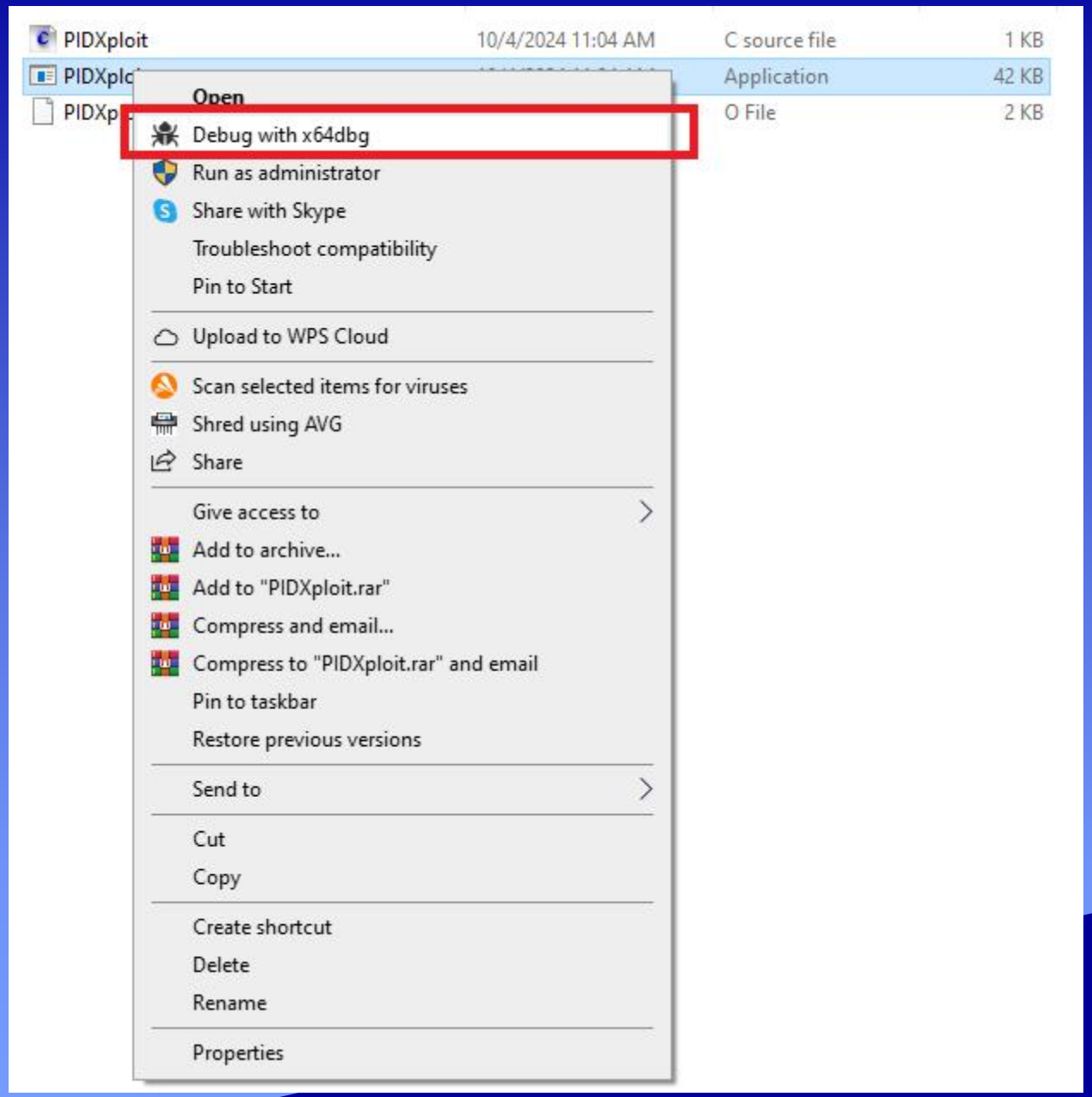
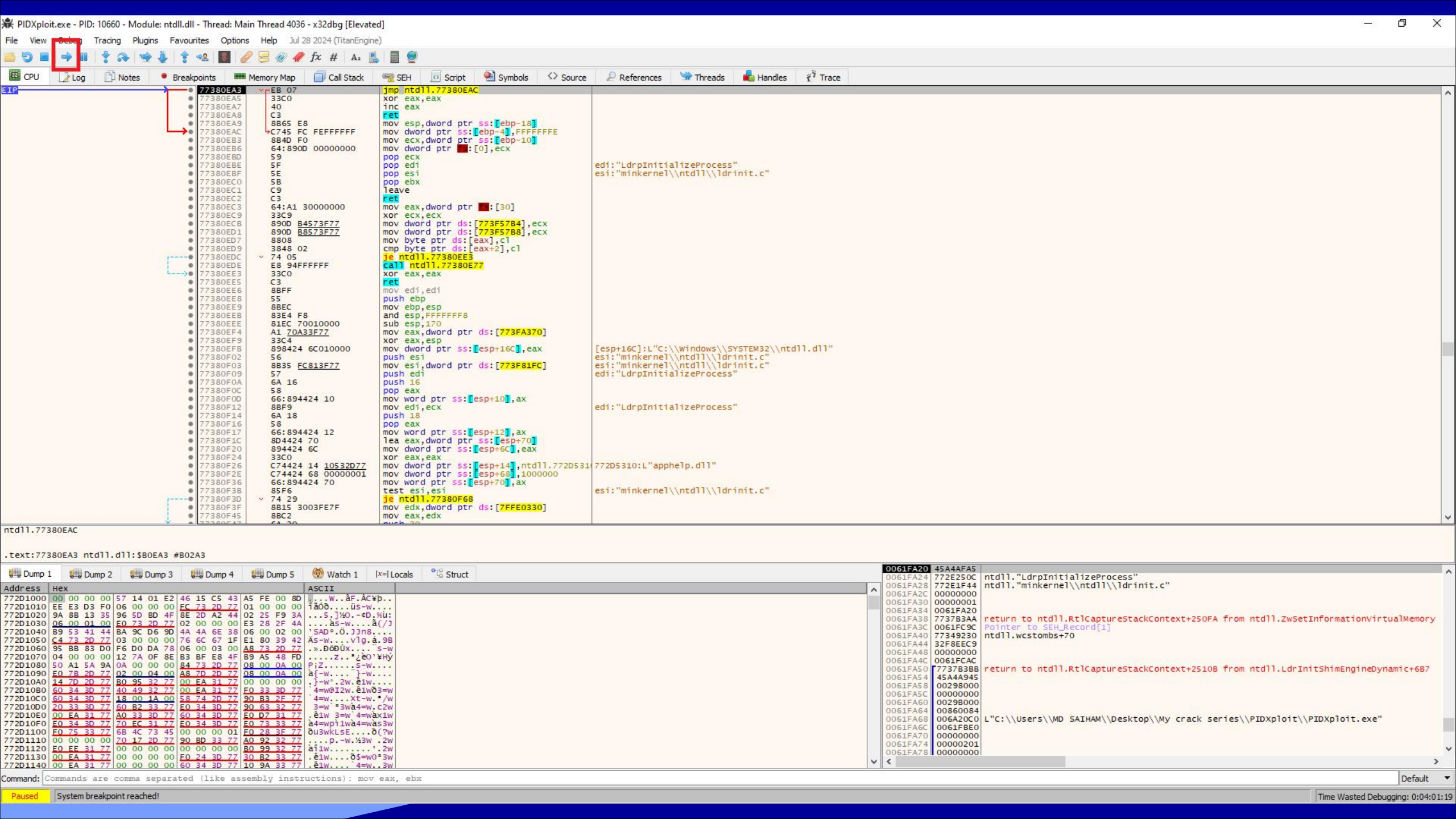
