# Министерство науки и высшего образования Российской Федерации

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Московский государственный технический университет имени Н.Э. Баумана**

**(национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)**

ФАКУЛЬТЕТ **ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ**

КАФЕДРА **Программное обеспечение ЭВМ и информационные технологии**

# О Т Ч Е Т

**по лабораторной работе № 9**

Название: Низкоуровневое программирование под Windows/Linux.  
 Дизассемблирование. Реверс-инжиниринг

Дисциплина: Машинно-зависимые языки программирования

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Студент | ИУ7-И46Б |  |  | Нгуен Ань Тхы |
|  | (Группа) |  | (Подпись, дата) | (И.О. Фамилия) |
|  |  |  |  |  |
| Преподаватель |  |  |  | Кузнецов Д. А. |
|  |  |  | (Подпись, дата) | (И.О. Фамилия) |

*Москва, 2020*

Цель программы: Вывод приглашения, ввод строки и проверка строки. Допустимые строки - это строки в следующем формате: первые 3 символа "asm" и сумма оставшихся символов составляет 200.

.text:00401150 ; int \_\_cdecl main()

.text:00401150 \_main proc near ; CODE XREF: \_\_scrt\_common\_main\_seh+F5↓p

.text:00401150

.text:00401150 str = byte ptr -70h

.text:00401150 var\_6F = byte ptr -6Fh

.text:00401150 var\_6E = byte ptr -6Eh

.text:00401150 var\_6D = dword ptr -6Dh

.text:00401150 var\_4 = dword ptr -4

.text:00401150

***; Сохранить ebp и верхний стек в eps:***

.text:00401150 push ebp

.text:00401151 mov ebp, esp

***; Выравнивать указатель стека по 8-байтовой границе:***

.text:00401153 and esp, 0FFFFFFF8h

***; размер переменных 74h:***

.text:00401156 sub esp, 74h

***; защита от переполнения стека:***

.text:00401159 mov eax, \_\_\_security\_cookie

.text:0040115E xor eax, esp

.text:00401160 mov [esp+74h+var\_4], eax

***; вывод приглашения:***

.text:00401164 mov ecx, ds:\_\_imp\_?cout@std@@3V?$basic\_ostream@DU?$char\_traits@D@std@@@1@A.gap0 ; \_Ostr

***; установить приглашение:***

.text:0040116A mov edx, offset \_Val ; "Enter string: "

***; сохранить esi:***

.text:0040116F push esi ; \_Str

***;установить esi = 0:***

.text:00401170 xor esi, esi

***; вызов функции вывода приглашения:***

.text:00401172 call ??$?6U?$char\_traits@D@std@@@std@@YAAAV?$basic\_ostream@DU?$char\_traits@D@std@@@0@AAV10@PBD@Z ; std::operator<<<std::char\_traits<char>>(std::basic\_ostream<char,std::char\_traits<char>> &,char const \*)

.text:00401177 mov ecx, ds:\_\_imp\_?cin@std@@3V?$basic\_istream@DU?$char\_traits@D@std@@@1@A.gap0 ; \_Istr

***; установить адрес введённой строки:***

.text:0040117D lea eax, [esp+78h+str]

.text:00401181 push eax ; \_Size

***; вызов функции std::cin:***

.text:00401182 call ??$\_Istream\_extract\_into\_buffer@DU?$char\_traits@D@std@@@std@@YAAAV?$basic\_istream@DU?$char\_traits@D@std@@@0@AAV10@IPAD@Z ; std::\_Istream\_extract\_into\_buffer<char,std::char\_traits<char>>(std::basic\_istream<char,std::char\_traits<char>> &,uint,char \*)

.text:00401187 add esp, 4

***; сравнить первый символ строки с 61h:***

.text:0040118A cmp [esp+78h+str], 61h

***; прыгать, если не равны:***

.text:0040118F jnz short loc\_4011CD

***; сравнить второй символ строки с 73h:***

.text:00401191 cmp [esp+78h+var\_6F], 73h

***; прыгать, если не равны:***

.text:00401196 jnz short loc\_4011CD

***; сравнить третий символ строки с 6Dh:***

.text:00401198 cmp [esp+78h+var\_6E], 6Dh

***; прыгать, если не равны:***

.text:0040119D jnz short loc\_4011CD

***; сохранить 4 символа строки (вначале из четвертой символа):***

.text:0040119F mov edx, [esp+78h+var\_6D]

***; прыгать, если dl = 0:***

.text:004011A3 test dl, dl

.text:004011A5 jz short loc\_4011CD

***; сохранить смещение четвертой символа:***

.text:004011A7 lea ecx, [esp+78h+var\_6D]

.text:004011AB nop dword ptr [eax+eax+00h]

.text:004011B0

***; выполнить когда 3 условия верны и сторка не закончить:***

.text:004011B0 loc\_4011B0: ; CODE XREF: \_main+6E↓j

***; сохранить байт из dl в уфы с знаком:***

.text:004011B0 movsx eax, dl

***; сохранить смещение следующего символа:***

.text:004011B3 lea ecx, [ecx+1]

***; сложение символа и esi :***

.text:004011B6 add esi, eax

***; значение следующего символа:***

.text:004011B8 mov al, [ecx]

.text:004011BA mov dl, al

***; Если следующий символ не нулевой, продолжить цикл, иначе установить сообщение вывода (“FAILED”):***

.text:004011BC test al, al

.text:004011BE jnz short loc\_4011B0

***; установить сообщение вывода:***

.text:004011C0 mov edx, offset aOk ; "OK"

***; cравнить esi c 0C8h :***

.text:004011C5 cmp esi, 0C8h

***; прыгать, если esi равен 0C8h:***

.text:004011CB jz short loc\_4011D2

.text:004011CD

.text:004011CD loc\_4011CD: ; CODE XREF: \_main+3F↑j

.text:004011CD ; \_main+46↑j ...

***; установить сообщение вывода:***

.text:004011CD mov edx, offset aFailed ; "FAILED"

.text:004011D2

.text:004011D2 loc\_4011D2: ; CODE XREF: \_main+7B↑j

.text:004011D2 mov ecx, ds:\_\_imp\_?cout@std@@3V?$basic\_ostream@DU?$char\_traits@D@std@@@1@A.gap0 ; \_Ostr

*; вызов функция вывод сообщения*

.text:004011D8 call ??$?6U?$char\_traits@D@std@@@std@@YAAAV?$basic\_ostream@DU?$char\_traits@D@std@@@0@AAV10@PBD@Z ; std::operator<<<std::char\_traits<char>>(std::basic\_ostream<char,std::char\_traits<char>> &,char const \*)

***; защитить от переполнения стека:***

.text:004011DD mov ecx, [esp+78h+var\_4]

.text:004011E1 xor eax, eax

.text:004011E3 pop esi

.text:004011E4 xor ecx, esp ; cookie

.text:004011E6 call @\_\_security\_check\_cookie@4 ; \_\_security\_check\_cookie(x)

.text:004011EB mov esp, ebp

.text:004011ED pop ebp

.text:004011EE retn

.text:004011EE \_main endp