Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Тульский государственный университет»

Институт прикладной математики и компьютерных наук

Кафедра информационной безопасности

**СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ**

Отчет по выполнению лабораторной работы №1

Выполнил

ст. гр. 230781 А. Р. Ивлев

Проверил

Асс. Чаговец Сергей Николаевич

Тула 2022

**Лабораторная работа №1**

**ИССЛЕДОВАНИЕ АТАКИ «ПЕРЕХВАТ ПАРОЛЕЙ»**

**Цель работы**

Изучение и исследование атаки «Перехват паролей».

**Задание на работу**

*Вариант №10*

1. Найти и скачать из Internet программу-sniffer «прослушать» внутреннюю сеть, выполнить подключение к http, ftp, smtp серверам во внутренней сети и попробовать обнаружить зашифрованные и незашифрованные пароли и другую важную информацию, передающуюся в незашифрованном виде в сети.
2. Найти и скачать из Internet программу взлома паролей, найти на диске в базе данных пользователя файл с паролями, и запустив программу взлома паролей, выявить слабые пароли.
3. Найти и скачать из сети Internet словарь для подбора паролей и ознакомиться с ним.
4. Попытаться взломать слабый пароль, хеш значение и алгоритм генерации хеша которого приведены в таблице 1, используя программу взлома.

SHA1: 13c1a9fb66f92a513aedfdb152a329947888a826

**Ход работы**

**Задание 1**

В качестве программы-sniffer была использована программа Wireshark.

Было произведено подключение к FTP-серверу с одного ПК на другой. Перехват пакетов производился на третьем ПК.

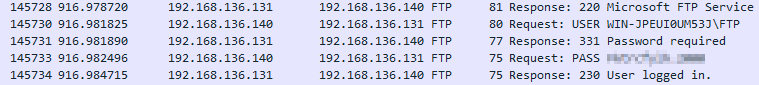


Рисунок 1 – Перехваченные пакеты (пароль скрыт)

В перехваченных пакетах были обнаружены незашифрованные логин и пароль для входа на FTP-сервер.

Также было получено содержание переданного файла.

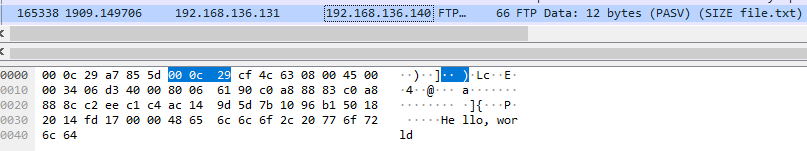


Рисунок 2 – Переданный файл

**Задание 2**

Для получения хэшей паролей пользователей в OC Ubuntu 21.10 были объединены файлы /etc/shadow и /etc/passwd командой unshadow, результат записан в passwd.txt.

Для взлома паролей была использована программа John the Reaper и ее графическая оболочка Johnny.

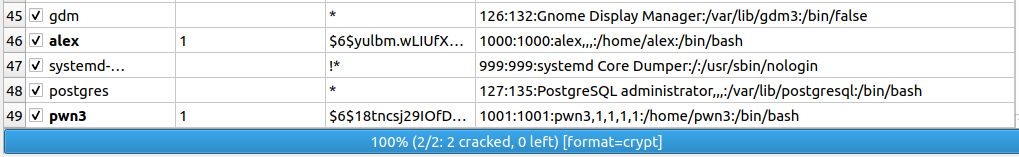


Рисунок 3 – Результат взлома паролей

В результате работы программы было взломано 2 пароля от учетных записей Ubuntu.

**Задание 3**

Из сети Internet был скачан словарь для подбора паролей rockyou.txt.

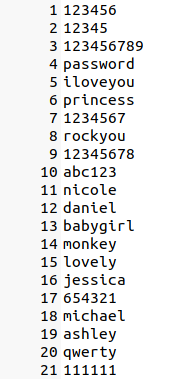


Рисунок 4 – Пример

В файле находятся наиболее популярные среди пользователей пароли. Все пароли, указанные в файле, являются ненадежными, их использование крайне не рекомендуется.

**Задание 4**

SHA1: 13c1a9fb66f92a513aedfdb152a329947888a826

С помощью программы hashcat было взломан данный хэш.

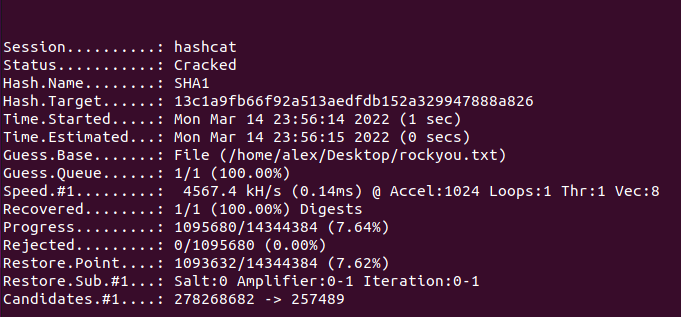


Рисунок 5 –Результат работы программы

Программа вычислила, что исходным сообщением был текст «272602».

**Вывод**

С помощью программы-sniffer была «прослушана» внутренняя сеть и обнаружены незашифрованные логин и пароль.

Были использованы программа и словарь для взлома паролей для выявления и взлома слабых паролей.