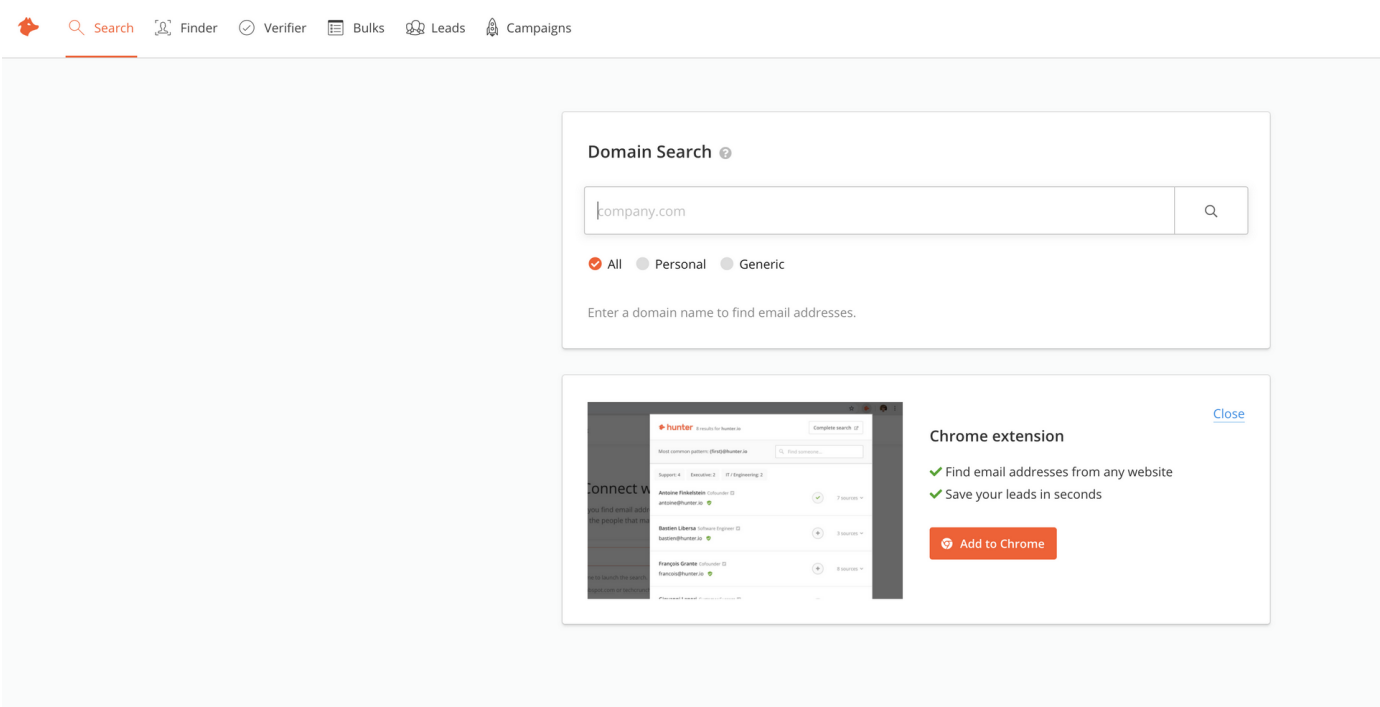
Gathering Emails/Breached Credentials with hunter.io and breach-parse

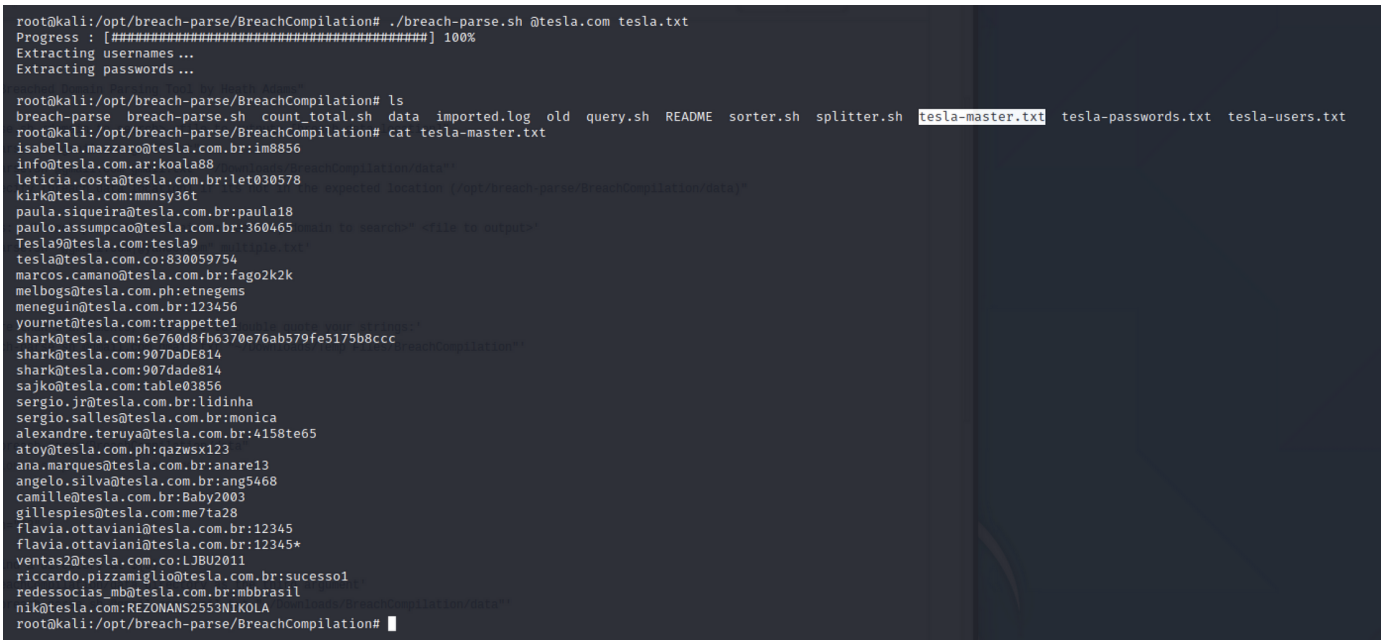
We use the hunter.io online resource shown below:



The following tool contains a datastore of multiple compromised emails and their corresponding passwords

The breach-parse tool and repository can be found at https://github.com/hmaverickadams/breach-parse. As stated above, this tool contains a datastore of multiple compromised emails and their corresponding passwords. There is a shell script that can be used to traverse the repository in search for specific email domains. The tool is called `breach-parse.sh`.

The tool is a few kilobytes in size. However, the repository of compromised credentials is about 44 gigabytes. The following is an example of how to use the tool on an email domain. We will be searching for the `@tesla.com` domain:



In the image, we can see the respective emails and their passwords. When looking through the list, we are looking for certain things/features:

1. The Email Syntax: `FirstnameLastname@domain.com`, `FirstinitialLastname@domain.com`, etc.
2. Repeat Offenders: Users whose emails have been compromised multiple times.
3. Weak or Similar Passwords: Users who did not make any significant changes to their passwords.
