PASSWORD CRACKING LAB

Gabriel Naples

gjn5070@psu.edu

Table of Contents

Section I: Introduction

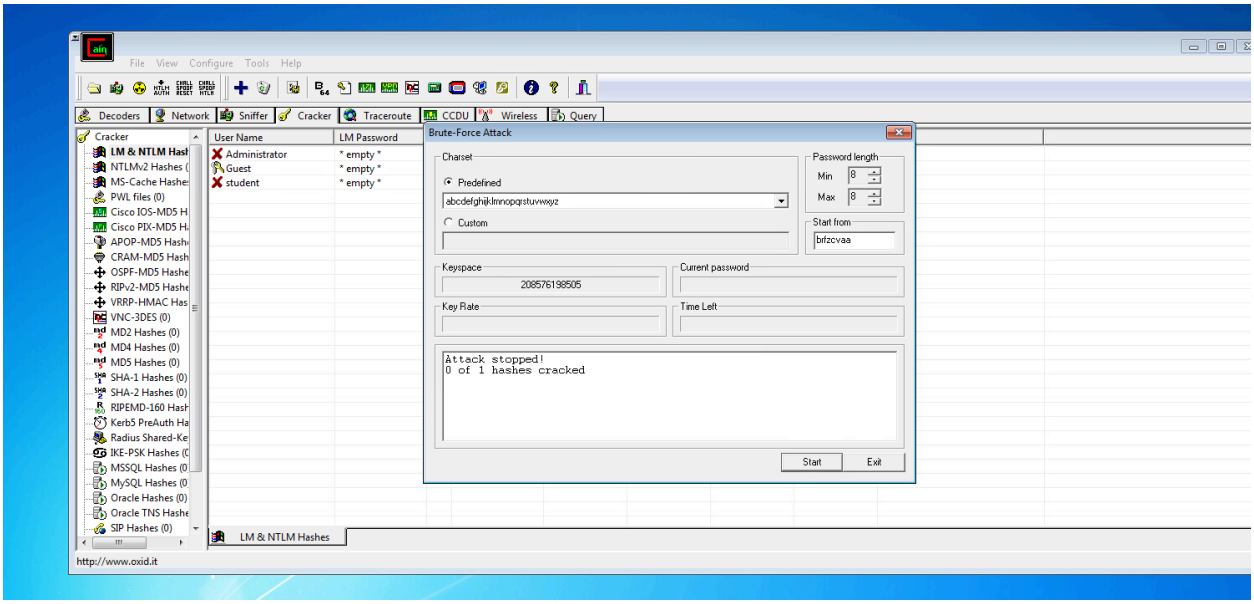
The purpose of this lab is to learn about the process of password cracking. The process of obtaining and cracking passwords is commonly used by hackers, for malicious means, and penetration testers to test the security of a network or system. This lab teaches the basics of how technical professionals would go about breaking into a password and the different methods to do so including: brute force attacks and dictionary attacks. This lab teaches how a strong password could take millennia to crack, yet a simple one could be cracked in as little as a few seconds.

