35

Now that we have a list of emails from linkedin we can format them into a custom wordlist with the email format we got from CORP-ADT01 and put them into a breached credentials service or in the case of Throwback Hacks an internal breached credentials server.

Introduction to Data Breaches
At the time of writing, HaveIBeenPwned has a collection of 10,189,054,980 breached user accounts, as well as 473 total breached websites. This is an alarmingly high number, but can offer a lot to an attacker looking to get an easy win. Data Breaches can confirm many things, not just if a user has been hacked, but it also confirms than an email account exists. This is arguably more valuable than a password. You can use this information in combination with Phishing to gain some really easy wins within an organization. For this next exercise, we have setup a Breach Credential Lookup service called Breach || GTFO, a fake service within the network that is modeled after https://dehashed.com -- A paid breach credential lookup service.

Namely Overview
Resource Link: https://github.com/OrielOrielOriel/namely
Namely is a template-based email wordlist generation tool that can also be used for doamin user wordlists, developed by Oriel. It takes a name list and a domain name or multiple domain names and

generates a wordlist around the two. Namely can also take custom template keys in order to customize the wordlist to your needs.

Installing Namely
1.) cd /opt
2.) sudo git clone https://github.com/OrielOrielOriel/namely

Formatting the User List
1.) sudo touch names.txt
2.) sudo nano names.txt
3.) Insert the names that should be formatted by namely for example:
Aras Gill
Amirah Mathis
Lewys Bloom
Marcos Halliday

Generating a Custom Wordlist with Namely
We have seen a variety of different email formats throughout the corporate environment but from the administrator desktop or CORP-ADT01 we know that the email format is being changed on the internal mail server. We can make templates around these formats.
1.) cd /opt/namely
2.) sudo python3 namely.py -nf names.txt -d TBHSecurity.com -t HRE-${first1}${last}@${domain}

Note: First and last names are not case sensitive for BREACH || GTFO

```
cryillic@human-eater:/opt/namely$ sudo python3 namely.py -nf names.txt -d TBHSecurity.com -t HRE-\${first1}\${last}@\${domain}
HRE-AGill@TBHSecurity.com
HRE-AMathis@TBHSecurity.com
HRE-LBloom@TBHSecurity.com
HRE-MHalliday@TBHSecurity.com
cryillic@human-eater:/opt/namely$
```

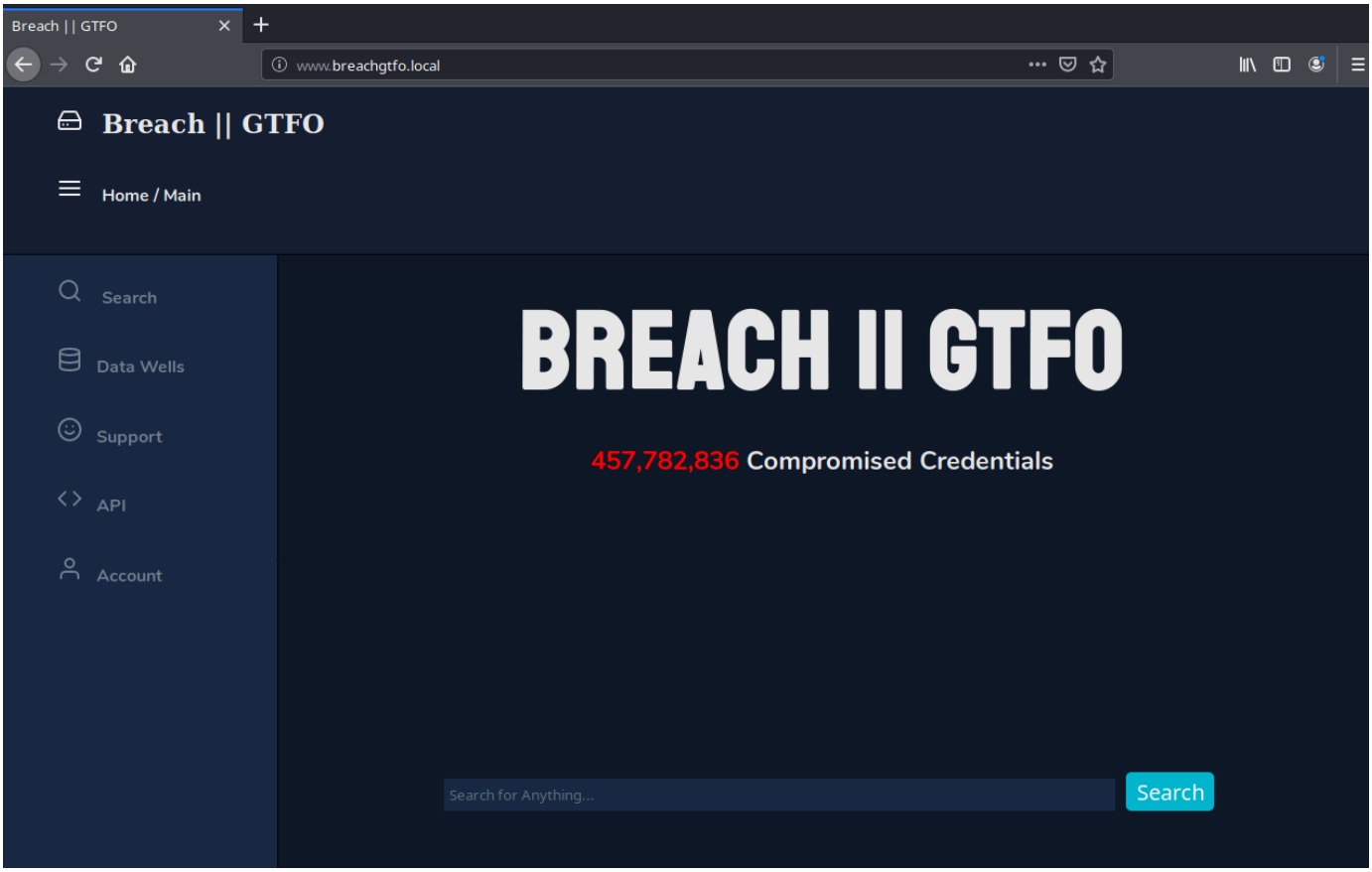
Generating a custom user wordlist with namely

In order to generate more complex user wordlists we can use the '-tf' switch to use a template file with a list of templates within it. We suggest putting your templates within a file and using the switch to automate the wordlist creation.

