Hunting Breached Credentials

Whenever a website or company is breached, then the data containing usernames, passwords, phone numbers and what not get dumped on the dark web. This data is very useful to the scammers who tried to scam you on the call claiming to be bank employee but it is very helpful to us also as a penetration tester.

See, people most of the times uses the same password for most of their online accounts. If we get hold on any one of their password from the data breaches, we can get a initial access very easily into one of their account. This is called credential stuffing, we will look into this technique later in the course but for now, lets focus on hunting the breached credentials.

We will start off by checking if our target email address is in some kind of a breach or not.

- Have i been pwned - https://haveibeenpwned.com/

Now that we know our target email address is what of which breaches. Lets see what we can do with it.

- Use **h8mail** to find out breached creds

```
h8mail -t info@zomato.com -lb ~/Desktop/BreachCompilation/
```

- **Dehashed** - https://dehashed.com/
- **We leak info** - https://weleakinfo.i
- **Breach Directory** - https://www.breachdirectory.org/
- **Ashley Madison Leaks check** - https://ashley.cynic.al/
- **Leakpeak** - https://leakpeek.com/
- **Leakcheck** - https://leakcheck.io/
- **PwdQuery** - https://pwdquery.xyz/
- **Intelligence X** - https://intelx.io/
- **Leak lookup** - https://leak-lookup.com/
