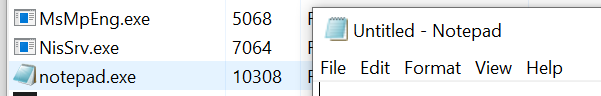
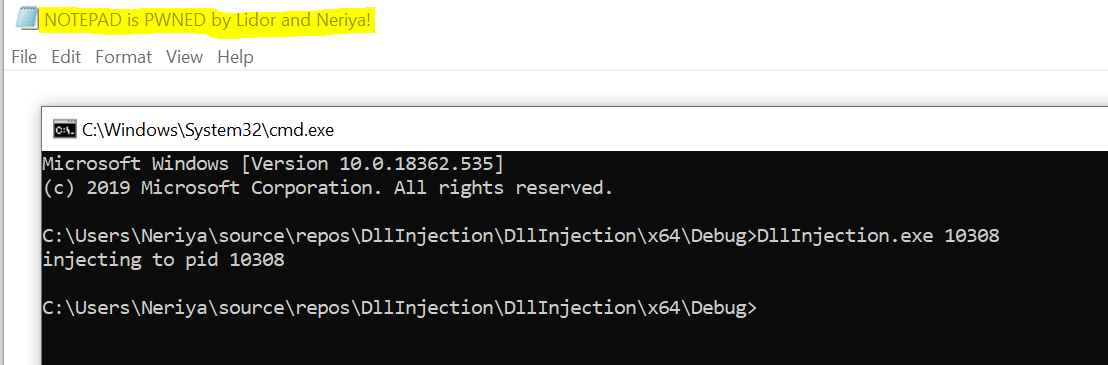
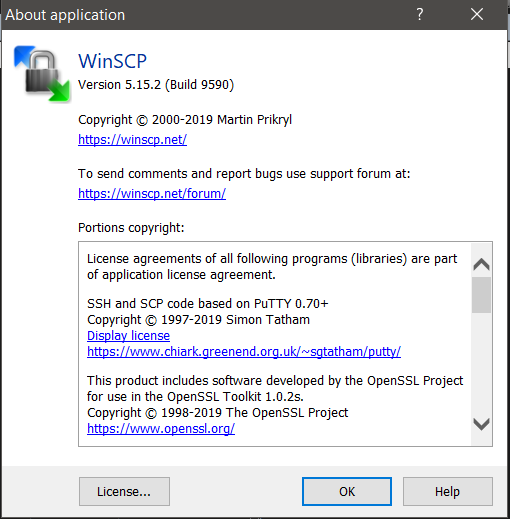
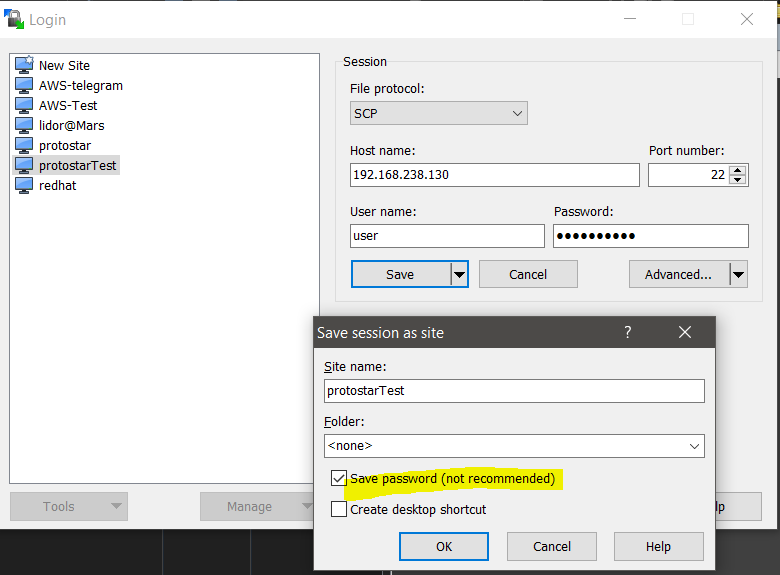
**Exercise 1: Dll Injection**

