Intro to Cybersecurity

1.1.3 - Authentication and Password Attacks

GALANTECH —with— GARDEN STATE CYBER

CYBER.ORG

Databases in Password Guessing Attacks

- **What is a database?**

  "any collection of data, or information, that is specifically organized for rapid search and retrieval by a computer" (Brittanica.com)

- **Dictionary Attack** – software programs which automate the process of rapidly testing many potential passwords for a given account.

  This attack uses a database (aka dictionary) of words that people are likely to use in their passwords including names of movies, teams, celebrities, foreign languages, AND including spelling with numbers or special characters substituted for letters.

Hybrid Attack = Dictionary + Brute Force

Attack assumes most passwords can be found in cracking dictionaries and depends on fast, high volume guessing.

Databases in Password Guessing Attacks

- **Password Spraying** – testing a weak password against a large number of accounts.

  For example, a malicious actor who has the usernames of all 10,000 employees at First Bank can automate trying the password "password123" on all the accounts, then, try again with another password from a database of commonly used passwords.

- Advantage – it avoids lockouts that are invoked after 2-3 incorrect password attempts.

Databases in Password Guessing Attacks

Password spraying is the **inverse** of a Brute Force attack.

- Dictionary brute force tries to access one account by trying lots of different passwords.
- Password spraying uses one password and tries it on lots of different accounts.

Attack assumes a percentage of people use common passwords and depends on fast login attempts to numerous accounts.

Databases in Password Guessing Attacks

Credentials = username + password pair used for authentication

Credential Stuffing – trying username/password from a breach in order to gain access to user accounts.

Example: the malicious actor steals the user account database from BigStore.com, then, automates trying those credentials to log into accounts at MovieNite.com and lots of other online sites.

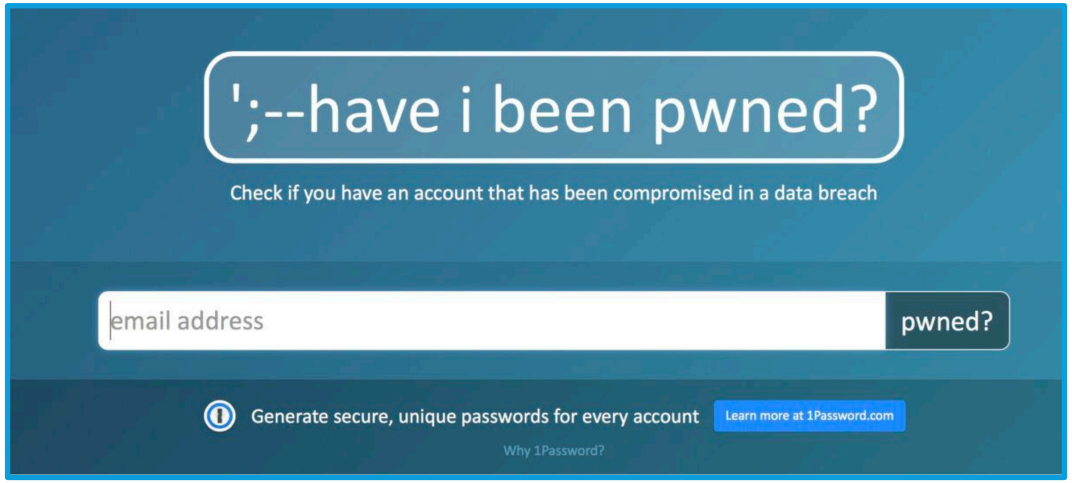
Databases in Password Guessing Attacks

- Reports show that 52 percent of people have a “favorite” password and use it on multiple accounts (Google/Harris Poll)
- Attack assumes most people reuse their passwords and depends on using breached credentials.

Database Breaches – Have I Been Pwned?

Many databases hold information that is valuable and/or confidential.

Breach – when a database is exposed or stolen – can be accidental or through insufficient security or from a malicious actor attack



';--have i been pwned?

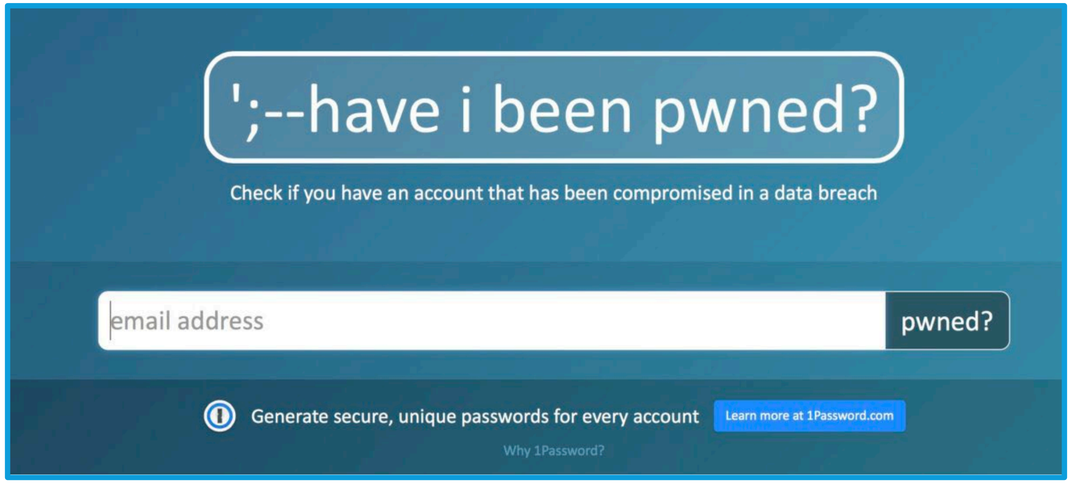
Check if you have an account that has been compromised in a data breach

Generate secure, unique passwords for every account

Database Breaches – Have I Been Pwned?

Every breach means that use data is at risk and often the users are unaware that a breach even occurred.

Troy Hunt created *Have I Been Pwned?* to help people identify if their credentials have been part of a data breach so they can take steps to reduce the risk – like changing their passwords!



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

Generate secure, unique passwords for every account

Intro to Cybersecurity

Activity – Have You Been Pwned?

GALANTECH —with— GARDEN STATE CYBER

CYBER.ORG