Практическая работа 7

Брутфорс паролей

Цель работы

Познакомиться с понятием брутфорса паролей на примере брутфорса пароля zip архива

Ход выполнения работы

1. **Подготовка окружения**

   Загружен Docker-образ Kali Linux.

   Запущен контейнер с подключением папки data для доступа к архиву.

2. **Установка инструментов**

   Обновлены списки пакетов в системе.

   Установлены утилиты john и wordlists для работы с хешами и словарями паролей.

3. **Подготовка словаря**

   В директории со словарями распакован популярный словарь rockyou.txt, содержащий часто используемые пароли.

4. **Получение хеша пароля**

   Из архива secured_data.zip с помощью zip2john извлечён хеш пароля и сохранён в текстовый файл.

5. **Полный перебор (брутфорс)**

   Запущен процесс подбора пароля методом полного перебора всех возможных комбинаций символов.

   Пароль успешно подобран, но процесс занял **около 15 минут**.

   Результаты удалены для чистоты следующего эксперимента.

6. **Атака по словарю**

   После повторного получения хеша запущен перебор с использованием словаря rockyou.txt.

Пароль был найден **практически мгновенно** (менее секунды).

7. **Сравнение методов**

   Брутфорс — работает медленно, так как перебирает все возможные комбинации символов, но гарантирует результат при достаточном времени.

   Атака по словарю — работает очень быстро, если пароль есть в словаре, но неэффективна для уникальных сложных паролей.

8. **Разархивация данных**

   С использованием найденного пароля архив успешно распакован, доступ к данным получен.

Выводы

Скорость: Атака по словарю оказалась в тысячи раз быстрее брутфорса для данного архива.

Причина: Пароль qazwsx является одним из самых распространённых и присутствовал в словаре rockyou.txt.

Практический смысл: Для реальных задач часто используют комбинированный подход: сначала проверяют пароли по словарю, затем применяют брутфорс для оставшихся вариантов.