Жуковский Павел Сергеевич, 4 курс, 12 группа

Лабораторное занятие (23.11.2021)

Эксперименты над 4-ой лабораторной работой

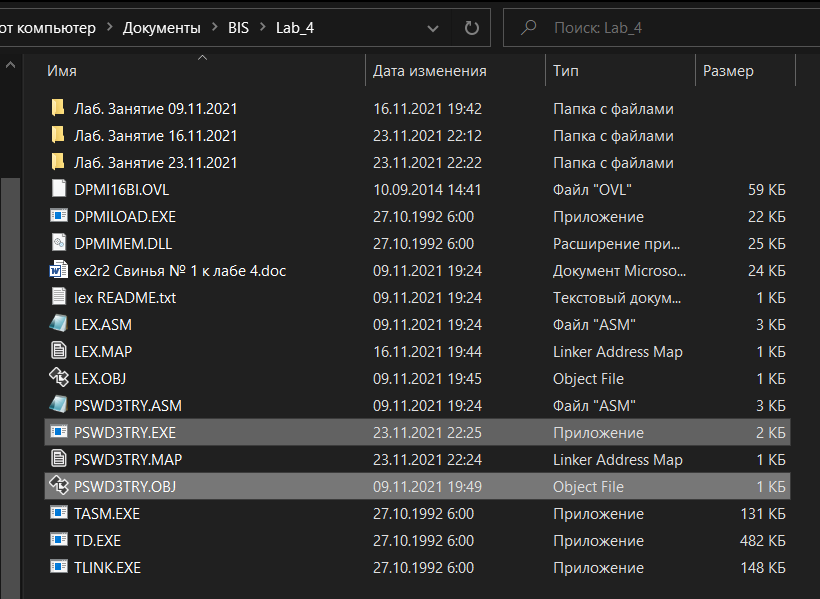
Пароль от архива: **041**

Итак, 09.11.2021 я экспериментировал с LEX.ASM, который позволяет уничтожить исполняемый модуль LEX.EXE при загрузке программы в оперативную память компьютера, а также экспериментировал с 1-ой свиньёй (которую я переименовал в PSWD3TRY.ASM), которая даёт пользователю 3 попытки на угадывание пароля, а при неправильном вводе (на всех трёх попытках) удаляет имя исполняемого модуля из реестра файлов, из-за чего происходит зависание. Я даже проверил, сохраняется ли количество попыток при закрытии терминала после одной или двух неудачных попыток, в этом случае количество оставшихся попыток действительно сохраняется, а не обновляется снова до трёх.

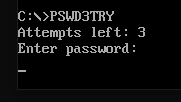
Позже, 16.11.2021, я поэкспериментировал с LEX.EXE в отладчике и сделал для себя два вывода: 1) при загрузке программы из исполняемого модуля LEX.EXE в оперативную память компьютера этот модуль удаляется не только из терминала DOSBOX, но и из отладчика TD.EXE; 2) удаление исполняемого модуля LEX.EXE происходит во время исполнения команды «MOV AX 4C00».

Сегодня, 23.11.2021, я проводил эксперименты с DHOG68 и самой маленькой программой, зримой для пользователя, но, несмотря на это, я решил, что выделю немного времени и на дальнейшие эксперименты с 4-ой лабораторной работой тоже. Так как в прошлый раз я экспериментировал с LEX.EXE, то в этот раз я проведу эксперимент с PSWD3TRY.EXE, а именно я хочу попробовать загрузить исполнимый модуль этой программы в отладчик и проверить, сохранится ли количество оставшихся попыток после неправильного ввода пароля, но уже не в терминале, а отладчике TD.EXE.

