ЦЕЛЬ

Разработать приложение подбора паролей.

Используемые языки программирования, технологии и протоколы:

* + язык программирования C# и технология WPF;
  + brute-force attack (метод прямого перебора);

ПАРОЛЬНЫЕ АТАКИ

Аутентификация пользователей (подтверждение их подлинности), обеспечивается в первую очередь путем использования парольной защиты.   
Слабая парольная защита является одной из основных причин уязвимости компьютерных систем к попыткам несанкционированного доступа. Большинство компьютерных взломов осуществляются вследствие несовершенства парольной защиты.

Самым популярным паролем по-прежнему остается «1234». На втором месте «12345678», на которые приходится 14 % взломов. Благодаря подбору только этих двух паролей, в прошлом году хакеры похитили с банковских счетов несколько миллионов долларов.

ВЗЛОМ ПАРОЛЬНОЙ ЗАЩИТЫ

Для взлома парольной защиты используются следующие методы:

1. Узнавание пароля.

2. Угадывание пароля

3. Словарная атака.

4. Использование программных закладок

5. Удаленный доступ к компьютеру.

6. Непосредственный доступ к компьютеру.

7. Перехват паролей с использованием технических средств.

8. Метод прямого перебора (brute-force attack). Этот метод предполагает прямой перебор всех возможных комбинаций всех допустимых в пароле символов.

Перебор символов осуществляется до тех пор, пока не будет найдена нужная комбинация.

Программная реализация метода автоматического перебора позволяет взломать любой пароль, но для сложных паролей может потребоваться значительное время, особенно учитывая возможное переключение верхнего и нижнего регистров и раскладки клавиатуры.

ПРИЛОЖЕНИЕ ПОДБОРА ПАРОЛЕЙ

На рисунке 1 представлен визуальный интерфейс разработанного приложения подбора паролей.

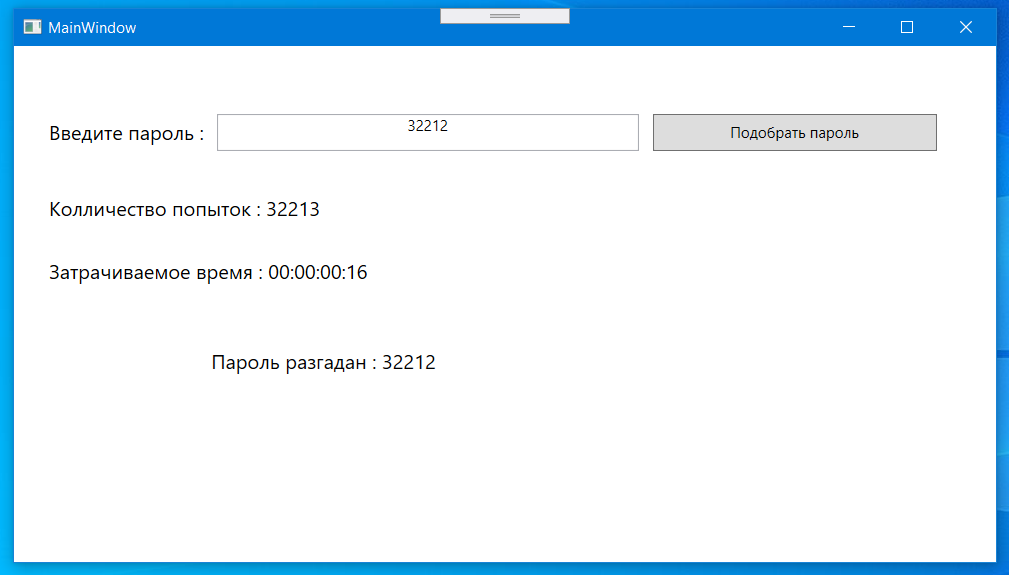


Рисунок 1 – Визуальный интерфейс приложения подбора паролей

На рисунке 2 изображен код функции password\_generate. Данная функция осуществляет перебор паролей до того момента пока пароль не будет подобран.



Рисунок 2 – Функции password\_generate

Проведенное исследование устойчивости паролей к взлому с использованием программы «Подбор паролей», на компьютере c процессором Intel Core I3-7100U (2,4GHz) показало следующее результаты, представленные в таблице 1.

Таблица 1 – Результаты выполнения программы «Подбор паролей»

|  |  |
| --- | --- |
| Пароль | Время подбора (мин:сек) |
| 86723 | 0:1 |
| 42354687 | 4:19 |
| !Za2 | 2:3 |
| @32&!1 | 3:13 |
| 693#@ | 0:5 |
| Asmq | 0:8 |
| vadim | 1:22 |
| sDAWzxs | 7:12 |
| AsZC | 0:7 |
| 1AsZC@ | 8:6 |

ВЫВОД

Было разработано приложение «Подбор паролей». Данное приложение работает по принципу brute-force (простого перебора). Данное приложение использует не самый оптимизированный принцип перебора и работает в однопоточном режиме, что замедляет скорость обработки паролей. Используя более оптимизированный алгоритм, а также многопоточный режим работы можно добиться большей скорости подбора паролей. А при использовании большей вычислительной мощности можно добиться подбора сложных и даже захэшированных паролей за довольно короткое время.

Следует отметить, что использование надежных сложных паролей может создавать определенные сложности.

Серьезная парольная защита невозможна, если недостаточно надежной является надежная антивирусная защита – троянские программы, ворующие пароли, способны перехватить любой пароль, каким бы сложным и длинным он ни был.

Также рациональная политика парольной защиты предполагает использование разных по сложности и защищенности паролей при получении доступа к разным по важности ресурсам. Например, сложный пароль, как правило, не очень важен при регистрации на веб-сайте, причем в этом случае, если пароль забыт, то можно заново пройти регистрацию, в тоже время сложный пароль необходим для доступа к банковскому счету, а сохранение секретности этого пароля является крайне важным.