ЛАБОРАТОРНАЯ РАБОТА. ВЫПОЛНЕНИЕ ПРОГРАММЫ НА ПРАВАХ АДМИНИСТРАТОРА

Цель. Изучить механизм разрешения выполнить программу на правах администратора.

Краткая теория.

Мы создадим приложение, которое будет содержать три метода. Первый:

BOOL IsRunAsAdministrator()

{

BOOL fIsRunAsAdmin = FALSE;

DWORD dwError = ERROR\_SUCCESS;

PSID pAdministratorsGroup = NULL;

SID\_IDENTIFIER\_AUTHORITY NtAuthority = SECURITY\_NT\_AUTHORITY;

if (!AllocateAndInitializeSid(

&NtAuthority,

2,

SECURITY\_BUILTIN\_DOMAIN\_RID,

DOMAIN\_ALIAS\_RID\_ADMINS,

0, 0, 0, 0, 0, 0,

&pAdministratorsGroup))

{

dwError = GetLastError();

goto Cleanup;

}

if (!CheckTokenMembership(NULL, pAdministratorsGroup, &fIsRunAsAdmin))

{

dwError = GetLastError();

goto Cleanup;

}

Cleanup:

if (pAdministratorsGroup)

{

FreeSid(pAdministratorsGroup);

pAdministratorsGroup = NULL;

}

if (ERROR\_SUCCESS != dwError)

{

throw dwError;

}

return fIsRunAsAdmin;

}

Этот метод проверяет, имеете ли Вы права администратора для выполнения программы. Возвращает булевскую переменную, которая определяет этот факт.

Второй метод повышает уровень Ваших прав.

#include <Windows.h>

BOOL IsRunAsAdministrator();

void ElevateNow()

{

BOOL bAlreadyRunningAsAdministrator = FALSE;

try

{

bAlreadyRunningAsAdministrator = IsRunAsAdministrator();

}

catch(...)

{

\_asm nop

}

if(!bAlreadyRunningAsAdministrator)

{

char szPath[MAX\_PATH];

if (GetModuleFileName(NULL, szPath, ARRAYSIZE(szPath)))

{

SHELLEXECUTEINFO sei = {sizeof(sei)};

sei.lpVerb = "runas";

sei.lpFile = szPath;

sei.hwnd = NULL;

sei.nShow = SW\_NORMAL;

if (!ShellExecuteEx(&sei))

{

DWORD dwError = GetLastError();

if (dwError == ERROR\_CANCELLED)

//Annoys you to Elevate it LOL

CreateThread(0,0,(LPTHREAD\_START\_ROUTINE)ElevateNow,0,0,0);

}

}

}

else

{

///Code

}

}

Переменная bAlreadyRunningAsAdministrator определяет, имеете ли Вы права администратора. Если нет, то делается попытка повысить Ваш уровень и выполнить файл szPath, определив для него структуру SHELLEXECUTEINFO sei.

Выполнение файла осуществляется по команде ShellExecuteEx(&sei).

Третий метод – это main:

#include<windows.h>

BOOL IsRunAsAdministrator();

void ElevateNow();

//Beware Scary

int main()

{

if(IsRunAsAdministrator())

{

}

else

{

if(MessageBox(0,"Need To Elevate","Critical Disk Error",MB\_SYSTEMMODAL|MB\_ICONERROR|MB\_YESNO) == IDYES)

{

ElevateNow();

}

else

{

MessageBox(0,"You Better give me Elevation or I will attack u","System Critical Error",MB\_SYSTEMMODAL|MB\_OK|MB\_ICONERROR);

ElevateNow();

}

}

return 0;

Итак, Вам нужно написать два файла:

Elevation.cpp, Main.cpp.

ЗАДАНИЕ.

СОБЕРИТЕ ПРИЛОЖЕНИЕ . ВЫПОЛНИТЕ ЕГО. Попробуйте загрузиться в систему не как администратор, а как обычный пользователь. Проверьте, как работает программа на повышение уровня доступа.