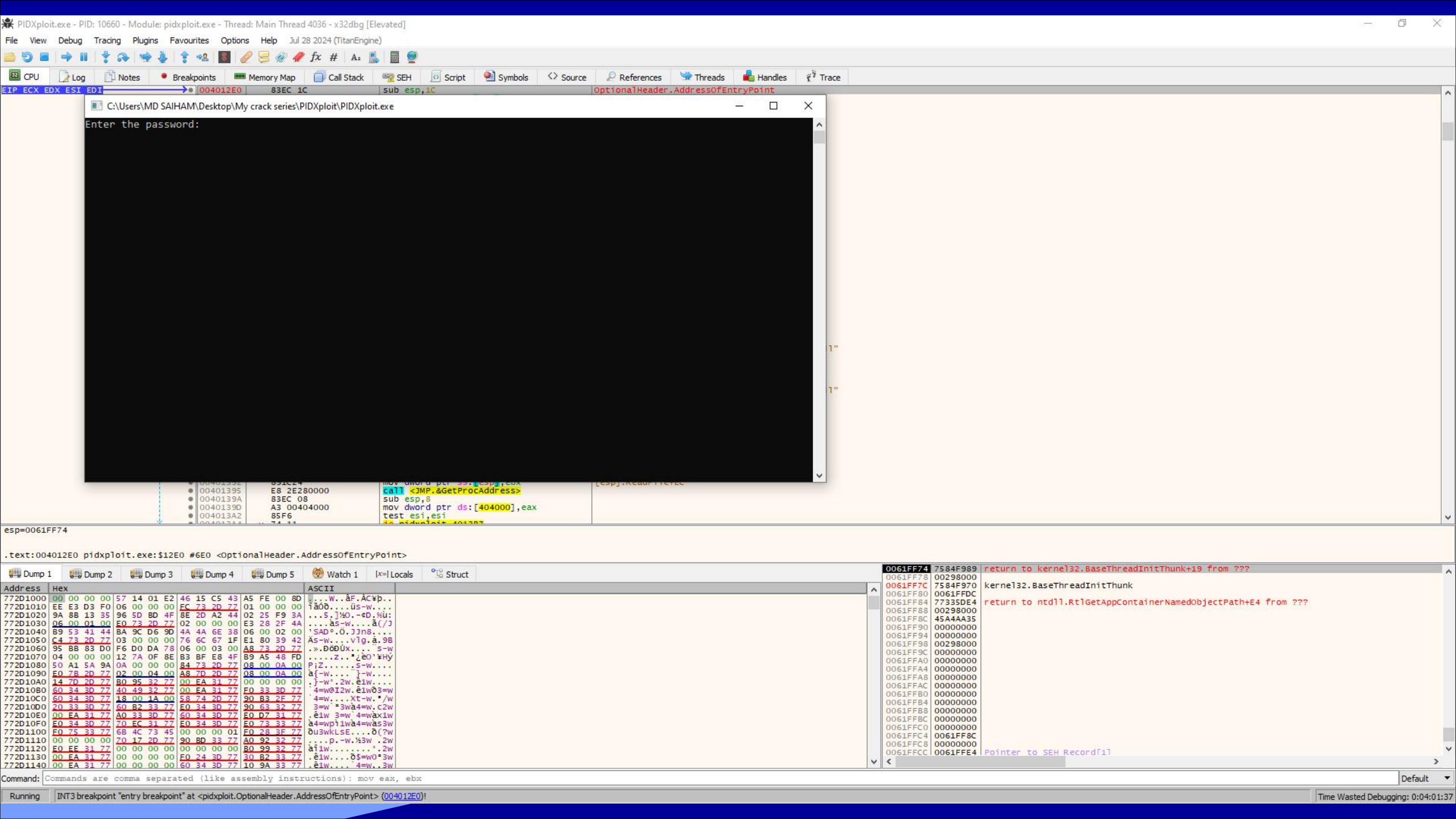
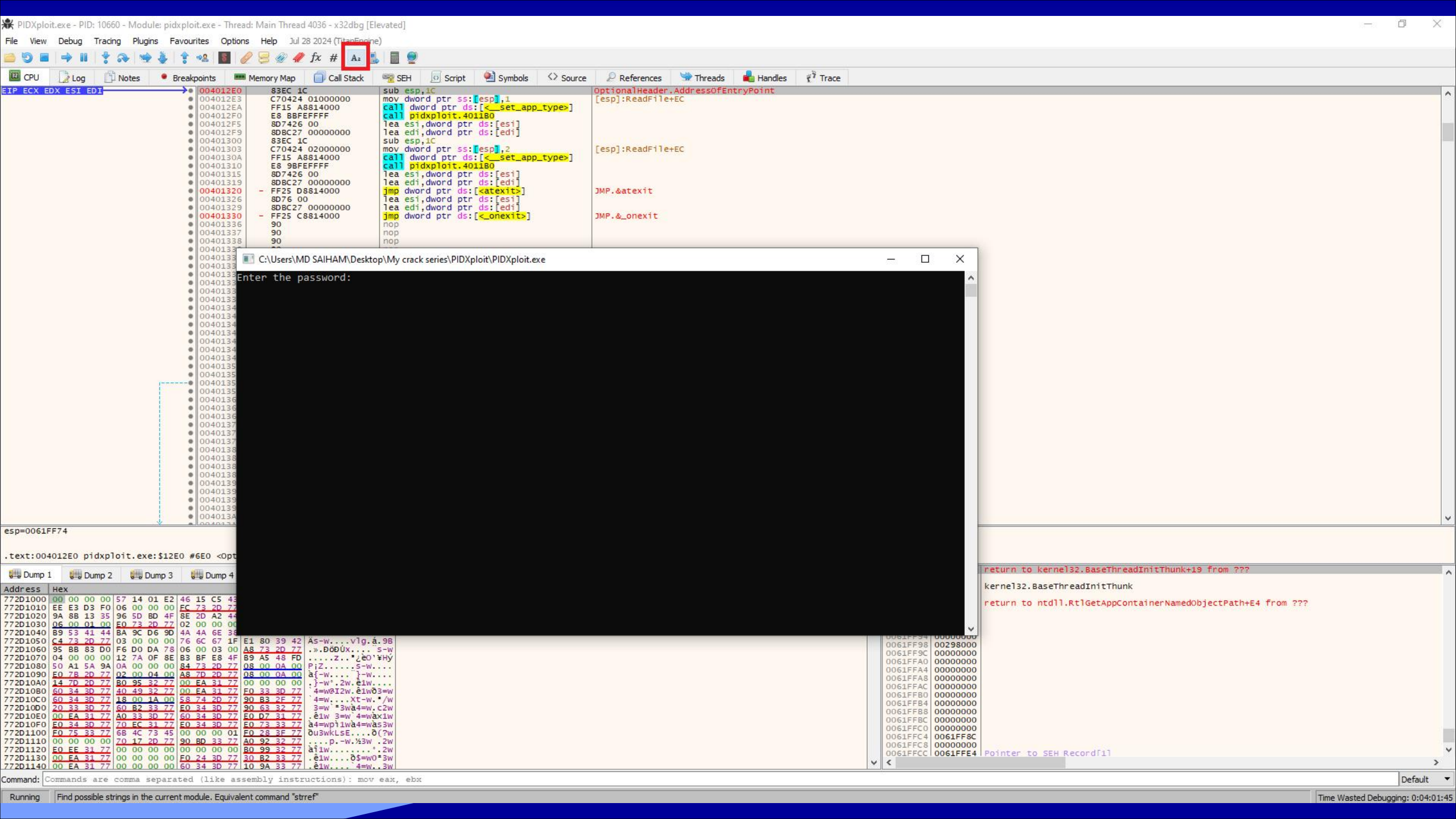

