1. Переписать абонентский справочник с использованием функции

Справочник был написан с использованием функций ещё во время выполнения задания «Структуры».

https://github.com/wild4est/EltexHomework/tree/main/4.%20%D0%A1%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D1%8B

2. Имеется программа (исходный код которой приводится ниже, компилировать с ключами: -fno-stack-protector -no-pie). Вам необходимо произвести анализ программы с помощью отладчика для выяснения длины массива для ввода пароля и адреса ветки условия проверки корректности ввода пароля, которая выполняется при условии совпадения паролей.
Ввести пароль (строку символов) таким образом, чтобы перезаписать адрес возврата на выясненный адрес (есть символы которые нельзя ввести с клавиатуры, поэтому можно использовать перенаправление ввода(<) при запуске программы).

Для начала необходимо выяснить адрес возврата функции IsPassOk. Заодно можно посмотреть раздел памяти, где лежит пароль. Для этого необходимо поставить breakpoint на `*IsPassOk+29` и запустить программу с использованием в качестве ввода заранее заготовленный файл (`run < file`). В данном файле записано 12 символов „a“, что должно полностью заполнить память, выделенную на массив `Pass`.

После запуска программы можно использовать комманду `x/20xw $rbp-16` для того, чтобы посмотреть содержание стека.

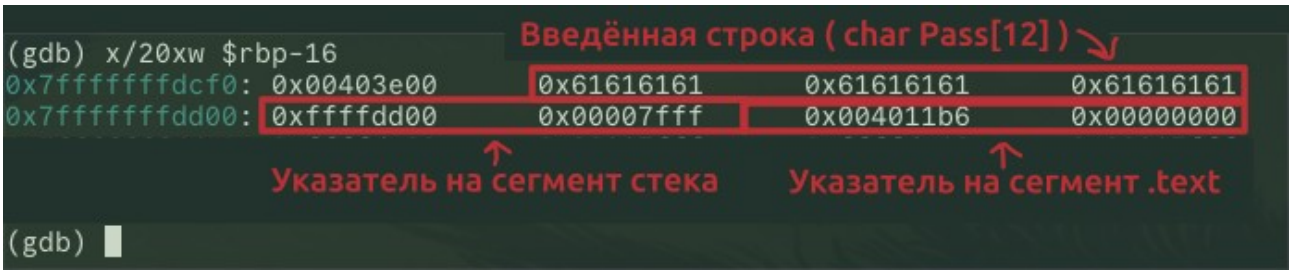

Рисунок 1 — содержание стека.

Исходя из полученной информации можно сделать вывод, что адрес возврата функции `IsPassOk` – `0x004011b6`. Так же можно увидеть, что массив Pass хранится достаточно близко к указателям. А это значит, что если ввести пароль длинее 12 символов, то он начнёт перезаписывать значение указателей. Таким образом достаточно ввести любые 12 символов, затем значение указателей на стек и адрес возврата на то место, где будет выполняться ветка else.

Теперь необходимо найти данный адрес. Для этого нужно разобрать ассемблерный листинг функции main.

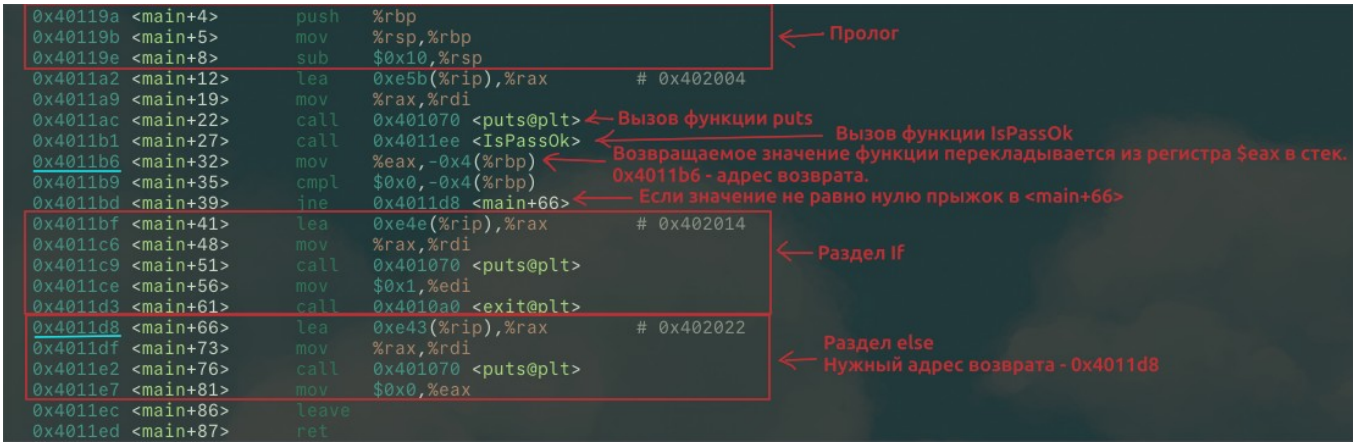

Рисунок 2 — ассемблерный листинг функции main

Подходящий адрес — `0x4011d8`.

Теперь можно записать подходящую строку в файл. Для этого выполним команду:

```
echo -e 'aaaaaaaaaaaa\xc0\xdc\xff\xff\xff\x7f\x00\x00\xd8\x11\x40' > file
```

Если запутить программу с использованием полученного файла, можно увидеть, что доступ был получен без ввода корректного пароля.

Рисунок 3 — результат запуска программы