Assignment 2 Solution – ENGI 9807 (Part 03)

Sourav Barua

20199158

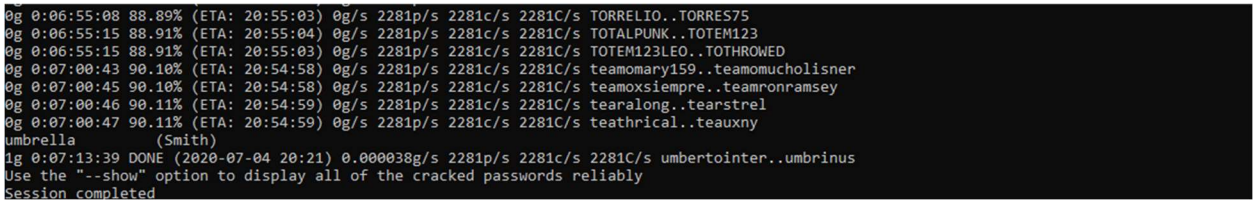
Part 3: Password Cracking

I have installed the tool **John the Ripper** on my WSL2 Kali Linux subsystem. The machine has an AMD Ryzen 7 3750H processor. Base speed of the processor is 2.30 GHz. And it has 16GB RAM.

- I created two user account and named Smith (pw: umbrella) and Michelle (pw: apple123). Then, I ran the command ***unshadow /etc/passwd /etc/shadow > passwords.txt*.** The **unshadow** tool combines the passwd and shadow files and outputs to a file named *passwords.txt,* so John can use them.
- Then I first tried to run the *john* command supplying the generated *passwords.txt* file without any other options. The command is ***john /etc/passwords.txt***. This command below tells JtR (John The Ripper) to try "simple" mode, then the default wordlists containing likely passwords, and then "incremental" mode. This command was running in my machine for 11 hours and it did not get completed.
- Later, I downloaded a wordlist from *crackstation.net,* it contains 15 GB collection of words (1,493,677,782 words) to use as JtRs wordlist. The file name is ***realhuman_phill.txt.***
- After that, I have run the john command with the option **–wordlist** where I supplied the name of the downloaded wordlist. Here is the command that I have run –

  john /etc/passwords.txt --wordlist=/mnt/d/realhuman_phill.txt --users=Smith

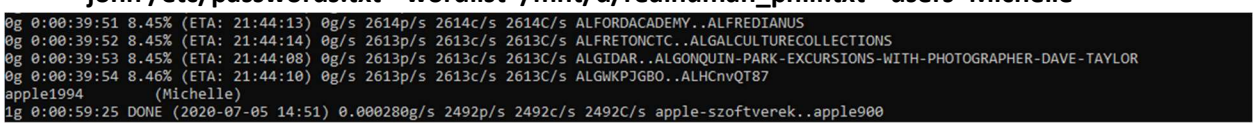
  Here the - -wordlist option tells about the wordlist to be used for the cracking process and the - - users option tell about the user name for which JtR needs to crack the password.



After 7 hours and 47 seconds John the ripper cracked the password.

- I tried the same command for cracking the second username's password (Michelle, pw: apple123). For this, I have run the command –

  john /etc/passwords.txt --wordlist=/mnt/d/realhuman_phill.txt --users=Michelle



It took around 59 minutes to crack the password for this user account. I think as the password contains ‘a’ as its first character, it took less time to be there and get the match.