DLL Injection via CreateRemoteThread - Process Flow

1. Purpose

This program injects a DLL (`MyDLL.dll`) into a target process (`explorer.exe`) by using Windows API functions.

2. Process Search

The `SearchProcess` function scans running processes to find the one matching `explorer.exe`. It returns the PID.

3. LoadLibraryA

`GetProcAddress` is used to get the address of `LoadLibraryA`, which will be used to load the DLL into the target process.

4. Open Target Process

`OpenProcess` is called with full access rights to open a handle to the target process using its PID.

5. Allocate Memory

`VirtualAllocEx` allocates memory in the target process for the DLL path string.

6. Write DLL Path

`WriteProcessMemory` writes the DLL path into the allocated memory in the target process.

7. Remote Thread Creation

`CreateRemoteThread` is used to execute `LoadLibraryA` in the context of the target process, passing in the DLL path. This results in the target process loading `MyDLL.dll`.

8. Cleanup

`CloseHandle` is called on the process handle to release resources after injection.