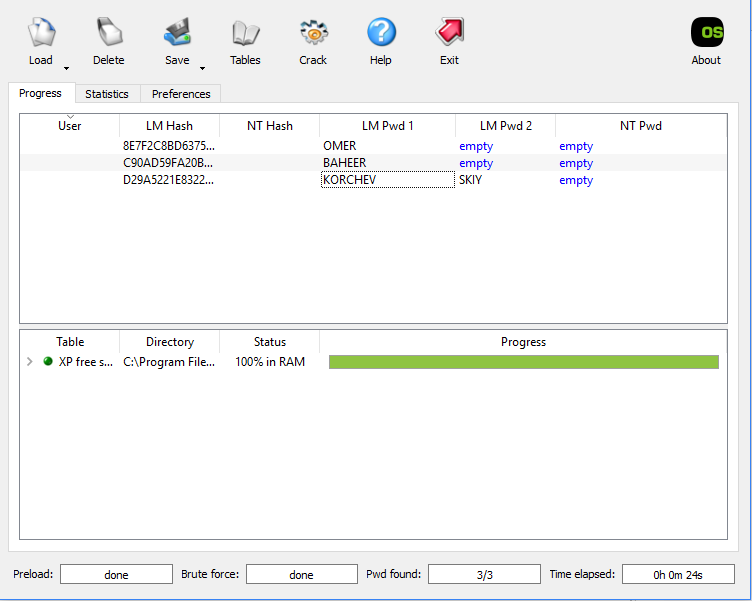
# Part 4



# Part 5

1. The salts effect the hash by making them more unique because they randomly generate characters that have no relation to the actual password of the hash and while it is possible to crack the password with just the hints even with the most difficult of encryptions without a salt the algorithm will always give the same the hash for the same password. With a huge table there will be multiple hints for the same hash. Salting causes brute force hacking to be more difficult and instead it requires double the effort in each attempt
2. With the encryption algorithm given to us with a null password, the algorithm depends heavily on the characters given and with a null character it will return nothing. Having a password with 8 or less characters can be cracked by using brute force within a few minutes.
3. The algorithm in this lab would output with the same length hash as the password given in due to the fact that a null character will return a null character. This would give the hacker the length of the password to search an using some random characters it can check whether the hash is in a region and brute force a smaller sample space with a few calculations. Example the characters in the hash are very independent of each other which the attacker could use to reduce the space of the region within the password. Confusion and Substitution are two good cryptographic hash functions we can use because we can substitute and mix around the characters of the hash to make the length of the password differ from the actual password length. Example a null character can be replaced with a different character depending on the location of the password within the database.
4. After 3 attempts let the user wait 30 secs to get another 2 attempts and if those 2 attempts are incorrect set the time limit to be 4x the previous penalty. The pros of having a shorter length is that its more convenient for the user to enter his password, the con is that if the time is short the chance of cracking the password will increase since the attacker can attempt guesses faster. The con for a longer time period is that the user will get frustrated faster with password attempts. The pro is that it is harder for the attack to crack the password.