PIDXploit 10/4/2024 11:04 AM C source file 1 KB
Application 42 KB
O File 2 KB
Open
Debug with x64dbg
Run as administrator
Share with Skype
Troubleshoot compatibility
Pin to Start
Upload to WPS Cloud
Scan selected items for viruses
Shred using AVG
Share
Give access to
Add to archive...
Add to "PIDXploit.rar"
Compress and email...
Compress to "PIDXploit.rar" and email
Pin to taskbar
Restore previous versions
Send to
Cut
Copy
Create shortcut
Delete
Rename
Properties


PIDXploit.exe - PID: 10660 - Module: ntdll.dll - Thread: Main Thread 4036 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
EIP
77380EA3 EB 07 jmp ntdll.77380EAC
77380EA5 33C0 xor eax,eax
77380EA7 40 inc eax
77380EA8 C3 ret
77380EA9 8B65 E8 mov esp,dword ptr ss:[ebp-18]
77380EAC C745 FC FEFFFFFF mov dword ptr ss:[ebp-4],FFFFFFFE
77380EB3 8B4D F0 mov ecx,dword ptr ss:[ebp-10]
77380EB6 64:890D 00000000 mov dword ptr fs:[0],ecx
77380EBD 59 pop ecx
77380EBE 5F pop edi edi:"LdrpInitializeProcess"
77380EBF 5E pop esi esi:"minkernel\\ntdll\\ldrinit.c"
77380EC0 5B pop ebx
77380EC1 C9 leave
77380EC2 C3 ret
77380EC3 64:A1 30000000 mov eax,dword ptr fs:[30]
77380EC9 33C9 xor ecx,ecx
77380ECB 890D B4573F77 mov dword ptr ds:[773F57B4],ecx
77380ED1 890D B8573F77 mov dword ptr ds:[773F57B8],ecx
77380ED7 8808 mov byte ptr ds:[eax],cl
77380ED9 3848 02 cmp byte ptr ds:[eax+2],cl
77380EDC 74 05 je ntdll.77380EE3
77380EDE E8 94FFFFFF call ntdll.77380E77
77380EE3 33C0 xor eax,eax
77380EE5 C3 ret
77380EE6 8BFF mov edi,edi
77380EE8 55 push ebp
77380EE9 8BEC mov ebp,esp
77380EEB 83E4 F8 and esp,FFFFFFF8
77380EEE 81EC 70010000 sub esp,170
77380EF4 A1 70A33F77 mov eax,dword ptr ds:[773FA370]
77380EF9 33C4 xor eax,esp
77380EFB 898424 6C010000 mov dword ptr ss:[esp+16C],eax [esp+16C]:L"C:\\Windows\\SYSTEM32\\ntdll.dll"
77380F02 56 push esi esi:"minkernel\\ntdll\\ldrinit.c"
77380F03 8B35 FC813F77 mov esi,dword ptr ds:[773F81FC] esi:"minkernel\\ntdll\\ldrinit.c"
77380F09 57 push edi edi:"LdrpInitializeProcess"
77380F0A 6A 16 push 16
77380F0C 58 pop eax
77380F0D 66:894424 10 mov word ptr ss:[esp+10],ax
77380F12 8BF9 mov edi,ecx edi:"LdrpInitializeProcess"
77380F14 6A 18 push 18
77380F16 58 pop eax
77380F17 66:894424 12 mov word ptr ss:[esp+12],ax
77380F1C 8D4424 70 lea eax,dword ptr ss:[esp+70]
77380F20 894424 6C mov dword ptr ss:[esp+6C],eax
77380F24 33C0 xor eax,eax
77380F26 C74424 14 10532D77 mov dword ptr ss:[esp+14],ntdll.772D5310 772D5310:L"apphelp.dll"
77380F2E C74424 68 00000001 mov dword ptr ss:[esp+68],1000000
77380F36 66:894424 70 mov word ptr ss:[esp+70],ax
77380F3B 85F6 test esi,esi esi:"minkernel\\ntdll\\ldrinit.c"
77380F3D 74 29 je ntdll.77380F68
77380F3F 8B15 3003FE7F mov edx,dword ptr ds:[7FFE0330]
77380F45 8BC2 mov eax,edx
ntdll.77380EAC
.text:77380EA3 ntdll.dll:$B0EA3 #B02A3
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct
Address Hex ASCII
772D1000 00 00 00 00 57 14 01 E2 46 15 C5 43 A5 FE 00 8D ....W..âF.ÅC¥þ..
772D1010 EE E3 D3 F0 06 00 00 00 FC 73 2D 77 01 00 00 00 îãÓð....üs-w....
772D1020 9A 8B 13 35 96 5D BD 4F 8E 2D A2 44 02 25 F9 3A ...5.]½O.-¢D.%ù:
772D1030 06 00 01 00 E0 73 2D 77 02 00 00 00 E3 28 2F 4A ....às-w....ã(/J
772D1040 B9 53 41 44 BA 9C D6 9D 4A 4A 6E 38 06 00 02 00 'SAD°.Ö.JJn8....
772D1050 C4 73 2D 77 03 00 00 00 76 6C 67 1F E1 80 39 42 Äs-w....vlg.á.9B
772D1060 95 BB 83 D0 F6 D0 DA 78 06 00 03 00 A8 73 2D 77 .».ÐöÐÚx.... s-w
772D1070 04 00 00 00 12 7A 0F 8E B3 BF E8 4F B9 A5 48 FD .....z..³¿èO'¥Hý
772D1080 50 A1 5A 9A 0A 00 00 00 84 73 2D 77 08 00 0A 00 P¡Z.....s-w....
772D1090 E0 7B 2D 77 02 00 04 00 A8 7D 2D 77 08 00 0A 00 à{-w....}-w....
772D10A0 14 7D 2D 77 B0 95 32 77 00 EA 31 77 00 00 00 00 .}-w°.2w.ê1w....
772D10B0 60 34 3D 77 40 49 32 77 00 EA 31 77 F0 33 3D 77 `4=w@I2w.ê1wð3=w
772D10C0 60 34 3D 77 18 00 1A 00 58 74 2D 77 90 B3 2F 77 `4=w....Xt-w.³/w
772D10D0 20 33 3D 77 60 B2 33 77 F0 34 3D 77 90 63 32 77 3=w`²3wð4=w.c2w
772D10E0 00 EA 31 77 A0 33 3D 77 60 34 3D 77 F0 D7 31 77 .ê1w 3=w`4=wð×1w
772D10F0 F0 34 3D 77 70 EC 31 77 F0 34 3D 77 F0 73 33 77 ð4=wpì1wð4=wðs3w
772D1100 F0 75 33 77 6B 4C 73 45 00 00 00 01 F0 28 3F 77 ðu3wkLsE....ð(?w
772D1110 00 00 00 00 70 17 2D 77 90 BD 33 77 A0 92 32 77 ....p.-w.½3w .2w
772D1120 F0 EE 31 77 00 00 00 00 00 00 00 00 B0 99 32 77 ðî1w........°.2w
772D1130 00 EA 31 77 00 00 00 00 F0 24 3D 77 30 B2 33 77 .ê1w....ð$=w0²3w
772D1140 00 EA 31 77 00 00 00 00 60 34 3D 77 10 9A 33 77 .ê1w....`4=w..3w
0061FA20 45A4AFA5
0061FA24 772E250C ntdll."LdrpInitializeProcess"
0061FA28 772E1F44 ntdll."minkernel\\ntdll\\ldrinit.c"
0061FA2C 00000000
0061FA30 00000001
0061FA34 0061FA20
0061FA38 7737B3AA return to ntdll.RtlCaptureStackContext+250FA from ntdll.ZwSetInformationVirtualMemory
0061FA3C 0061FC9C Pointer to SEH_Record[1]
0061FA40 77349230 ntdll.wcstombs+70
0061FA44 32F8EEC9
0061FA48 00000000
0061FA4C 0061FCAC
0061FA50 7737B3BB return to ntdll.RtlCaptureStackContext+2510B from ntdll.LdrInitShimEngineDynamic+6B7
0061FA54 45A4A945
0061FA58 00298000
0061FA5C 00000000
0061FA60 0029B000
0061FA64 00860084
0061FA68 006A20C0 L"C:\\Users\\MD SAIHAM\\Desktop\\My crack series\\PIDXploit\\PIDXploit.exe"
0061FA6C 0061FBE0
0061FA70 00000000
0061FA74 00000201
0061FA78 00000000
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Paused
System breakpoint reached!
Time Wasted Debugging: 0:04:01:19


