PwnyCorral

April 29, 2019

Overview

PwnyCorral takes advantage of the haveibeenpwned API to determine if an account has been part of a data breach. The primary goal of this script is to allow organizations/companies to track the breaches in which their users have fallen victim. Identifying and tracking accounts that come from one particular source may allow proactive remediation to occur.

Installation

Prerequisites

TinyDB

```
# pip install tinydb
```

Requests

```
# pip install requests
```

Termgraph

```
# pip3 install termgraph
```

Usage

Help

python pwnycorral.py -h

```
usage: pwnycorral.py [-h] [-a ADDACCNAME] [-r REMACCNAME] [-c] [-s]
                     [-f FILENAME] [-l] [-e ACCEXISTS] [-d ACCDET] [-v] [-g]

optional arguments:
  -h, --help     show this help message and exit
  -a ADDACCNAME  ADD account to database. Support -v flag.
  -r REMACCNAME  REMOVE account from database.
  -c             COUNT accounts in database.
  -s             Number of SITES in database.
  -f FILENAME    Bulk add accounts based on FILE. One email address per line.
  -l             List accounts in database
  -e ACCEXISTS   Determine if account is in database
  -d ACCDET      Show details of specific account
  -v             VERBOSE output. Display description of compromise
  -g             GRAPH breaches to show greatest threat.
```

Add Account

python pwnycorral.py -a [email address]

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -a obama@whitehouse.gov
The account obama@whitehouse.gov has been added to the DB
```

Remove Account

python pwnycorral.py -r [email address]

Number of Breached Accounts in DB

python pwnycorral.py -c

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -c
15
```

Number of Breached Sites in DB

python pwnycorral.py -s

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -s
B2BUSABusinesses count:  1
Dailymotion count:  1
Dropbox count:  4
Houzz count:  3
Lastfm count:  3
OnlinerSpambot count:  2
Tumblr count:  2
```

Bulk load Accounts into DB

python pwnycorral.py -f [filename]

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -f bulk.txt
The account obama@whitehouse.gov was found.
The account trump@whitehouse.gov was not found.
The account 123@aol.com was found.
```

List Breached Sites and Number of Accounts in Each

python pwnycorral.py -l

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -l
obama@whitehouse.gov count:  24
123@aol.com count:  96
```

Does Account Exist in DB

python pwnycorral.py -e [email address]

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -e 123@aol.com
The account 123@aol.com exists in the database
```

Details of Specific Account in DB

python pwnycorral.py -d [email address]

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -d 123@aol.com
Details for 123@aol.com...
000webhost
In approximately March 2015, the free web hosting provider <a href="http://www.troyhunt.com/2015/10/breaches-traders-plain-text-passwords.h
ata breach</a> that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The

8tracks
In June 2017, the online playlists service known as <a href="https://blog.8tracks.com/2017/06/27/password-security-alert/" target="_blank"
18 million accounts. In their disclosure, 8Tracks advised that &quot;the vector for the attack was an employee's GitHub account, which was
assword hashes for users who <em>didn't</em> sign up with either Google or Facebook authentication were also included. The data was provide
avies and contained almost 8 million unique email addresses.
```

Verbose Output

python pwnycorral.py -v

Graph Breaches and Accounts in Each

python pwnycorral.py -g

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -g
BitcoinTalk          : 1.00
Disqus               : 2.00
Dropbox              : 2.00
Dubsmash             : 2.00
Evony                : 2.00
HeroesOfNewerth      : 2.00
```

Description of Breach

python pwnycorral.py -b [Breach Name (case sensive)]

```
(project_env) brad@ubuntu:~/Desktop/PwnyCorral$ python pwnycorral.py -b MyFitnessPal
Details for MyFitnessPal...
In February 2018, the diet and exercise service <a href="https://content.myfitnesspal.com/security-information/FAQ.html" target="_blank" rel="noopener">M
t exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier ac
 href="https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/" target="_blank" rel="noopener">the data appeared listed for sale o
ner large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to &quot
```