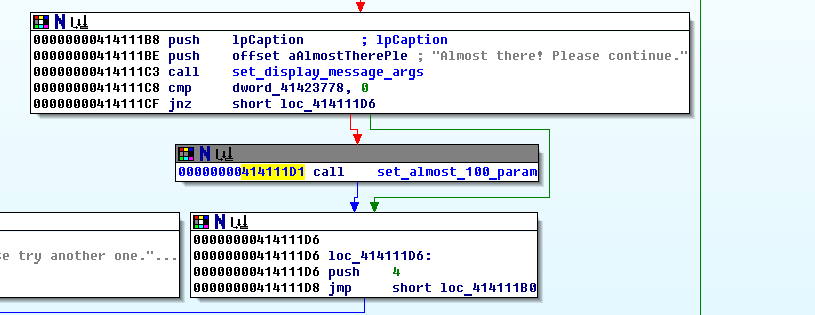
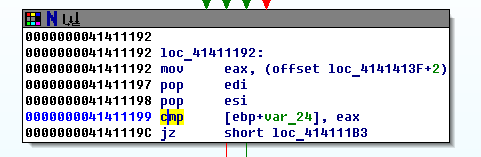
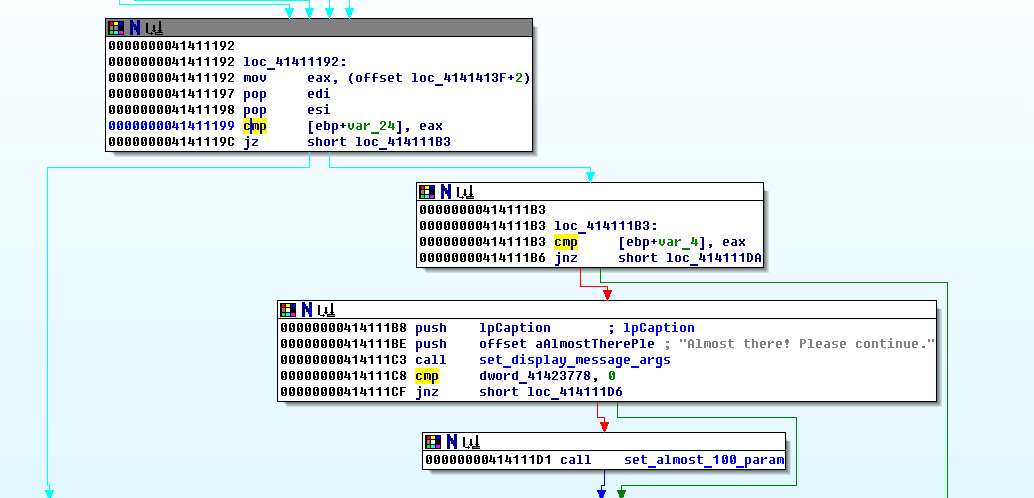
1. В данной программе происходит запись в стек символов аргумента командной строки в качестве двоичных значений (записывается не код символа, а код, который этот строковый символ представляет, т.е. для “AA” запишется не 0x6161, 0xAA)
2. Чтобы получить сообщение Almost100% необходимо выполнить инструкцию по адресу 0x414111D1



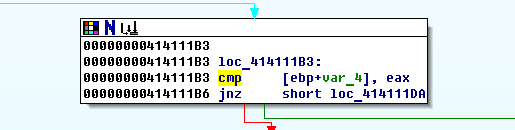
1. Чтобы перейти к этой команде сперва необходимо, чтобы было пройдено 2 проверки для введенного параметра командной строки:
2. Первые 8 символов должны представлять строку “41414141”:



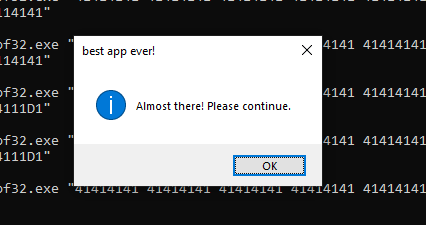
Т. к. начало введенной строки на стеке находится по адресу ebp+var\_24 и регистр eax содержит значение (0x41414141) – инструкция по адресу 0x41411192, следовательно, чтобы выполнилась инструкция jz и случился переход не к выводу окна с информацией о неверных аргументах.



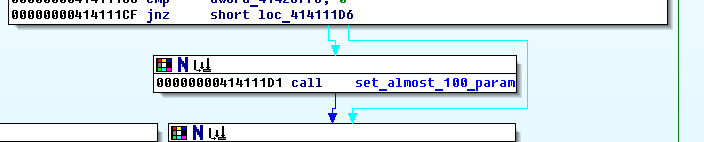
1. Вторая проверка значения – 9-го восьмисимвольного слова в введенной строке (адрес инструкции – 0x414111B3), данное значение тоже должно быть равно 0x41414141



Таким образом, введя в консоль строку вида “41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141”, можно получить сообщение:

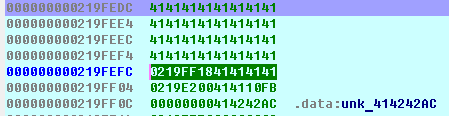


Но, чтобы получить Almost 100%, не нашлось более подходящего и простого решения, чтобы перезаписать адрес возврата из функции, проверяющей введенные параметры (адрес начала функции – 0x4141112B), на адрес инструкции с выводом окна Almost 100% (адрес команды – 0x414111D1):



Адрес возврата находится по смещению +28h байт от адреса начала введенного в консоль строкового параметра в стеке. Из этого следует, что необохдимо ввести строку, где будет 10 слов вида “41414141”, разделенных пробелами, а в конце строки будет нужный нам адрес возврата “414111D1”.

Стек при выводе окна Almost there!:



В данном случае был введен параметр “41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141”. Адрес возврата из функции находится по адресу 0x0219FF04 и равен 0x414110FB – его необходимо заменить на адрес команды, выводящей окно Almost 100% - 0x414111D1

Стек при последовательном выводе окон Almost there! и Almost 100%:



Новый адрес возврата выделен серым.

В этом случае был введен параметр “41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141 41414141 414111D1”.

Получили желаемое окно:  
