Information Security COMP 421

Spring 2022

Course Project Proposal

Topic: Gmail-Brute

Group Members:

Hamza Zahid (22-11157)

Muhammad Taha Bin Nauman (22-10279)

Yesheb Mark (22-10281)

Project description

We are working on a project called the Gmail brute force attack. A brute force attack is one of the more prevalent attacks that contribute to roughly 5% of data breaches online. The tool can be used to ethically (or unethically), that depends on the user. Our purpose as programmers is to provide enhancements to the code and help improve the tool overall.

Gmail brute force tool allows us to gain access to a Gmail account. This is done by a trial and error method where we code the program in such a way that it tries to randomly guess the passcode by applying different combinations of alphanumeric/special keys to the field. It is a highly effective method since a large portion of breaches happen through brute force attacks. Our program is divided into two types of code. Python, which is 90% of the code as well as the HTML client for the user interface. Changes made to the HTML file in comparison to the Python code would be rather easy to contribute to since it is only going to be a visual overhaul, to provide an interface that is a bit more visually friendly. The Python part of this tool however is the real deal which helps us get the job done. In order to make these changes (enhancements), we would have to run the code first of all and see where the program lacks. To do that we have a number of steps to run the tool (mentioned below). Just to be on the safe side we would implement these steps on Kali Linux. We would like to structure the code in a way that makes it more efficient while also increasing the input that it takes for the passwords (in terms of alphanumeric keys).

Steps

To implement our tool, we would first have to install python version 3 in Kali Linux operating system. We will be using Visual Studio Code as our text editor/ide. We will clone the git repository to create the copy of the code so that we can bring changes to it. We will be needing Colorama, it provides a simple cross-platform API to print colored terminal text from Python Application. The code for HTML file has already been provided however we would like to make changes to it so that it becomes a little more visual friendly. We need to install Pysocks as it our major requirement. To execute the program, we need to use the command terminal. Next, we will execute the "chmod +x *" it's used to change the access permissions of files and directories. The "crack.py" file will be used to fetch the passwords once the program is running it will prompt us to enter the path for the email address file where are stored in txt file. In the next step we will extract guess passwords from another txt file where default wordlists are stored. There is no need for any default proxy to be used.

Outcome

The possible outcome after our enhancements is to make the code more user friendly by adding comments as well as make the tool more effective when used ethically.