PIDXploit.exe - PID: 10660 - Module: pidxploit.exe - Thread: Main Thread 4036 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe
Enter the password:
00401395 E8 2E280000 call <JMP.&GetProcAddress>
0040139A 83EC 08 sub esp,8
0040139D A3 00404000 mov dword ptr ds:[404000],eax
004013A2 85F6 test esi,esi
esp=0061FF74
.text:004012E0 pidxploit.exe:$12E0 #6E0 <OptionalHeader.AddressOfEntryPoint>
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct
Address Hex ASCII
0061FF74 7584F989 return to kernel32.BaseThreadInitThunk+19 from ???
0061FF78 00298000
0061FF7C 7584F970 kernel32.BaseThreadInitThunk
0061FF80 0061FFDC
0061FF84 77335DE4 return to ntdll.RtlGetAppContainerNamedObjectPath+E4 from ???
0061FF88 00298000
0061FF8C 45A4AA35
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Running
INT3 breakpoint "entry breakpoint" at <pidxploit.OptionalHeader.AddressOfEntryPoint> (004012E0)!
Time Wasted Debugging: 0:04:01:37


PIDXploit.exe - PID: 10660 - Module: pidxploit.exe - Thread: Main Thread 4036 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
EIP ECX EDX ESI EDI
004012E0 83EC 1C sub esp,1C OptionalHeader.AddressOfEntryPoint
004012E3 C70424 01000000 mov dword ptr ss:[esp],1 [esp]:ReadFile+EC
004012EA FF15 A8814000 call dword ptr ds:[<__set_app_type>]
004012F0 E8 BBFEFFFF call pidxploit.4011B0
004012F5 8D7426 00 lea esi,dword ptr ds:[esi]
004012F9 8DBC27 00000000 lea edi,dword ptr ds:[edi]
00401300 83EC 1C sub esp,1C
00401303 C70424 02000000 mov dword ptr ss:[esp],2 [esp]:ReadFile+EC
0040130A FF15 A8814000 call dword ptr ds:[<__set_app_type>]
00401310 E8 9BFEFFFF call pidxploit.4011B0
00401315 8D7426 00 lea esi,dword ptr ds:[esi]
00401319 8DBC27 00000000 lea edi,dword ptr ds:[edi]
00401320 FF25 D8814000 jmp dword ptr ds:[<atexit>] JMP.&atexit
00401326 8D76 00 lea esi,dword ptr ds:[esi]
00401329 8DBC27 00000000 lea edi,dword ptr ds:[edi]
00401330 FF25 C8814000 jmp dword ptr ds:[<_onexit>] JMP.&_onexit
00401336 90 nop
00401337 90 nop
00401338 90 nop
C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe
Enter the password:
esp=0061FF74
.text:004012E0 pidxploit.exe:$12E0 #6E0 <Opt
Dump 1 Dump 2 Dump 3 Dump 4
Address Hex
772D1000 00 00 00 00 57 14 01 E2 46 15 C5 43
772D1010 EE E3 D3 F0 06 00 00 00 EC 73 2D 77
772D1020 9A 8B 13 35 96 5D BD 4F 8E 2D A2 44
772D1030 06 00 01 00 E0 73 2D 77 02 00 00 00
772D1040 B9 53 41 44 BA 9C D6 9D 4A 4A 6E 38
772D1050 C4 73 2D 77 03 00 00 00 76 6C 67 1F
772D1060 95 BB 83 D0 F6 D0 DA 78 06 00 03 00
772D1070 04 00 00 00 12 7A 0F 8E B3 BF E8 4F
772D1080 50 A1 5A 9A 0A 00 00 00 84 73 2D 77
772D1090 E0 7B 2D 77 02 00 04 00 A8 7D 2D 77
772D10A0 14 7D 2D 77 B0 95 32 77 00 EA 31 77
772D10B0 60 34 3D 77 40 49 32 77 00 EA 31 77
772D10C0 60 34 3D 77 18 00 1A 00 58 74 2D 77
772D10D0 20 33 3D 77 60 B2 33 77 E0 34 3D 77
772D10E0 00 EA 31 77 A0 33 3D 77 60 34 3D 77
772D10F0 E0 34 3D 77 70 EC 31 77 E0 34 3D 77
772D1100 F0 75 33 77 68 4C 73 45 00 00 00 01
772D1110 00 00 00 00 70 17 2D 77 90 BD 33 77
772D1120 E0 EE 31 77 00 00 00 00 00 00 00 00
772D1130 00 EA 31 77 00 00 00 00 E0 24 3D 77
772D1140 00 EA 31 77 00 00 00 00 60 34 3D 77
return to kernel32.BaseThreadInitThunk+19 from ???
kernel32.BaseThreadInitThunk
return to ntdll.RtlGetAppContainerNamedObjectPath+E4 from ???
0061FF98 00298000
0061FF9C 00000000
0061FFA0 00000000
0061FFA4 00000000
0061FFA8 00000000
0061FFAC 00000000
0061FFB0 00000000
0061FFB4 00000000
0061FFB8 00000000
0061FFBC 00000000
0061FFC0 00000000
0061FFC4 0061FF8C
0061FFC8 00000000
0061FFCC 0061FFE4 Pointer to SEH Record[1]
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Running
Find possible strings in the current module. Equivalent command "strref"
Time Wasted Debugging: 0:04:01:45

