Tutorial 3: Hybrid Attack

* Hybrid attacks use a dictionary alongside a brute-force attack
* In this example we’ll be using hashcat to apply a mask, like in tutorial 2, but to a dictionary instead.

Process:

* Check out the directory pwcrack/3/
* Look at prob1.txt
  + From the description we know that the passwords be an episode of Spongebob from season 1 followed by 4 digits. There will be no capital letters or spaces.

1. We have to generate a list of season 1 Spongebob episodes. Do this any way you like. The only formatting that is required is making sure that each episode is on its own line in the dictionary and that the episodes are formatted according to the above criteria. Save this as a .txt file.
2. Create another list of just the hashes from prob1.txt. Save as a .txt file
3. There are two methods of applying masks to a dictionary:
   1. These masks work the same way as the brute force method
      1. Pre:
         1. Hashcat attack mode 7 (-a 7)
         2. Hashcat -a 7 <hash\_list> <mask\_definition> <dictionary>
      2. Post:
         1. Hashcat attack mode 6 (-a 6)
         2. Hashcat -a 6 <hash\_list> <dictionary> <mask\_defintion>
   2. Since we want to add 4 digits to the end of the dictionary, we will use the post attack mode. Our mask definition will be this: ?d?d?d?d
4. Create our hashcat command:
   1. Hashcat -a 6 -m 1400 <hash\_list> <dictionary> ?d?d?d?d
      1. Our attack mode is 6 (-a 6)
      2. Our hash function is SHA256 (-m 1400)

An Example Command:

1. A screenshot of a cell phone

   Description generated with very high confidenceRun the command. The output should look like this:

Try on Your Own: prob2.txt

\*Hint – use the pre-mask mode\*