Передо мной была поставлена задача о разработке защищенного клиент-серверного приложения, основной функцией которого является обеспечение обмена текстовыми сообщениями между пользователями. Исходным языком разработки является С++. Система состоит из двух частей: непосредственно клиента, и сервера. После запуска клиент и сервер ждут ввода лицензионного ключа. Если аутентификация проходит успешно, запускается сервер/клиент, иначе программа закрывается.

В клиентской части приложения также реализована защита от пустых полей.

В данном программном продукте реализованы защита от динамического и статического анализа, как для клиента, так и для сервера. Защита от статического анализа представлена в виде аутентификации по паролю. Принцип создания пароля основан на следующем алгоритме хэширования: пользователь вводит пароль, от каждого символа пароля вычисляется его ASCII-код, далее этот код изменяется с помощью формулы (1), потом полученный ASCII-код преобразуется в новый символ, таким образом, это и получается хэш пароля, который сравнивается с эталонной строкой, которая хранится в коде программы. Также в серверной части приложения реализован таймер. Если пароль не будет введён за определённое время, то программа закрывается. Защита от динамического анализа реализована в виде защиты от отладчика, т.е. после запуска программы сервера вызывается функция, отслеживающая присутствие отладчика, осуществляющая защиту от динамического анализа. Если отладчик запущен, то программа закрывается.

Пароль является статическим, т.е. В коде программы хранится «эталонная» строка, с которой и происходит сравнение хэша пароля. Это строка разделена на 4 части и хранится в разных местах кода программы. Полученный хэш введенного пароля посимвольно сравнивается с эталонной строкой, при сравнении идет накапливание в переменную lkt. Далее сравнивается значение переменной lkt с установленным значением, которое соответствует длине эталонной строки. Если переменная lkt не соответствует установленному значению, программа прекращает свою работу и закрывается.

Также в данной работе была поставлена задача о проведении аудита безопасности клиент-серверного приложения Зеленцовой Арины. Программный продукт (сервер/клиент) дизассемблировался, отлаживался и редактировался с помощью программы IDA Pro 7.0.

1 шаг: просмотр всевозможных функций позволил выявить реализацию динамическую защиту - функцию от отладчика такую, как IsDebuggerPresent. 2 шаг: далее проводила статический анализ, при переводе программы в строковой вид, заметила, что присутствует строка Enter Password и The time, сделала вывод, что установлен таймер на ввод пароля.

3 шаг: перешла к найденной строке программы, там заметила строку со значением «Мимесис», перед которой была найдена сама функция, осуществляющая хэширование пароля. 4 шаг: проанализировав функцию, не трудно заметить, что проверка пароля осуществляется с помощью цикла.

5 шаг: анализируя эту функцию, я смогла восстановить формулу, по которой изменяется каждый символ строки.6 шаг: теперь реализовала функцию, обратную хэшированию, чтобы восстановить исходный пароль на языке программирования С++

7 шаг: теперь введем полученные пароли в сервер и клиент. При вводе пароля в сервер, символы не отображаются, но это не повлияло на ввод пароля. Аудит безопасности завершен.