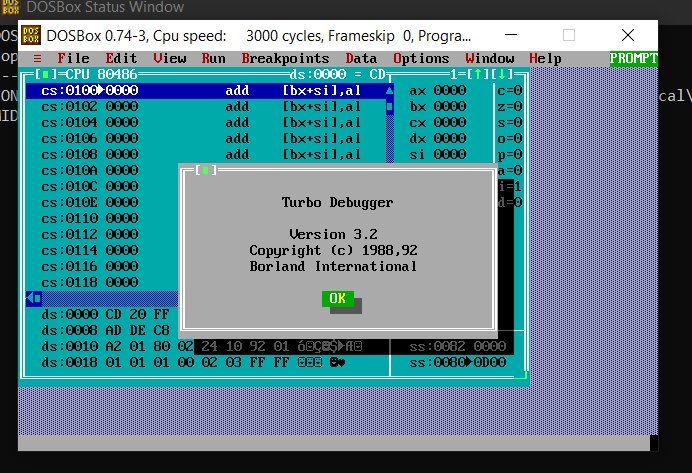
Итак, объектный модуль PSWD3TRY.OBJ и исполнимый модуль PSWD3TRY.EXE у нас уже есть (я их получал ещё 09.11.2021):



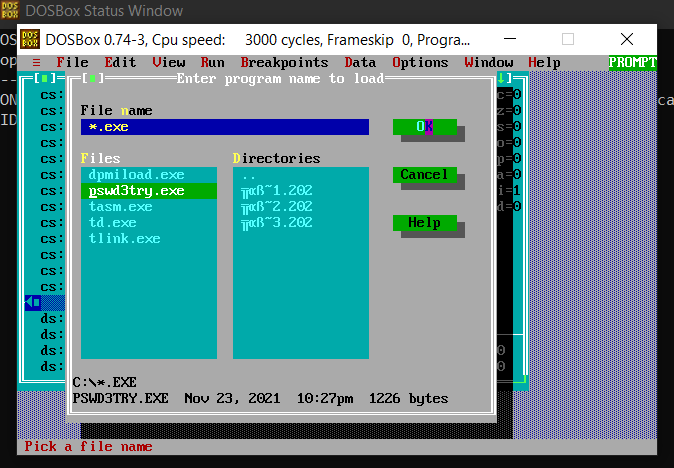
Загрузим исполнимый модуль PSWD3TRY.EXE в оперативную память компьютера и убедимся, что у нас осталось ещё три попытки:



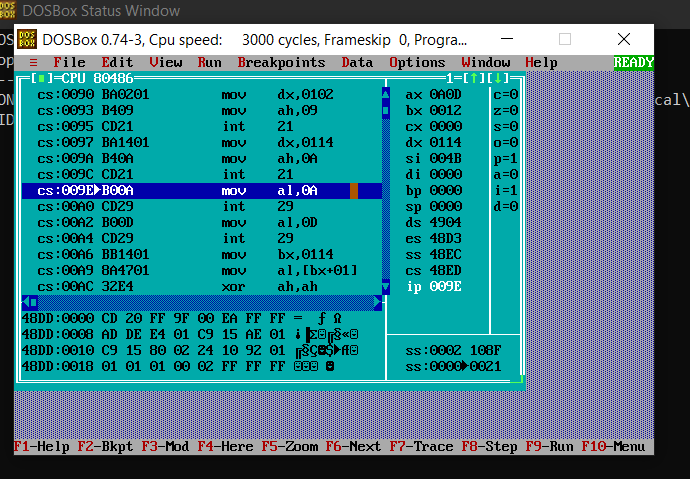
Отлично, теперь, с тремя попытками в запасе запускаем отладчик TD.EXE:



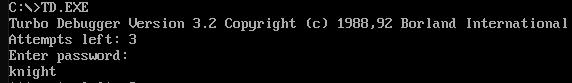
Загружаем в отладчик исполнимый модуль PSWD3TRY.EXE:



На шаге, показанном на скриншоте ниже, программа впервые запросила меня ввести какой-нибудь пароль:



Я ввёл неправильный пароль «knight»:

