Intro to Cybersecurity

Foundations and Threats

1.1.3 - Authentication and Password Attacks

How are passwords stored on a system and what is password hashing?

Overview

The student will be able to:

- Define database as a collection of data organized for efficient organization and retrival.
- Explain 3 password guessing attack methods that use database information

Grade Level(s)

6, 7, 8, 9, 10, 11, 12

Cyber Connections

- CIA Triad
- Access Control
- Data Security

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

GALANTECH with GARDEN STATE CYBER
CYBER.ORG

Teacher Notes:

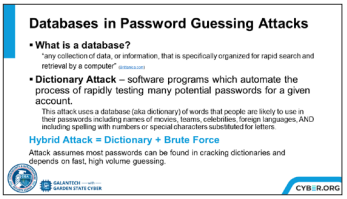
Authentication and Password Attacks

Materials (if needed)

Power Point: Intro into Cybersecurity - Authentication and Password Attacks 1.1.3

Instructions/rubric for project: see folder.

Slide 1 - Intro Slide



Slide 2 - Databases in Password Guessing Attacks

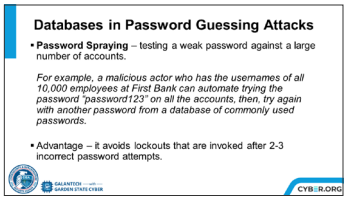
Definte databases and help students to understand that a database is like an Excel spreadsheet or Google sheet but on a much larger scale and with code to make data retrieval fast and efficient. Databases are used for data such as airplane reservations, credit card numbers, student grades, and….account user credentials.

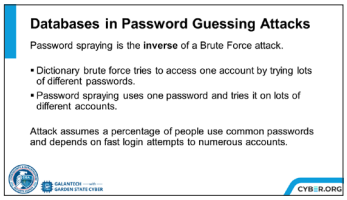
The slide shows the first of 3 ways in which databases are used for password guessing attacks:

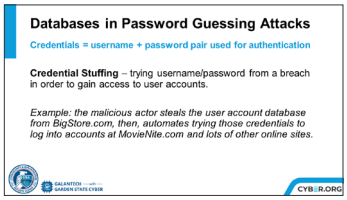
- A dictionary attack doesn't use a real dictionary like Websters. It uses a large database of words in many different languages. Hackers create these dictionaries to include common names, movie names, teams, even l33t spelling. (Pronounced "leet", this is when the use of alternate keyboard characters to replace letters - i.e., 1 is used for i or t, @ is used for a, etc.) if there is a word in your password, even misspelled, the dictionary attack can find it.
- A Hybrid attack uses a combination of a dictionary database and brute force methods.

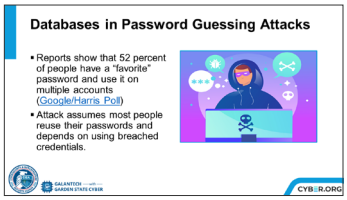
****Reminder that in 1.1.2, slide 6 we defined Brute Force Attack as software programs which automate the process of rapidly testing **all** possible combinations of characters.****

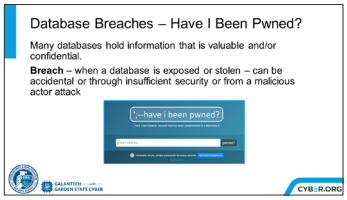
Teacher Notes:











Slide - 3 & 4

Password Spraying takes a database of common passwords and tests each one against a large number of different accounts. In the example above, getting access to even a few bank employee accounts could be a big payoff for the hacker. The same is true if they manage to take over user bank accounts that have large dollar balances.

In dictionary brute force attacks, the attacker can be slowed down by account lockouts that are triggered after 2-3 incorrect password attempts. Password Spraying won't trigger this type of lockout so the hacker can be highly efficient in trying lots of accounts.

Slide - 5 & 6

In attacking online accounts, the attacker needs 3 things:

1. a website where the user has an account
2. the username
3. the password.

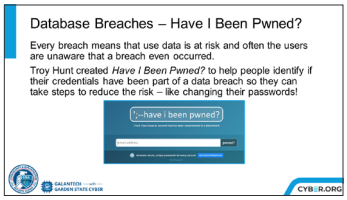
Most attacks start with the first and second, then use a method to test out passwords. But with Credential Stuffing the attacker has the second and third from the database breach and must try out different websites to see where the credentials will work. Given the high percentage of people who reuse passwords, credential stuffing has become a successful account hacking technique. Note that the Google/Harris Poll link is to an infographic with other interesting statistics.

Slide - 7 & 8

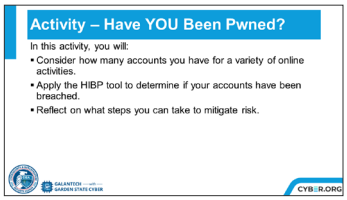
"Pwned" pronounced like "Poned." The term originated with gamers, and it means an opponent has been defeated, or "owned".

Many databases hold valuable and sometimes confidential information which makes them prime targets for hackers. When a database is no longer secure - whether it is accidentally made publicly accessible or stolen by hackers - that is called a "breach". Often the attacker steals a company's database in order to access a list of usernames and passwords. This could be a list of credentials for internal employees or for customers or for patients of a hospital, etc. Teacher Notes: 4 Copyright © 2023 Cyber Innovation Center All Rights Reserved. Not for Distribution.

Teacher Notes:



Note that Troy Hunt, the creator of *Have I Been Pwned?* (HIBP), is a highly respected cybersecurity practitioner. HIBP is considered a safe tool by the cybersecurity community. From Troy Hunt's blog: "I created HIBP as a free resource for anyone to quickly assess if they may have been put at risk due to an online account of theirs having been compromised or "pwned" in a data breach. All the data on this site comes from "breaches" where data is exposed to persons that should not have been able to view it. Data breaches are rampant, and many people don't appreciate the scale or frequency with which they occur. By aggregating the data here I hope that it not only helps victims learn of compromises of their accounts, but also highlights the severity of the risks of online attacks on today's internet." https://www.troyhunt.com/about/



Slide - 9

In this activity students will use the HIBP tool to investigate whether they have accounts that have been breached and to estimate their risk. https://haveibeenpwned.com/