# Information Gathering

Iker M. Canut

8 de julio de 2020

## 1. TOOL: hunter.io

Hunter is a Domain Search. It gives a list of people that works in the organization: You get the first and last name and the most common pattern as far as email addresses are concerned. You can export all this information in a .csv. Maybe it tells you the department: Human Resources, IT/Engineering, Management, Executive, Legal, Sales, Support,...

This service may not list all the workers, but if you know that the email pattern is, for example, **{f}{last}@tesla.com**, and you know because of Linkedin, that "*Iker Canut*" works there, you can probably assume his email is *icanut@tesla.com*. This is crucial when we perform attacks (e.g password spraying in a login form).

## 2. TOOL: Breach Parse

In hmaverickadams' Github, we can find a breach-parse. It's quite heavy, but it has emails and password from breaches: credentials got dumped out and you can use them. The bash script is for searching more easily. To illustrate this, you can write: **./breach-parse.sh @tesla.com tesla.txt**. Then, the results are extracted to three files: A master, passwords and users. You can take advantage if people utilize their work credentials and they log into websites.

## 3. TOOL: theHarvester

You can use it to get emails and domains. It's fast, but it's not as powerful as other tools. Options in **theHarvester –help**.

## 4. Hunting subdomains

For example, if you need to analyze ***.tesla.com**, you can search for subdomains like *dev.tesla.com* or something that should have never been there, like logs. You shouldn't be limiting yourself to one website where there could be potenially tons of websites.

## 5. TOOL: sublist3r

To install it: **apt install sublist3r**. Options as usual in **sublist3r –help**. This is going to list a bunch of Unique Subdomains, because it uses Baidu, Yahoo, Google, Bing, Ask, Netcraft, DNSdumpster, Virustotal, ThreatCrowd, SSL Certificates, PassiveDNS, ... It will even find 4th level subdomains.

## 6. TOOL: crt.sh

You can use this for certificate fingerprinting: You look for certificates that have been registered; You can find a lot of information. For example, APIs, VPN, dev, SSO, QA, mail, ... The wildcard is %.

## 7. TOOL: owasp amass

This is THE go to tool for a lot of people. You can go to the Github and download it. You can configure it to do a lot of things and find a lot more subdomains.

- amass intel – Discover targets for enumerations
- amass enum – Perform enumerations and network mapping
- amass viz – Visualize enumeration results
- amass track – Track differences between enumerations
- amass db – Manipulate the Amass graph database

## 8. Narrowing the lists

You can use for example the thomnomnom's tool named httprobe to check a list of domains, to see which ones are alive.