PIDXploit.exe - PID: 10660 - Module: pidxploit.exe - Thread: Main Thread 4036 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)

CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

Strings (Region pidxploit.exe) Strings (Region pidxploit.exe)

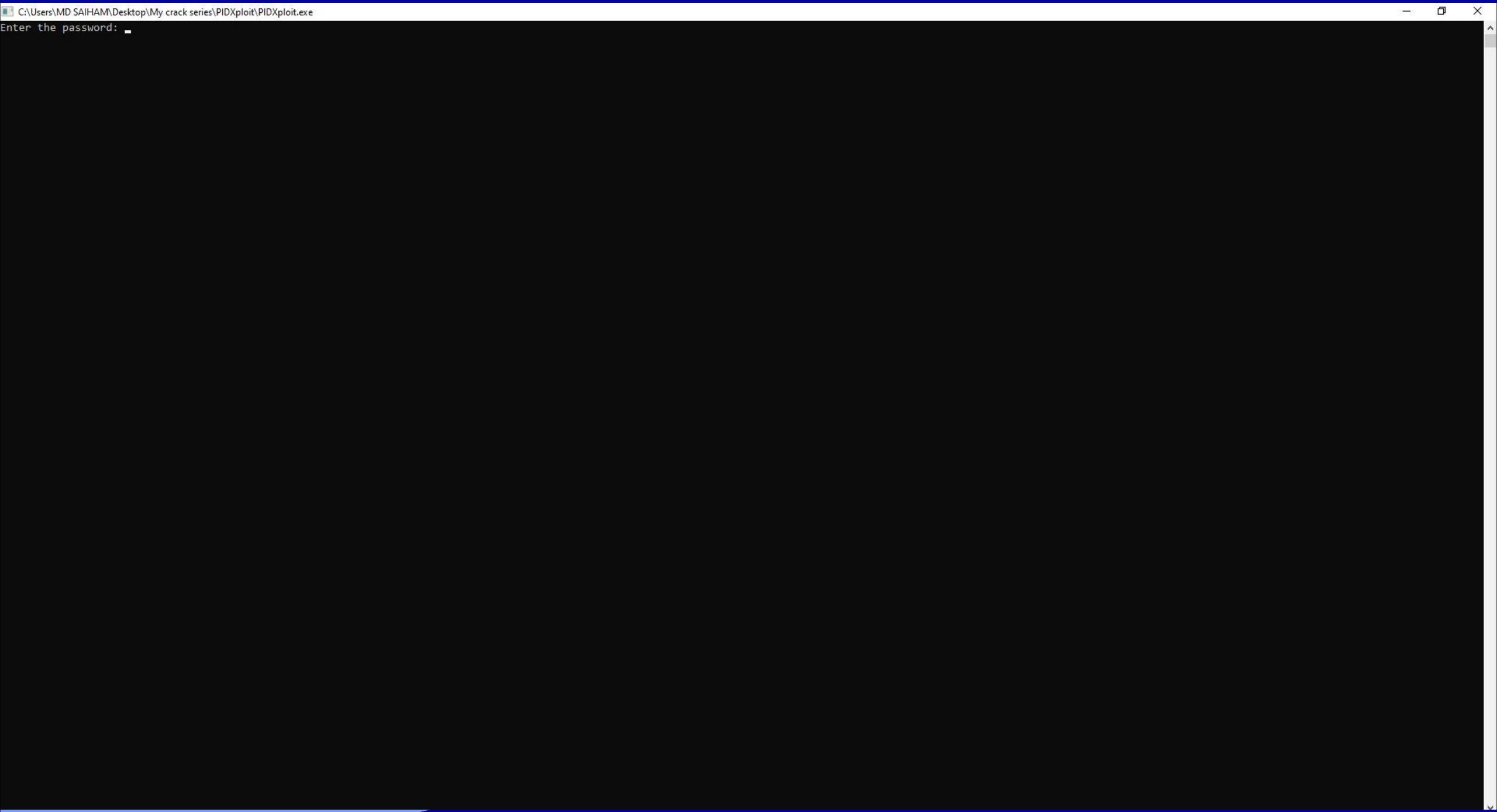
Address	Disassembly	String A	String
00401348	mov dword ptr ss:[esp],pidxploit.405000	00405000	"libgcc_s_dw2-1.dll"
0040135F	mov dword ptr ss:[esp],pidxploit.405000	00405000	"libgcc_s_dw2-1.dll"
00401375	mov dword ptr ss:[esp+4],pidxploit.405013	00405013	"__register_frame_info"
0040138A	mov dword ptr ss:[esp+4],pidxploit.405029	00405029	"__deregister_frame_info"
004013C0	mov dword ptr ss:[esp],pidxploit.405041	00405041	"libgcj-16.dll"
004013D8	mov dword ptr ss:[esp+4],pidxploit.40504F	0040504F	"_Jv_RegisterClasses"
00401475	mov dword ptr ss:[esp+4],pidxploit.405064	00405064	"EndIsNear-%d"
00401499	mov dword ptr ss:[esp],pidxploit.405071	00405071	"Enter the password: "
004014AD	mov dword ptr ss:[esp],pidxploit.405086	00405086	"%s"
004014DD	mov dword ptr ss:[esp],pidxploit.405089	00405089	"Access Granted!"
004014F0	mov dword ptr ss:[esp],pidxploit.405099	00405099	"Access Denied!"
00401929	xor dword ptr ss:[esp+C8],13C0DE	0013C0DE	L"da"
00401956	cmp ebx,13C0DE	0013C0DE	L"da"
004019C0	mov eax,dword ptr ds:[404010]	00404010	"P<@"
004019D2	mov eax,dword ptr ds:[404010]	00404010	"P<@"
004019DD	mov dword ptr ds:[404010],edx	00404010	"P<@"
00401D9E	mov dword ptr ss:[esp],pidxploit.4050AC	004050AC	"Mingw runtime failure:\n"
00401E84	mov dword ptr ss:[esp],pidxploit.4050C4	004050C4	" VirtualQuery failed for %d bytes at address %p"
00401F81	mov dword ptr ss:[esp],pidxploit.40512C	0040512C	" Unknown pseudo relocation bit size %d.\n"
0040207F	mov dword ptr ss:[esp],pidxploit.4050F8	004050F8	" Unknown pseudo relocation protocol version %d.\n"
0040308E	cmp dword ptr ds:[esi],pidxploit.40515A	0040515A	"glob-1.0-mingw32"
0040309D	mov dword ptr ds:[esi],pidxploit.40515A	0040515A	"glob-1.0-mingw32"
0040316A	cmp dword ptr ds:[esi],pidxploit.40515A	0040515A	"glob-1.0-mingw32"

