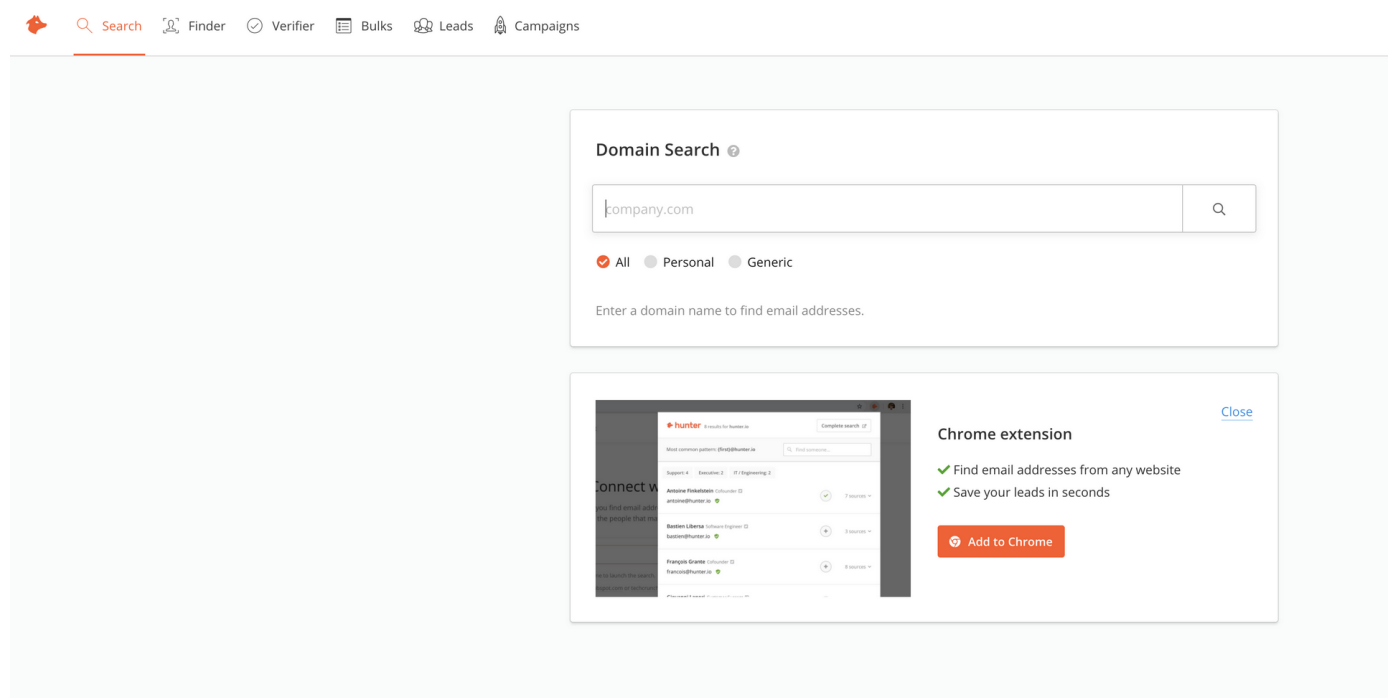


Gathering Emails/Breached Credentials with hunter.io and breach-parse

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:

```

root@kali:/opt/breach-parse/BreachCompilation# ./breach-parse.sh @tesla.com tesla.txt
Progress : [#####] 100%
Extracting usernames ...
Extracting passwords ...

root@kali:/opt/breach-parse/BreachCompilation# ls
breach-parse  breach-parse.sh  count_total.sh  data  imported.log  old  query.sh  README  sorter.sh  splitter.sh  tesla-master.txt  tesla-passwords.txt  tesla-users.txt
root@kali:/opt/breach-parse/BreachCompilation# cat tesla-master.txt
isabella.mazzaro@tesla.com.br:im8856
info@tesla.com.ar:koala88
leticia.costa@tesla.com.br:let030578
kirk@tesla.com:mnnsy36t
paula.siqueira@tesla.com.br:paula18
paulo.assumpcao@tesla.com.br:360465
Tesla9@tesla.com:tesla9
tesla@tesla.com.co:830059754
marcos.camano@tesla.com.br:fago2k2k
melbogs@tesla.com.ph:etnegems
meneguina@tesla.com.br:123456
yournet@tesla.com:trappette1
shark@tesla.com:6e760d8fb6370e76ab579fe5175b8ccc
shark@tesla.com:907DaDE814
shark@tesla.com:907dade814
sajko@tesla.com:table03856
sergio.jr@tesla.com.br:lidinha
sergio.salles@tesla.com.br:monica
alexandre.teruya@tesla.com.br:4158te65
atoy@tesla.com.ph:qazwsx123
ana.marques@tesla.com.br:anare13
angelo.silva@tesla.com.br:ang5468
camille@tesla.com.br:Baby2003
gillespies@tesla.com:me7ta28
flavia.ottaviani@tesla.com.br:12345
flavia.ottaviani@tesla.com.br:12345*
ventas2@tesla.com.co:LJB02011
riccardo.pizzamiglio@tesla.com.br:sucesso1
redessocias_mb@tesla.com.br:mbbrasil
nik@tesla.com:REZONANS2553NIKOLA
root@kali:/opt/breach-parse/BreachCompilation#

```

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.
-