Information Gathering

Iker M. Canut

7 de julio de 2020

1. 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. 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.