stategy*
  - *And so much more...*

- Try to improve your methodology and loop over it regularly

To go further...

- Some resources there
  - https://cheatsheet.haax.fr/open-source-intelligence-osint/tools-and-methodology/opsec/

- ShutUpTrackers
  - https://shutuptrackers.com/