Search: Type here to filter results... Regex

Region Search 100% Total Progress 100% 23

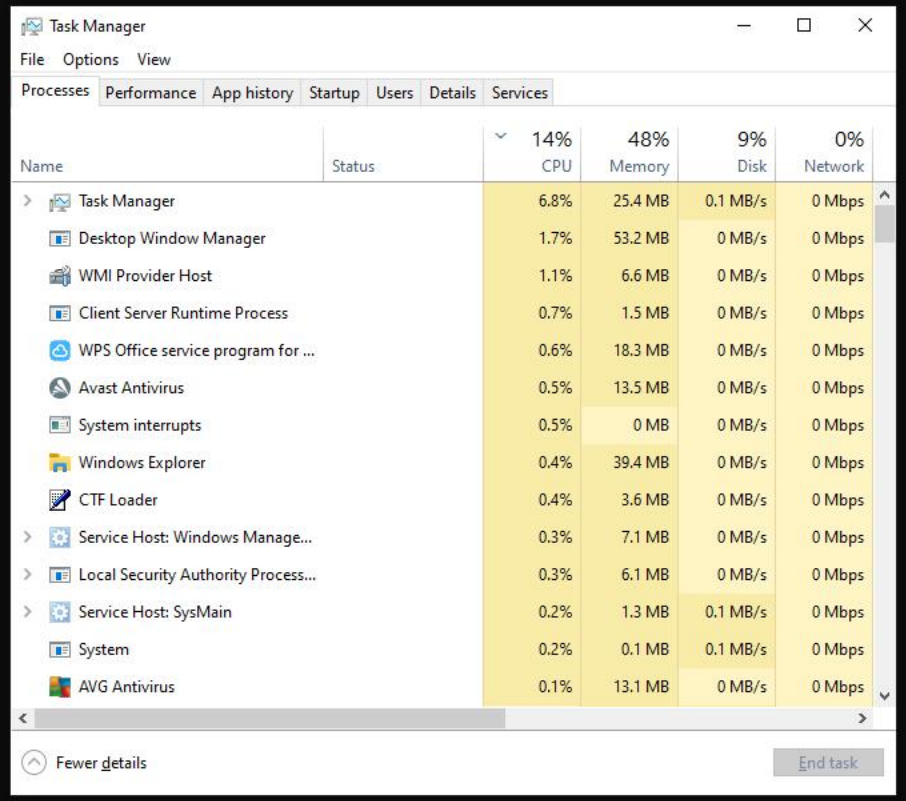
Command: Commands are comma separated (like assembly instructions): mov eax, ebx Default

Running 23 string(s) in 16ms Time Wasted Debugging: 0:04:04:43


C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe
Enter the password:

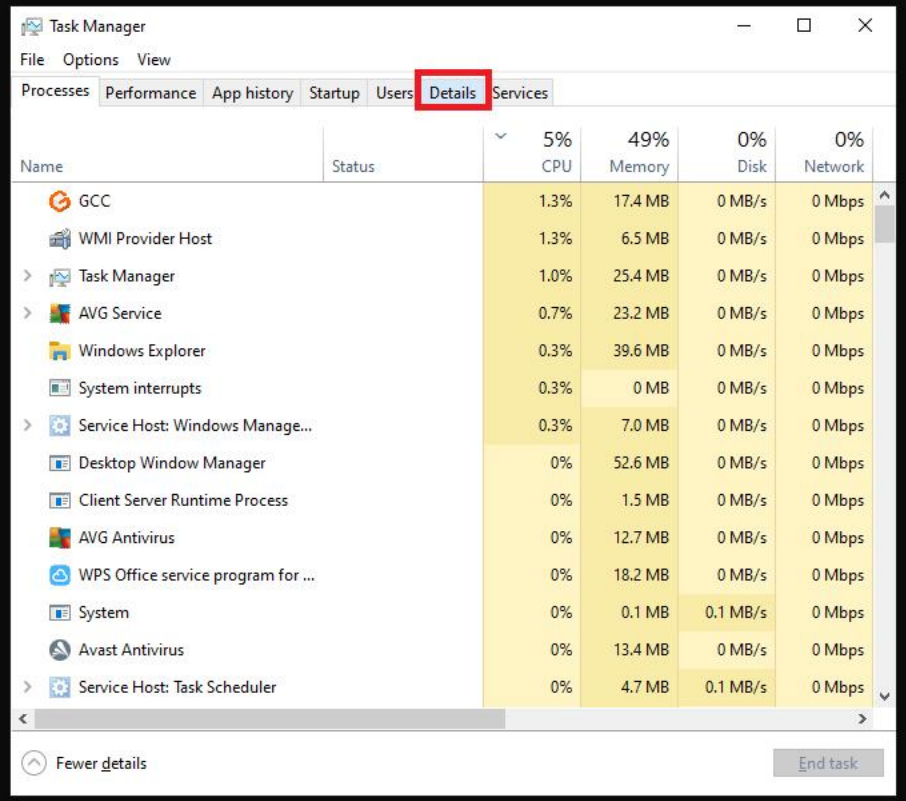
C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe

