**a) Dictionary Attacks**

**1. Search online for the \RockYou word list". What is it? Where does it come from?**

**Do you think it is a suitable list to crack real-life passwords?**

**A:** RockYou wordlist is a 139MB (~70MB compressed) text file available online, [1], which contains a comprehensive list of passwords. This file can be used as a dictionary to crack passwords.

**What is it -**

This file is a collection of most common, most used and easily guessable passwords used in the world. This file serves as a dictionary for penetration testing. (Kali Linux)

**Where does it come from –**

It comes from the BackTrack Linux distro developers Offensive Security Limited. It is now available offline in the Kali Linux versions, which is the current version based on BackTrack. Kali is a debain based linux used in penetration testing

**Do you think it is a suitable list to crack real-life passwords –**

No, users choose more complex passwords in real life. This list contains realistic strings which are sub passwords but not whole passwords. This list cant be used to demonstrate how not to choose a password.

**2. What do we learn about how most users picked their password?**

**A:** We learn that most users pick passwords based on their personal preferences, such as family, pets, location or sports clubs. Also a possible combination with important dates such as birthdates and anniversaries.

**3. How would you define “weak” and “strong" passwords in general? Why?**

**A:** Weak passwords are ones which are common nouns and those which are common words across the globe. (example, cities, names etc) A continuous sequence of characters, or predictable upper and lower case characters are also weak passwords.

Strong passwords are completely random. However, completely random passwords are hard to remember. Hence, a combination of random string, and a not so random easy to remember string can also be considered a strong password (for example, not so popular noun, plus few random digits) Using a combination of upper and low cases also make a password strong.

**4. Optional question: Is your favorite password in the list?**

Unfortunately, yes. Part of my favorite password was part of the list.

**b) Brute-Force Attacks**

**A:** Brute force attack checks all possible combinations. The number of possible combinations can be given using the following formula,

Let u =|U|, l =|L|, d =|D| and s = |S|, and let c = u + l + d + s and n be the length of the password, the number of Combinations are

**cPn**

Increasing n causes the password combinations to grow faster.