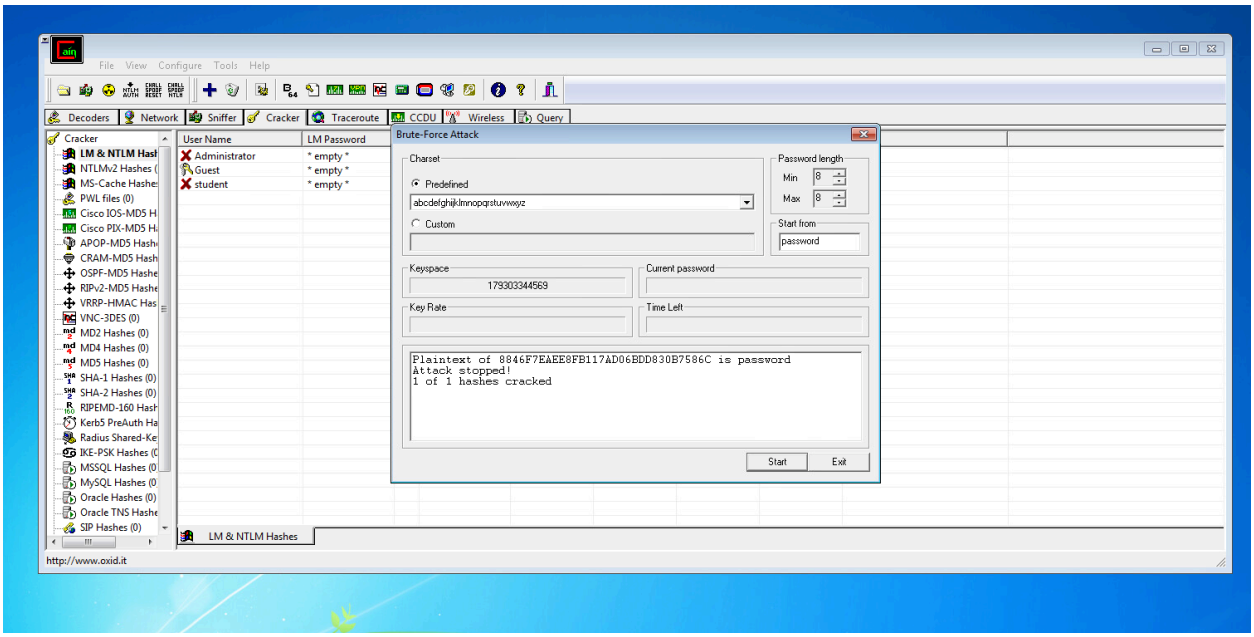
I expected to learn how to use a simple program to carry out both a password attack and a dictionary attack, and also about the different methods of cracking a password. I also expected to gain a deeper understanding about the process and gain some technical skills to carry out these attacks myself.

Section II: Task 1 (brute force attack)

A brute force attack tries every possible combination of letters and numbers and matches that hash with the one you are trying to crack until it lines up. A brute force attack can be very strong against a weak password because eventually it will get the correct password. For example, if the password is a simple string of numbers like “12345678” then a brute force attack will gain that password rather quickly. However, a brute force attack could take ages against a strong password. If the password contains a combination of letters, numbers, and different characters then a brute force attack could take hundreds of years to complete, it varies greatly depending on the computing power available to the attacker. This is the major

drawback of a brute force attack.

