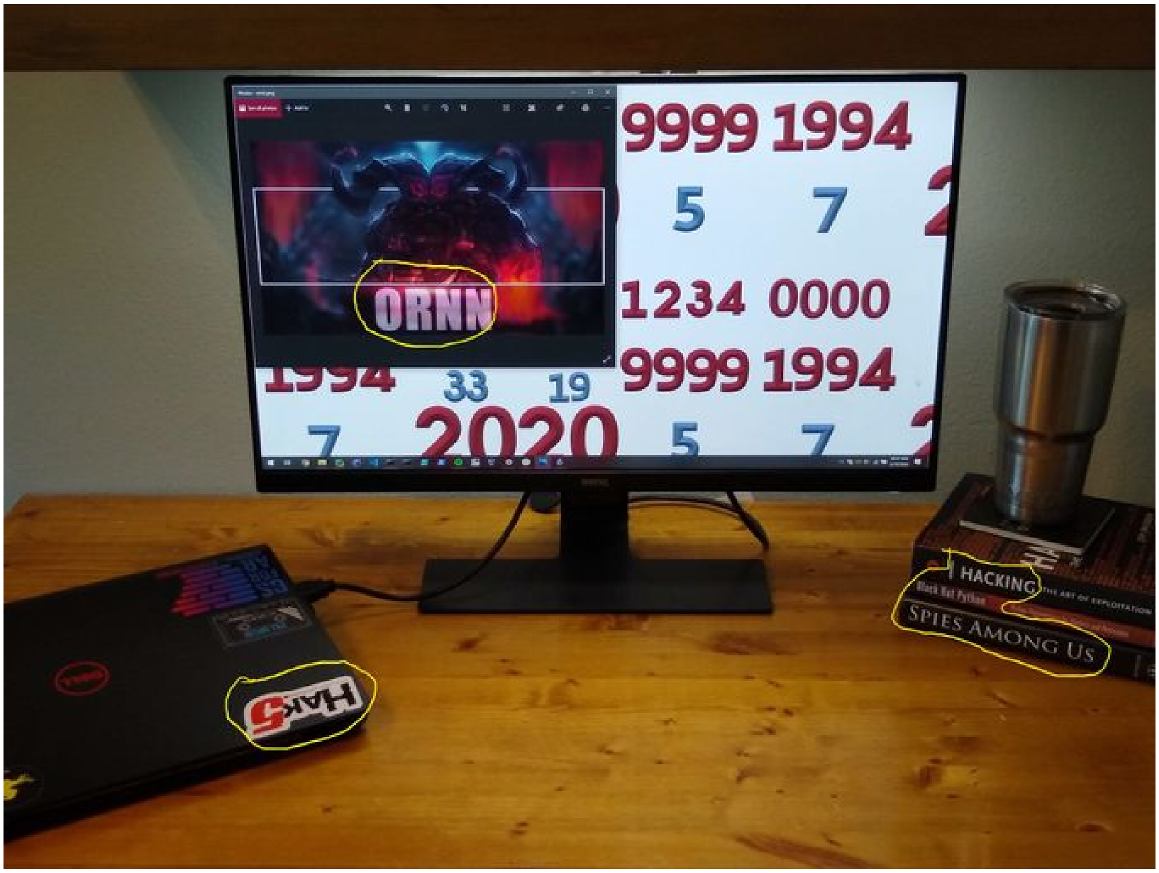
Johnny Hash Teacher Workout Instructions

Introduction

This workout is built in the style of a CTF and assumes that everyone has the basic knowledge of what a cryptographic hash is. This article from Auth0 provides an easy-to-understand overview of hashing and basic password security practices. The students will be provided a username, an unsalted MD5 hash, and a picture. Their job is to create a word list from words and numbers that appear in the picture and see if they can “brute force” the password.

The Gist

The password for the login will be generated based off of a preset word list. This word list contains a combination of five words (circled below) and any number shown on the screen background. *Book titles and company names are considered to be one word.*



To make things a little easier, students are given a password policy that is used to help determine password length and complexity.

Password Policy:
1. Must contain whole words only
2. Be a minimum of eight characters long
3. Must contain at least one upper-case letter
4. Must contain at least one digit

For example, *Hacking7* and *9999Ornn5* are a valid passwords. Password *Ornn5* **does not meet the length constraints** and is therefore not a valid password.

Depending upon the level of the students **there are basically two ways of solving this problem**:

1. **Brute Force** - Manually create combinations of words and numbers and place them in a file with a new line between each guess.
2. **Create a simple program that will**:
    a. Create passwords based upon the list of provided words and numbers
    b. Check if password length is greater than eight characters long. If not maybe append a number to the beginning.
    c. (Optional) Calculate the MD5 hash for each created password.
    d. (If C) Programmatically compare the resulting hashes with the provided hash

You can build the program with Python in about 10-15 lines not counting the word list.

ⓘ A word or number is only used once per password. Example: *Hak50000Hak5* is not a valid guess as the word *Hak5* appears twice. *9999Hak55* **is valid** as the 5 in *Hak5* is part of the company name.

Once students have a list of passwords guesses, they can upload the file to the JohnnyHash where it will automatically calculate and print out the MD5 hash for each guess. Compare the generated hashes with the provided one. If one of the passwords created an identical hash as the one provided at the beginning of the workout, they have guessed the password. Log in with that password and the workout is complete!

ⓘ If students went for option 2 *and* completed options C and D, they can skip the manual hash comparison and simply log in with the correct password