# Access Control Assignment – Password Cracking Questions

CPSC 348 – Computer Security

Fall 2021

Name: your\_name

**Pre-Assignment Questions**

|  |  |
| --- | --- |
| ***Wordlists.*** |  |
| 1. Read this article from Rapid7, [“Brute-Force and Dictionary Attacks”](https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks/). In your own words, what is a wordlist? |  |
| 1. In the Github repo, open the small wordlist. Skim the first 100 or so passwords and tell me which one is your favorite. |  |
| 1. How many lines are in the small wordlist? |  |
| 1. How many lines are in the large wordlist? |  |
| 1. Read about [some of the wordlists sold by the team at John the Ripper](https://www.openwall.com/wordlists/). (You can stop at “Three good reasons to purchase the wordlists”.) How big is it? How many entries does it have? How many different languages are included? |  |
| 1. Read about [the CrackStation wordlist in short first section of this article, “What's in the list?”](https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm). How big is it? How many entries does it have? |  |
| 1. ***Word-mangling.*** [Read about word-mangling](https://www.tunnelsup.com/getting-started-cracking-password-hashes/). In your own words, what is it? |  |

**Post-Assignment Questions**

Each of these questions refers to a table in “Password Cracking Results.xlsx”.

|  |  |
| --- | --- |
| 1. Look at the first table *Salted vs. Unsalted*.    1. Look at the first row. How much time did test case 5 take? Test case 9? What was the percent increase?    2. Similarly, look at the third row. By what percent did the time increase between test cases 7 and 11?    3. Which wordlist was used in cases 5 and 9? Which in cases 7 and 11?    4. Why are attacks using the large wordlist slowed down so much more by salting than attacks using the small wordlist? |  |
| 1. Look at the table *Small vs. Large Wordlist*.    1. Look at the first row. How much time did test case 1 take? Test case 3? What was the percent increase?    2. Similarly, look at the second row. By what percent did the time increase between test cases 2 and 4?    3. Was word-mangling used in cases 1 and 3?    4. Was word-mangling used in cases 2 and 4?    5. Why are attacks using the large wordlist slowed down so much more by word-mangling than attacks using the small wordlist? |  |
| 1. Look at the table *Small vs. Large Wordlist.*    1. For each row in the table, how many passwords were cracked with a small wordlist? How many with a large wordlist? What was the increase?    2. What is the average increase across all rows? |  |
| 1. Look at the table *Word-Mangling vs. None*.    1. For each row in the table, how many passwords were cracked with word-mangling? How many with none? What was the increase?    2. What is the average increase across all rows? |  |
| 1. Based on your answers to the previous two questions, it is more important for an attacker to use word-mangling or have a large wordlist? |  |
| 1. Compare the time to crack test case 11 to that of test case 12.    1. Which took longer? By what percent?    2. How may entries are in “sha1-salted.txt”? How many entries are in “sha1-salted-tiny.txt”?    3. Which wordlist was used in test case 12? Was word-mangling used? Were the hashes salted?    4. Why did test case 12 take so much more time than test case 11, despite having fewer hashes to crack? |  |
| 1. Compare the time to crack test case 9 to that of test case 13. What is the only difference between the test cases (besides number of passwords cracked and time to crack)? Why does that difference cause such a dramatic difference in the time to crack? |  |
| 1. Which three hash algorithms did you crack in this assignment? Which of them are still considered secure today? |  |