**Lesson 2 – Every Bit of the Internet**

**\*\*Instructions:** Please change the text color of your responses to red text. Please organize the endings to each page.

**ACTIVITY 2.1.3 – Password Strength -- Strong**

**VOCABULARY**

| System administrator | **A person that managers computing resources for a group or organization.** |
| --- | --- |
| Brute force attack | **An attack where an attacker tries every possible combination of passwords to try to find the correct one.** |
| authorization | **Giving permission, such as to access information** |
| authentication | **Confirming identity with private knowledge** |
| Multi-factor authentication | **Authentication with something that is not a password, such as a self-set security message.** |
| GUI | **A graphical interface that the user interacts with to use a program.** |

Explain why using a passphrase with words from the middle of the dictionary represents an average time. (Step 9)

| **Because the time required to brute force a password is proportional to its location in the dictionary, due to each password being checked in order, a password in the middle of the dictionary has the middle of the times, which is the average time.** |
| --- |

Explain why finding a two-word passphrase takes so much longer than finding a one-word passphrase. (Step 9)

| **A two-word passphrase has many more combinations, and since the number of combinations increases exponentially with each symbol that is added to the password, brute-forcing a two-word passphrase takes exponentially more tries than brute-forcing a one-word passphrase.** |
| --- |

Since an average search time takes too long, data estimates have been provided for you. Using these estimates, or your own test results, fill in the missing entry by calculating how many times longer it took to match a two-word-and-digit password. (Step 12)

| Algorithm | Average Time | Times Longer Than Previous Analysis |
| --- | --- | --- |
| One word | .01 seconds | - |
| Two words | 40 seconds | 4,000 |
| Two words and a digit | 1,200 seconds or 20 minutes | 30 |

Fill in the blank fields, predicting the performance of functions that will take too long to run. For each calculation, assume the same increase in search times as *either*the increase from two-words to two-words-and-a-digit *or* the increase from one-word to two-words, whichever is applicable. (Step 13)

| Algorithm | Average Time | Times Longer Than Previous Analysis |
| --- | --- | --- |
| One word | .01 seconds | - |
| Two words | 40 seconds | 4,000 |
| Two words and a digit | 1,200 seconds or 20 minutes | 30 |
| Two words, a digit, and a symbol | 36,000 seconds or 600 minutes or 10 hours | 30 |
| Three words (no digits, numbers) | 160,000 seconds or 2,666.67 minutes or 44.44 hours | 4,000/90 = 44.44 (4,000 times longer than two words) |
| Three words and a digit | 480,000 seconds or 8,000 minutes or 133.33 hours or 5.56 days | 30 |

Why do you think a good security policy requires a user to include numbers and symbols in a passphrase? (Step 14)

| **These will cause the passwords to take much longer to brute force, as they greatly increase the number of possible combinations before the password is guessed.** |
| --- |

What would using capital letters randomly in a passphrase do to the search time? Use an example in your answer. (Step 14)

| **Using capital letters would double the amount of possibilities for each character, causing the number of combinations before the password is guessed to become 2^n times higher, where n is the number of letters in the original password.** |
| --- |

**Using Repl.it, provide a digital link of your modified code for Steps 17 – 19 in Canvas and in the space provided below.**

| https://replit.com/@KyleHuang5/CSP-213-multifactorauth |
| --- |

Why are individual security measures important to the entire internet? (Conclusion)

| **Security measures are important to the entire internet because good security practices by all individuals helps to decrease the number of entry points hackers could have to access important information.** |
| --- |

How do strong passwords and multi-factor authentication increase security to a restricted application or service? (Conclusion)

| **Strong passwords make brute-force attacks infeasible, as they will take too long to brute-force or guess, and multi-factor authentication can stop an attacker even if they do obtain the password by requiring personal information that only the authorized user knows or another form of hidden information, such as an alert on a device that is already logged in.** |
| --- |