Accessing Corporate Resources
In order to access Breach || GTFO, you also need to update your /etc/hosts file with a new entry to www.breachgtfo.local
Your /etc/hosts file should look like this
10.200.x.232 www.breachgtfo.local
10.200.x.232 mail.corporate.local
127.0.0.1 localhost
After adding the vhosts to your /etc/hosts file, you should now be able to access Breach || GTFO and Corporate Mail from within your browser.

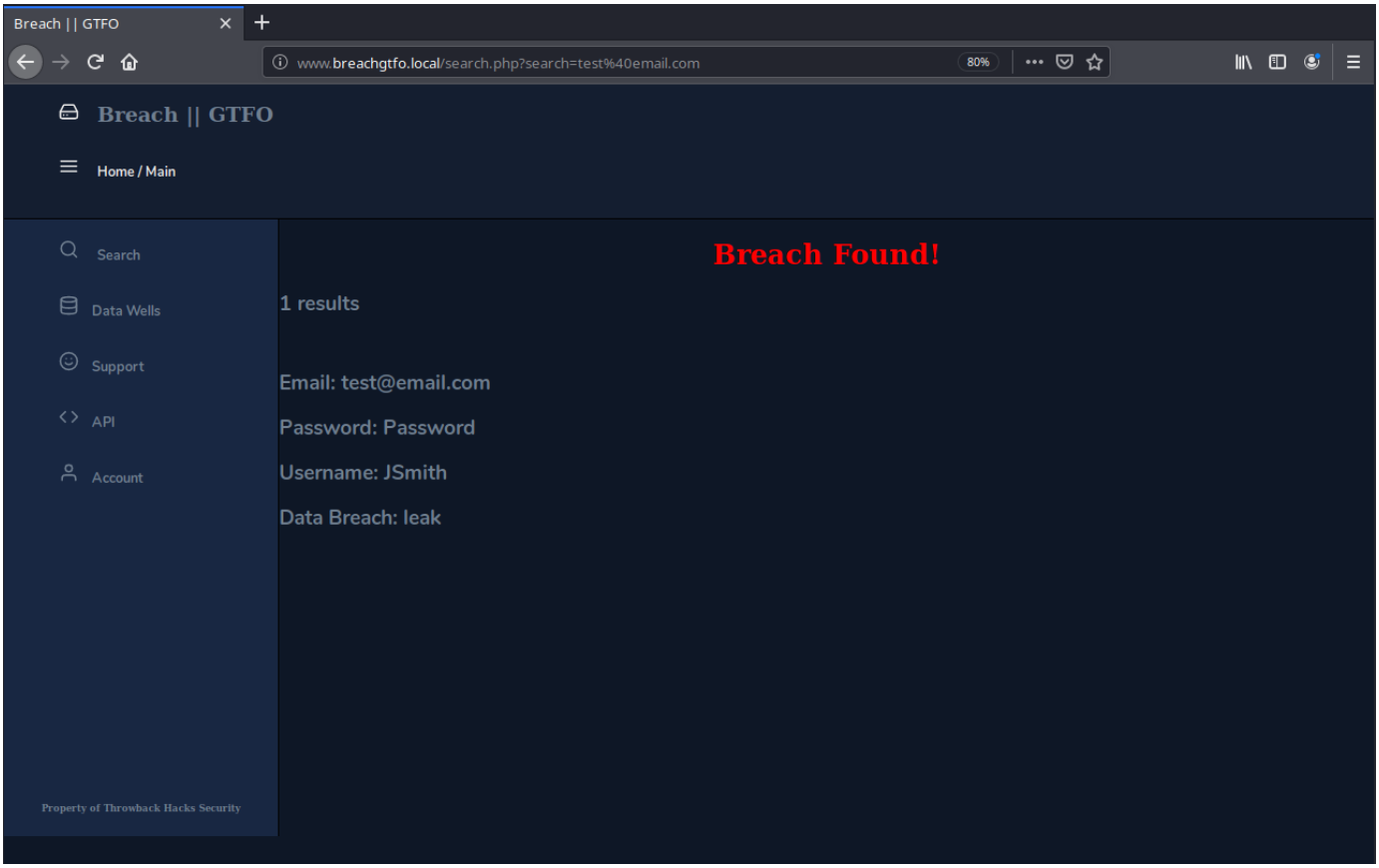
Searching and Utilizing Breached Credentials

After navigating to the page, you'll be presented with a web server called Breach || GTFO with a simple side menu and search bar.



The Breach || GTFO website

You can enter the email address of a user in the search bar to check if the users has been impacted by a data breach. Below are some samples results.



Sample results from Breach || GTFO

Now you can combine this internal breached credentials service with the email list from leetLinked to find a potential set of valid credentials.

Answer the questions below

What is the Users email who has been affected by the Databreach?

Submit

What was the Users password?

Submit

What credentials could be found in the Email?
Format: User:Pass

Submit

Submit flags for reconnaissance in Task 4

Completed