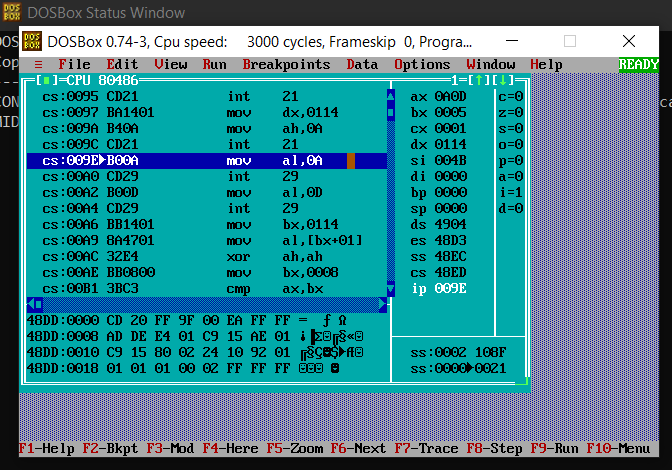


Затем, когда программа запросила меня ввести пароль во второй раз, я убедился в том, что у меня осталось 2 попытки, я снова ввёл неправильный пароль, на этот раз «queen»:

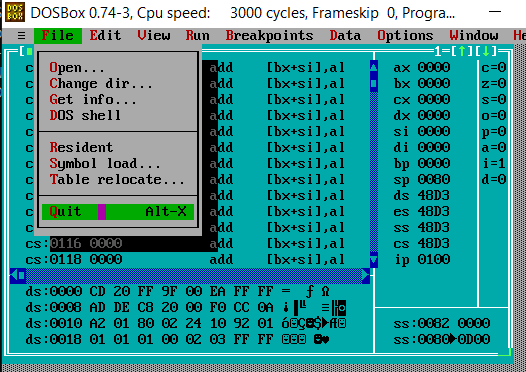


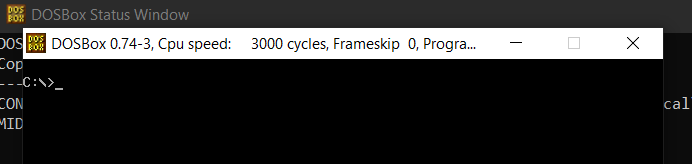
Согласно моему плану, у меня должна была остаться одна попытка.

В тот момент, когда я ввёл «queen» и нажал Enter, отладчик был на этом шаге:



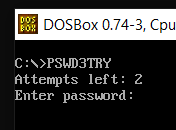
Не дожидаясь момента, пока отладчик запросит пароль в третий раз, я просто закрыл его:





После этого я проверил, сколько попыток осталось в программе. Если меньше трёх, то это значит, что программа способна сохранять количество оставшихся попыток после неправильного ввода не только в терминале, но ещё и в отладчике. Если три попытки, то это значит, что глупая редиска может злоупотреблять отладчиком, чтобы каждый раз перезагружать программу в оперативную память и начинать с тремя попытками.

Итак, я снова запустил программу и увидел следующее:



Осталось 2 попытки. То есть даже находясь в отладчике, попытки тратятся, однако у программы есть слабое место – должна пройти определенная последовательность команд, прежде чем введенный пароль будет сопоставлен с настоящим. Например, введенный нами 2-ой пароль не был правильным, однако попытка не успела сняться. В случае, если количество команд, необходимое для успешного ввода пароля, меньше, чем количество команд, которое необходимо пройти, чтобы снялась одна попытка, можно использовать отладчик для «халявного» ввода пароля бесконечное число раз. В этом случае злоумышленник может просто останавливать отладчик в тот момент, когда прошло необходимое количество шагов для успешного ввода, но не достаточное количество шагов для снятия одной попытки в случае неправильного пароля. Таким образом, при грамотном использовании отладчика есть шанс получить преимущество, если считать количество шагов, которое совершается между попытками ввода пароля.

На этом мои эксперименты касательно лабораторной работы №4 (23.11.2021) были завершены.

Пароль от архива: **041** (на всякий случай, укажу пароль на самом верху этого отчёта тоже)