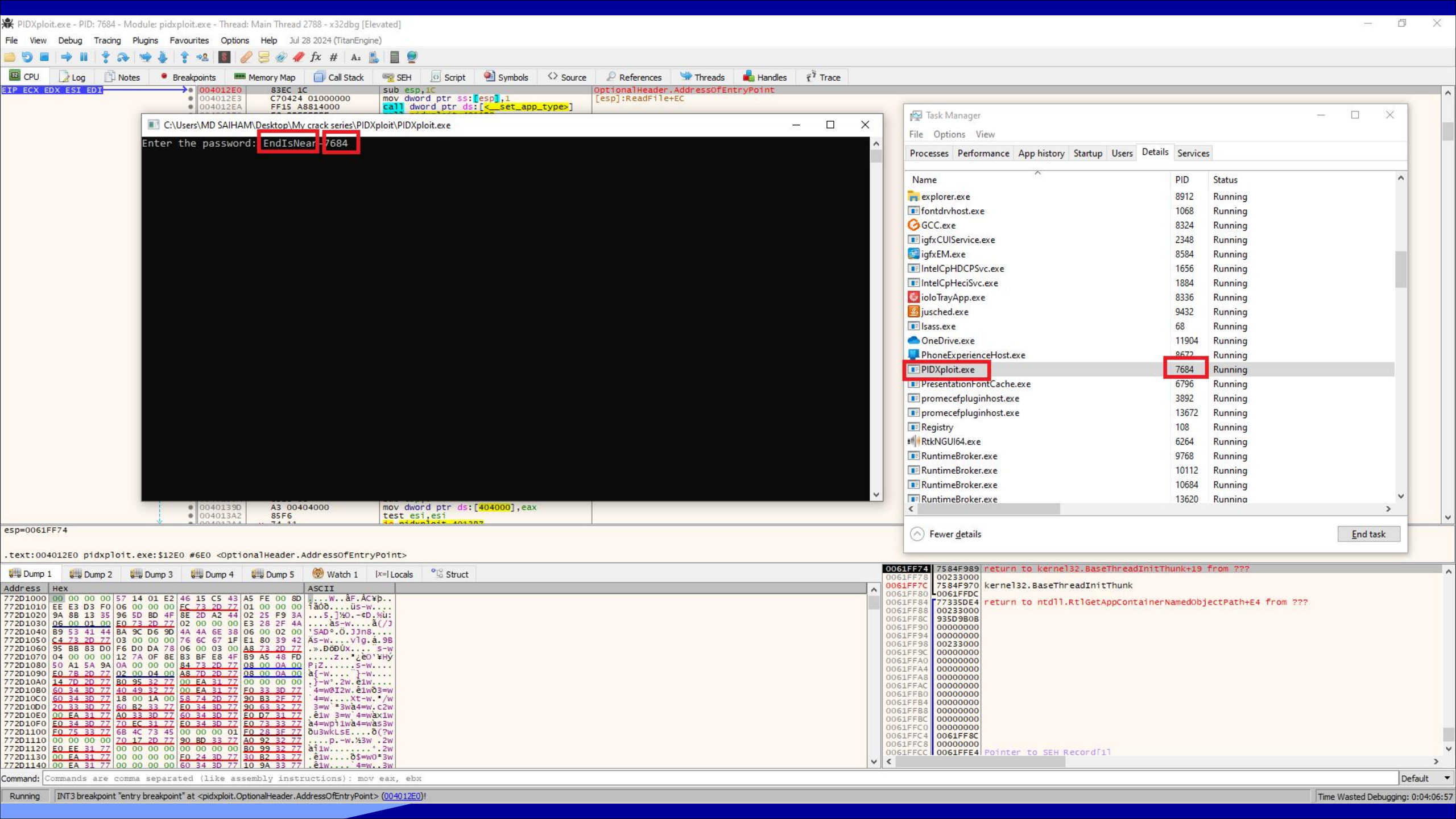
```
Enter the password:
```

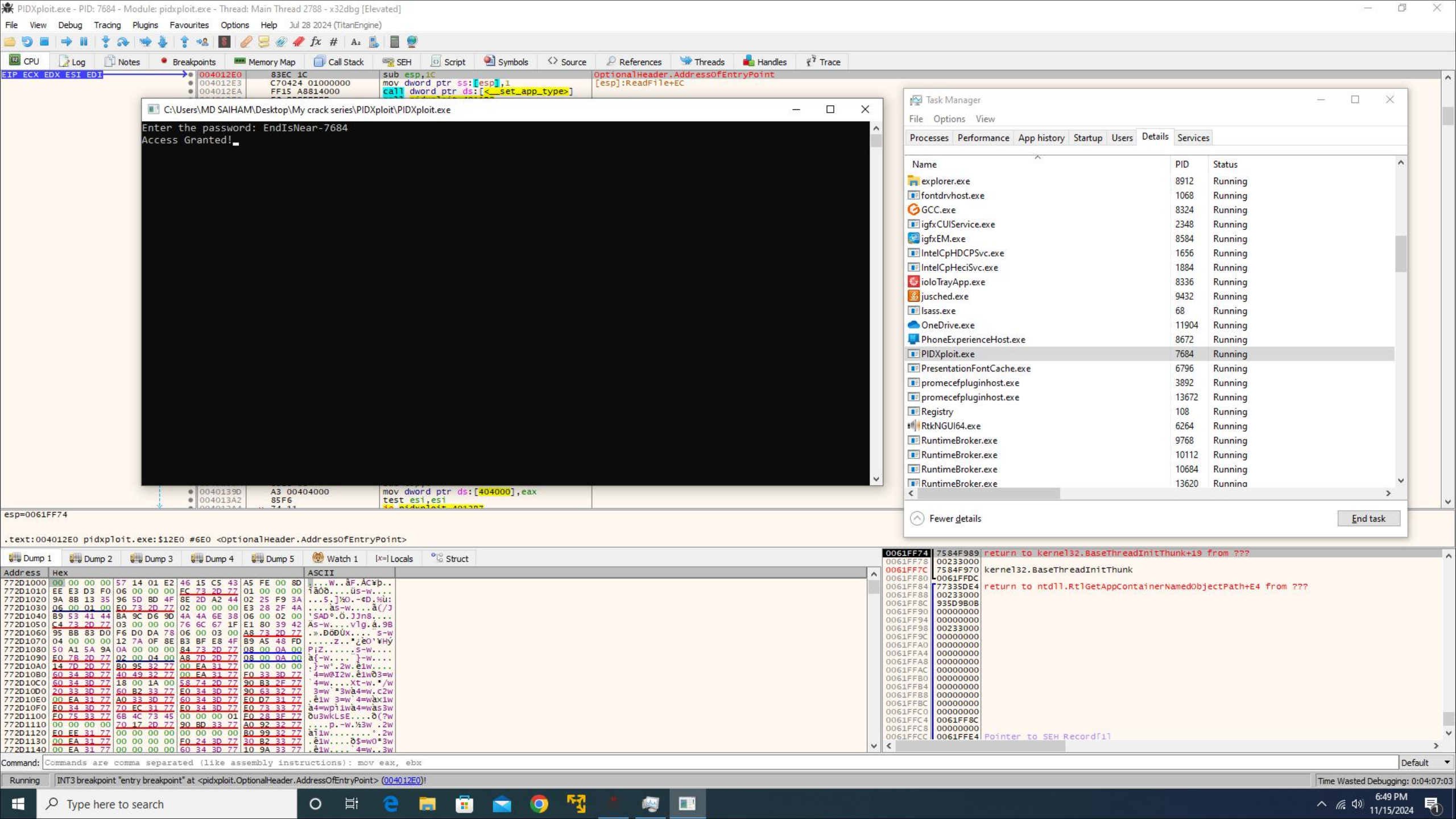


C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe

```
Enter the password:
```




