Team Members:
Ross Young
Alicia Yong

Project Proposal

Problem

The average computer user is either uneducated or educated very little on the concept of cyber security and how important it is that they practice computer safety both on the internet and beyond what is just on the screen.

Basic Idea

We plan to create a platform that educates users about cybersecurity concepts, as well as some common attacks they may encounter through interactive games.

Difference From Existing Work

Cybersecurity games online usually teach the user about cybersecurity concepts and attacks through rote memorization and have the user complete multiple choice and fill-in-the-blank style questions. We think it is more useful if the user is able to implement some attacks on their own with visuals to help them understand the underlying concepts.

Implementation Overview

In this project, we will be using Python and/or Java, to implement a GUI interface for the user to interact with. There will be a window popup that displays the text of the story line with some options given for the user to pick. The goal of the game is to successfully mitigate or perform an attack the user encounters. The outcome of the game will also depend on what the user's choices are -- they can either be negative or positive.

Game Options:

The user will be able to pick from 3 different storylines/events from the main menu--some of our ideas include:

- Buffer Overflow Attack
  - Show the user a visual representation of the stack and how overflow works
  - The user will select from a list of choices as to what offset to make the address the return address would point to
  - The user would also select the size of the buffer they are using to overflow the buffer and how that affects the stack
- SQL Injection
  - The user would be told how and why SQL injection works
  - The user would be told to write an query to obtain information a web application would not normally allow a user to see (a list of users, password hashes, etc)

Team Members:
Ross Young
Alicia Yong

Project Proposal

- Password Cracking/Password Strength
  - The user enters a password that is weak (seven characters or less with no numbers or special characters), and we will show how quickly the password can be cracked when a password is extremely weak. We will print out the various password hashes of all the permutations of lower + upper case letters and stop when we find a hash that matches the user's password hash.
  - User will also have to decide what dictates as a good or bad password, and based on their choice we will explain why their option is ideal or not
  - Can also tie in to educating the user on how to properly manage passwords
  - Based on what they pick on what is the "best" way to properly manage passwords, we will explain why that is a good or bad choice
- Physical Aspects of Cybersecurity
  - The user will have choices on what to do based on the event happening (ex: the user notices that someone is following them to an authorized room, what should the user do?)
  - Based on user's choice the events will be negative or positive
  - Educate users on how cybersecurity isn't just about keeping your system safe, but the environment that your system is in as well