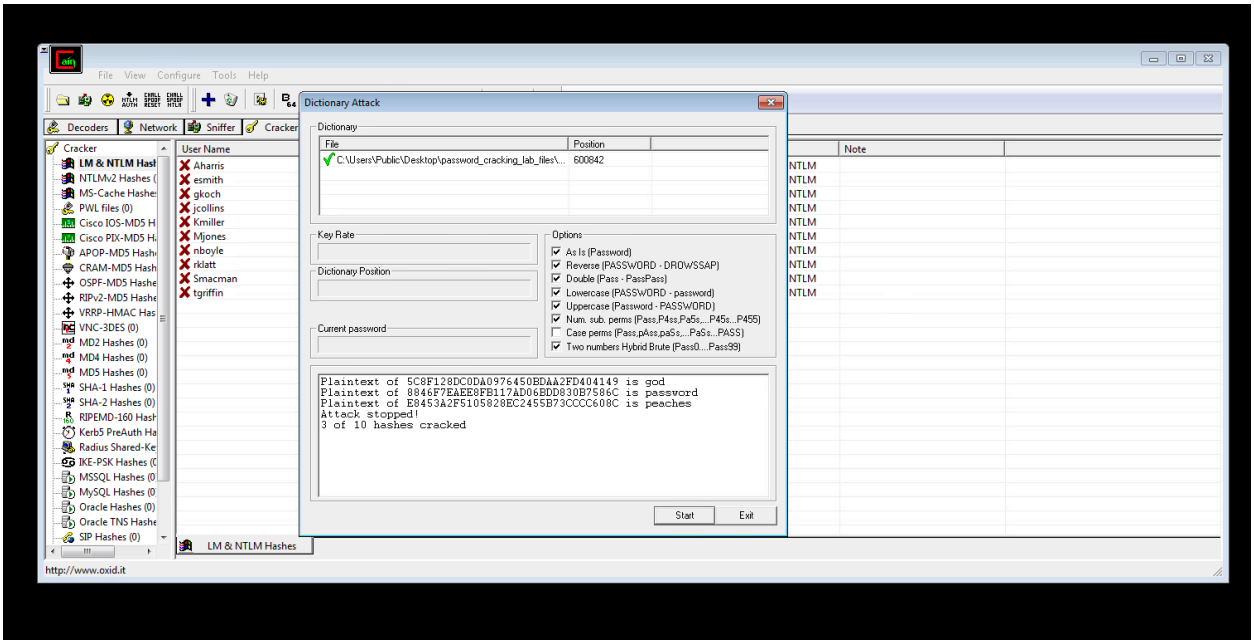


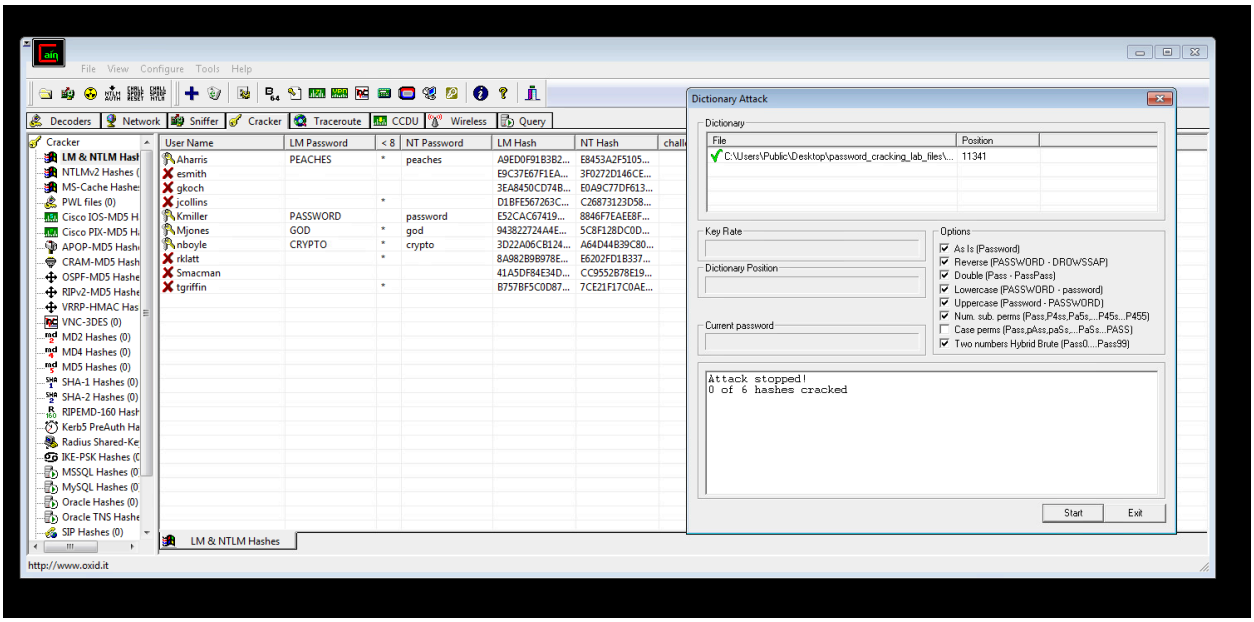


Section III: Task 2 (dictionary attack)

A dictionary attack is when an attacker runs a file full of common phrases and combinations frequently used as passwords against the hash they are trying to crack. The upside of this type of attack is that it is very quick and very efficient to find the passwords, as

long as the dictionary being used is a good one. However, a drawback to this attack is that if the dictionary being used doesn't contain the password inside of its file that matches the one used then it will never figure out the password, so while it is quick it's not always effective. A more effective use of this attack would be a hybrid attack where it uses the values stored in the dictionary along with varying them by adding numbers and symbols to the end of the passwords to test even more possibilities, however this type of attack is longer than a regular dictionary attack.





Kmiller	password
Smacman	
gKoch	
Mjones	god
Tgriffin	
rKlatt	
nboyle	crypto
Esmith	
Jrollins	
Aharris	peaches