Section 6

In this password cracking competition, the main approach was to implement a dictionary attack and rule-based attack because now without any prior knowledge of the password, a simple brute-force attack does not guarantee huge success. Also, I decided to not use the rainbow table because the table generation time to cover a password length of 6 characters (with each character having 95 possibilities) and above is unfeasible. The software used was **Hashcat.**

Dictionary attack

I slowly gathered a list of dictionaries over the Internet and iterate through each of them with Hashcat attack mode 0. The results were tabulated below.

Dictionary	Passwords found
realhuman_phil.txt source	65
realuniq.lst source	79
rockyou.txt source	56
wpa2-wordlist source	81
hashesorg2019 source	143
Md5decrypt-awesome-wordlist source	80

Rules-based attack

After I have tried all the dictionaries that I gathered, I switched to a rule-based attack with different sets of rules that is readily available in the Hashcat package. Rules such as best64, toggle1, toggle2, toggle3, toggle4, oscommerce were applied across the dictionaries that I gathered. However, **only 2 new passwords** were recovered in this attack.

To conclude my attempt, I managed to get an effective recovery rate of 97.9% (145/148) using both dictionary and rule-based attack. If I were to fully commit myself to complete the recoveries, a few approaches that I would take is to gather more diverse(e.g. different languages) and quality dictionaries, and apply different rules again on those dictionaries. Also, I would consider Combinator Attack with the dictionaries that are based in common words across different languages to generate possible phrases.