1. We wrote a dll that changes the window title of the current process when the dll is attached to a process.  
In order to do that we used **EnumWindows** to enumerate over all the open windows and find the window that related to the current process (which is the process the dll injected to).  
Then we used **SetWindowText** in order to change the window text.  
2. In order to make this code run, we needed an execute file to inject this dll into notepad.exe.  
We received a pid as argument and used **OpenProcess** to get handle to this process.  
Then we used **GetModuleHandle** and **GetProcAddress** in order to get the address of **LoadLibrayA** function. In that stage we needed to inject a string which is the path of the dll, we did that using **VirtualAllocEx** and **WriteProcessMemory**.  
Finally we called **CreateRemoteThread** to make **LoadLibrayA** run on the remote process.  
**Screenshots**:  
Find notepad pid:  
  
Run the injector:  


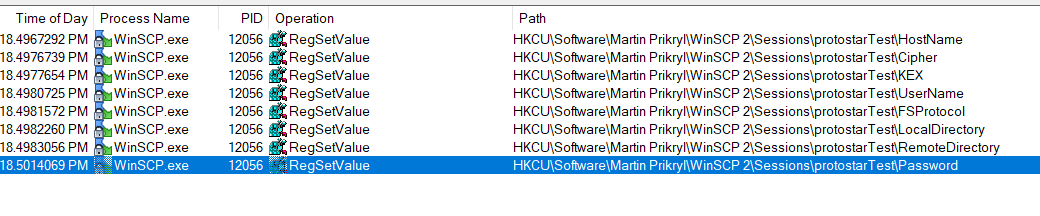
**Exercise 2: IAT Patching**

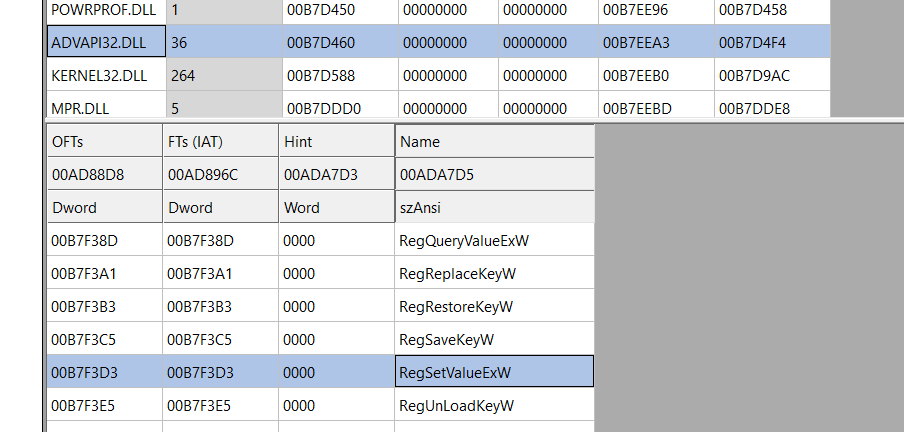
We chose WinScp.exe as Windows application which allow to user to connect to SSH server and move file to/from the server.



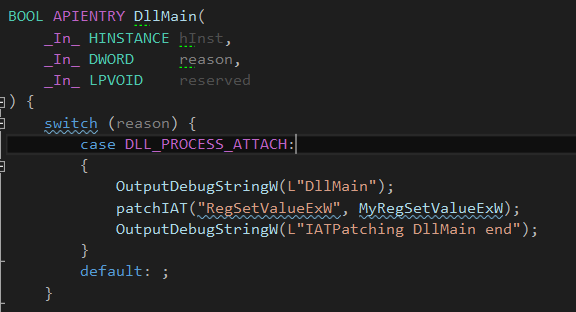
WinScp allow the user to store the password to the server in order to make it easier to connect to the server again:

We used procmon and found out that registry is used in order to store the passwords that the user choose to save:

We used CFFexplorer and realized that the WinAPI function **RegSetValueExW** from **ADVAPI32.dll** is used to save the password in the registry:



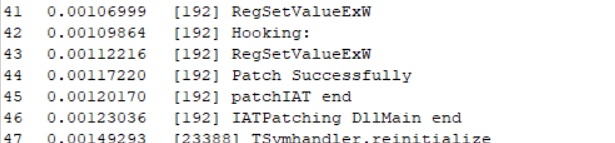
We wrote DLL that Patch IAT. it patches the IAT and call to **MyRegSetValueExW** instead of **RegSetValueExW:**



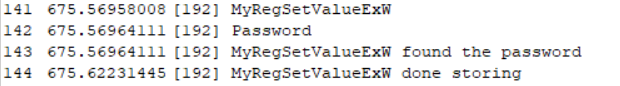
Our function, **MyRegSetValueExW,** just store the password in c:\output.txt, and return the call to the original **RegSetValueExW** in order to not breaking winscp application from operating successfully:



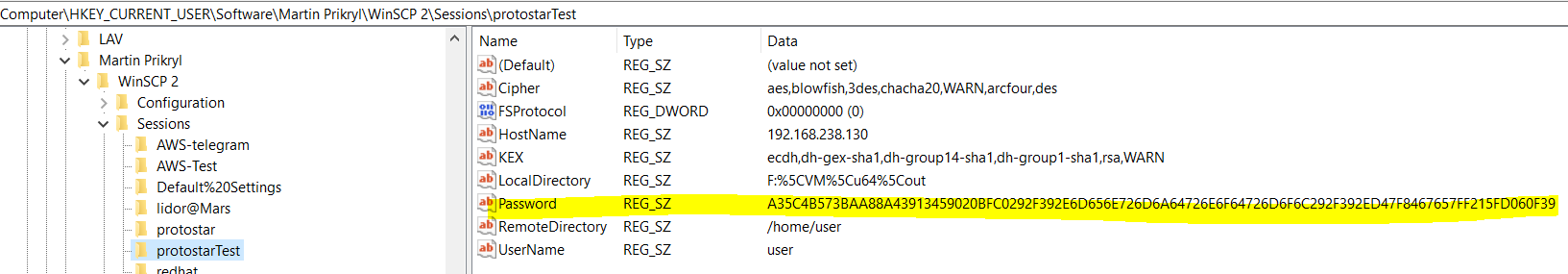
Now we tested the code; we used OutputDebugString to debug our code and view the debug messages from dbgview. The IAT Patching worked succefully:

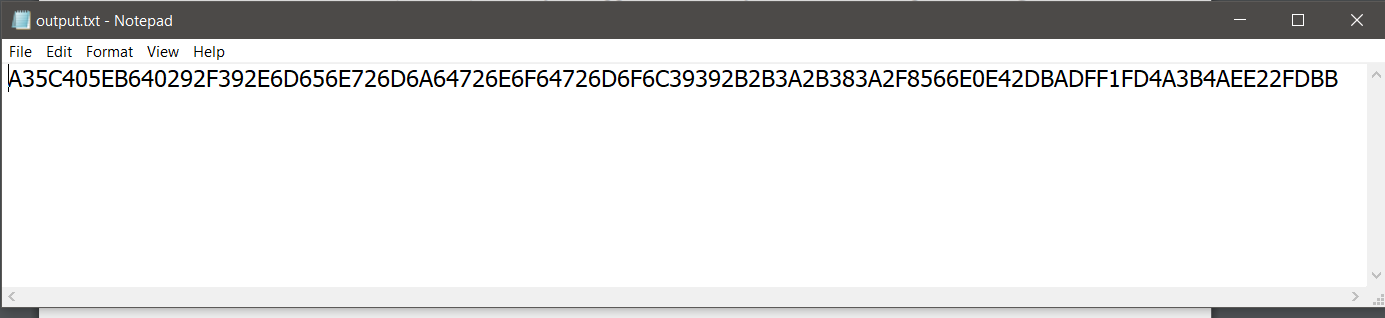


Then we store the password, and according to debug messages it works!



We also check that the contents saved to registry is same as contents saved to registry:





And it is the same!