Subject: Re: Function Hooking
Posted by iRANian on Sun, 28 Dec 2014 14:05:21 GMT
View Forum Message <> Reply to Message

What you can also do is place a JMP at the very start of the original function to your own hook. Then when you want to call the original function you re-create the first 5 bytes you overwrote in assembly then just jmp 5 bytes into the original function.

function:
push ebp ; byte 1
push edi ; byte 2
push esi ; byte 3
push ebx ; byte 4
push ecx ; byte 5
push edx ; byte 6

Then after jumping hooking:

function:
jmp <hookfunc> ; byte 1-5
push edx ; byte 6

void HookFunc()
{
 blabla
}

void _declspec(naked)Call original func()
{
 _asm
{
push ebp ; byte 1
push edi ; byte 2
push esi ; byte 3
push ebx ; byte 4
push ecx ; byte 5
jmp to byte 6; where 'push edx' is located
}
}