PIDXploit.exe - PID: 7684 - Module: pidxploit.exe - Thread: Main Thread 2788 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
EIP ECX EDX ESI EDI
004012E0 83EC 1C sub esp,1C
004012E3 C70424 01000000 mov dword ptr ss:[esp],1
004012EA FF15 A8814000 call dword ptr ds:[<__set_app_type>]
OptionalHeader.AddressOfEntryPoint
[esp]:ReadFile+EC
C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe
Enter the password: EndIsNear-7684
0040139D A3 00404000 mov dword ptr ds:[404000],eax
004013A2 85F6 test esi,esi
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name PID Status
explorer.exe 8912 Running
fontdrvhost.exe 1068 Running
GCC.exe 8324 Running
igfxCUIService.exe 2348 Running
igfxEM.exe 8584 Running
IntelCpHDCPSvc.exe 1656 Running
IntelCpHeciSvc.exe 1884 Running
ioloTrayApp.exe 8336 Running
jusched.exe 9432 Running
lsass.exe 68 Running
OneDrive.exe 11904 Running
PhoneExperienceHost.exe 8672 Running
PIDXploit.exe 7684 Running
PresentationFontCache.exe 6796 Running
promecefpluginhost.exe 3892 Running
promecefpluginhost.exe 13672 Running
Registry 108 Running
RtkNGUI64.exe 6264 Running
RuntimeBroker.exe 9768 Running
RuntimeBroker.exe 10112 Running
RuntimeBroker.exe 10684 Running
RuntimeBroker.exe 13620 Running
Fewer details
End task
esp=0061FF74
.text:004012E0 pidxploit.exe:$12E0 #6E0 <OptionalHeader.AddressOfEntryPoint>
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct
Address Hex ASCII
0061FF74 7584F989 return to kernel32.BaseThreadInitThunk+19 from ???
0061FF78 00233000
0061FF7C 7584F970 kernel32.BaseThreadInitThunk
0061FF80 0061FFDC
0061FF84 77335DE4 return to ntdll.RtlGetAppContainerNamedObjectPath+E4 from ???
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Running
INT3 breakpoint "entry breakpoint" at <pidxploit.OptionalHeader.AddressOfEntryPoint> (004012E0)!
Time Wasted Debugging: 0:04:06:57


PIDXploit.exe - PID: 7684 - Module: pidxploit.exe - Thread: Main Thread 2788 - x32dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Jul 28 2024 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
EIP ECX EDX ESI EDI
004012E0 83EC 1C sub esp,1C
004012E3 C70424 01000000 mov dword ptr ss:[esp],1
004012EA FF15 A8814000 call dword ptr ds:[<__set_app_type>]
OptionalHeader.AddressOfEntryPoint
[esp]:ReadFile+EC
C:\Users\MD SAIHAM\Desktop\My crack series\PIDXploit\PIDXploit.exe
Enter the password: EndIsNear-7684
Access Granted!
0040139D A3 00404000 mov dword ptr ds:[404000],eax
004013A2 85F6 test esi,esi
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Name PID Status
explorer.exe 8912 Running
fontdrvhost.exe 1068 Running
GCC.exe 8324 Running
igfxCUIService.exe 2348 Running
igfxEM.exe 8584 Running
IntelCpHDCPSvc.exe 1656 Running
IntelCpHeciSvc.exe 1884 Running
ioloTrayApp.exe 8336 Running
jusched.exe 9432 Running
lsass.exe 68 Running
OneDrive.exe 11904 Running
PhoneExperienceHost.exe 8672 Running
PIDXploit.exe 7684 Running
PresentationFontCache.exe 6796 Running
promecefpluginhost.exe 3892 Running
promecefpluginhost.exe 13672 Running
Registry 108 Running
RtkNGUI64.exe 6264 Running
RuntimeBroker.exe 9768 Running
RuntimeBroker.exe 10112 Running
RuntimeBroker.exe 10684 Running
RuntimeBroker.exe 13620 Running
Fewer details
End task
esp=0061FF74
.text:004012E0 pidxploit.exe:$12E0 #6E0 <OptionalHeader.AddressOfEntryPoint>
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 [x=] Locals Struct
Address Hex ASCII
772D1000 00 00 00 00 57 14 01 E2 46 15 C5 43 A5 FE 00 8D
772D1010 EE E3 D3 F0 06 00 00 00 EC 73 2D 77 01 00 00 00
772D1020 9A 8B 13 35 96 5D BD 4F 8E 2D A2 44 02 25 F9 3A
772D1030 06 00 01 00 E0 73 2D 77 02 00 00 00 E3 28 2F 4A
772D1040 B9 53 41 44 BA 9C D6 9D 4A 4A 6E 38 06 00 02 00
772D1050 C4 73 2D 77 03 00 00 00 76 6C 67 1F E1 80 39 42
772D1060 95 BB 83 D0 F6 D0 DA 78 06 00 03 00 A8 73 2D 77
772D1070 04 00 00 00 12 7A 0F 8E B3 BF E8 4F B9 A5 48 FD
772D1080 50 A1 5A 9A 0A 00 00 00 84 73 2D 77 08 00 0A 00
772D1090 E0 7B 2D 77 02 00 04 00 A8 7D 2D 77 08 00 0A 00
772D10A0 14 7D 2D 77 B0 95 32 77 00 EA 31 77 00 00 00 00
772D10B0 60 34 3D 77 40 49 32 77 00 EA 31 77 F0 33 3D 77
772D10C0 60 34 3D 77 18 00 1A 00 58 74 2D 77 90 B3 2F 77
772D10D0 20 33 3D 77 60 B2 33 77 E0 34 3D 77 90 63 32 77
772D10E0 00 EA 31 77 A0 33 3D 77 60 34 3D 77 E0 D7 31 77
772D10F0 E0 34 3D 77 70 EC 31 77 E0 34 3D 77 E0 73 33 77
772D1100 E0 75 33 77 68 4C 73 45 00 00 00 01 E0 28 3F 77
772D1110 00 00 00 00 70 17 2D 77 90 BD 33 77 A0 92 32 77
772D1120 E0 EE 31 77 00 00 00 00 00 00 00 00 B0 99 32 77
772D1130 00 EA 31 77 00 00 00 00 E0 24 3D 77 30 B2 33 77
772D1140 00 EA 31 77 00 00 00 00 60 34 3D 77 10 9A 33 77
0061FF74 7584F989 return to kernel32.BaseThreadInitThunk+19 from ???
0061FF78 00233000
0061FF7C 7584F970 kernel32.BaseThreadInitThunk
0061FF80 0061FFDC
0061FF84 77335DE4 return to ntdll.RtlGetAppContainerNamedObjectPath+E4 from ???
0061FF88 00233000
0061FF8C 935D9B0B
0061FF90 00000000
0061FF94 00000000
0061FF98 00233000
0061FF9C 00000000
0061FFA0 00000000
0061FFA4 00000000
0061FFA8 00000000
0061FFAC 00000000
0061FFB0 00000000
0061FFB4 00000000
0061FFB8 00000000
0061FFBC 00000000
0061FFC0 00000000
0061FFC4 0061FF8C
0061FFC8 00000000
0061FFCC 0061FFE4 Pointer to SEH Record[1]
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Default
Running
INT3 breakpoint "entry breakpoint" at <pidxploit.OptionalHeader.AddressOfEntryPoint> (004012E0)!
Time Wasted Debugging: 0:04:07:03
Type here to search
6:49 PM
11/15/2024