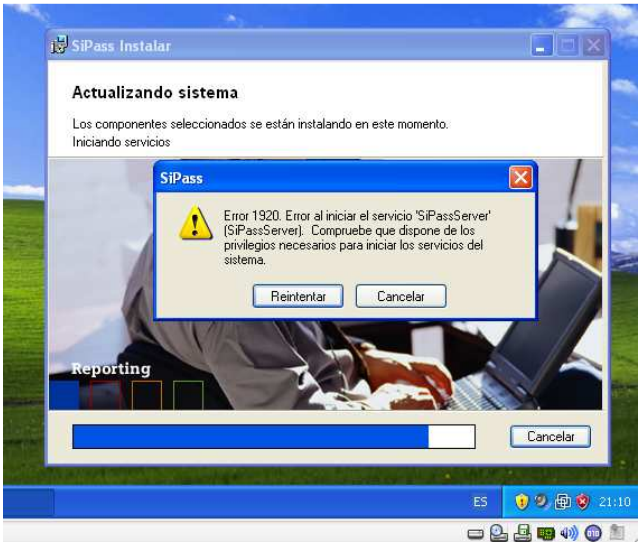
CRACKSLATINOS 2007
ORCA+OLLY+WINDBG+VMWARE II

ESTE DOCUMENTO ES DE CARÁCTER PUBLICO, SI LO COMPRASTE PIDE QUE TE DEVUELVAN TU DINERO.

Continuando…..

Cargamos la VM, llevamos el msi parchado y reinstalamos ahí:



En este punto, el windbg ya esta depurando a la vm (teoría 722 del maestro), sabemos que el servicio ya esta instalado y se niega a correr.

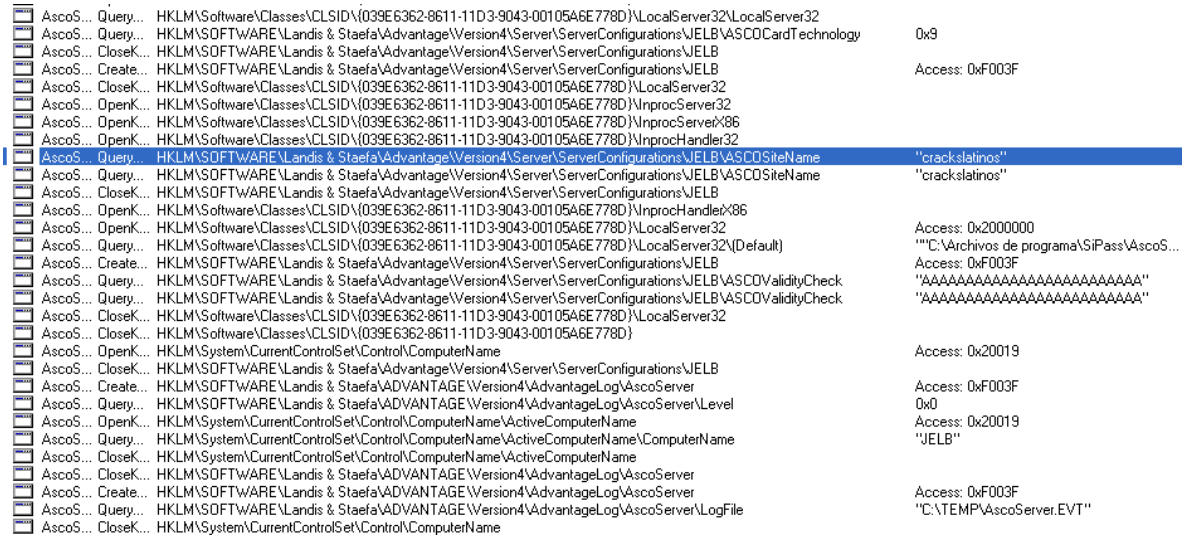
Lo que tenemos que hacer es depurar el servicio, tenemos que romper en el debugger justo donde sabemos que llama a la dll de las licencias.

No se me ocurre mucho, asi que robare la idea del armadillo team: nanomites.

Pondremos INT3 cerca de cada llamada y veremos los valores de retorno. Podemos tener el exe abierto en olly y guardar cambios, y usamos el service manager para arrancarlo en la vm.

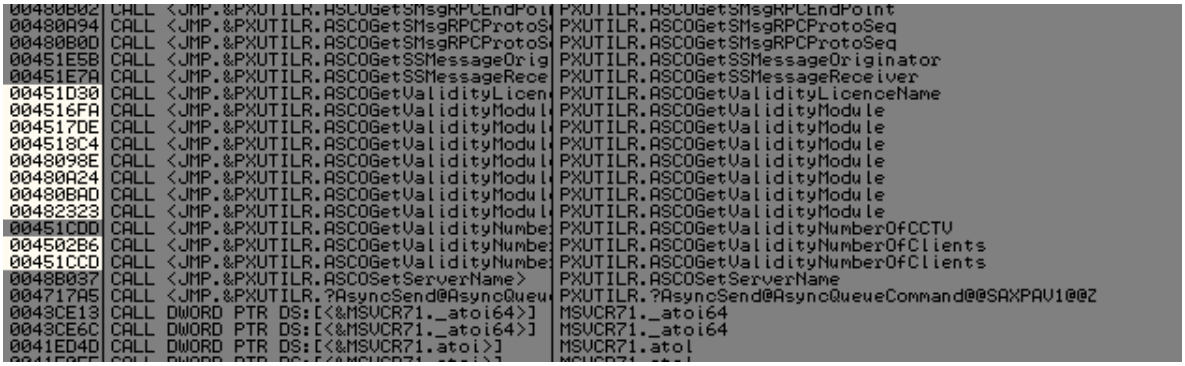
Veamos de nuevo los accesos al registro:

Cls2007



AscoS...	Query...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\LocalServer32\LocalServer32	
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB\ASCOCardTechnology	0x9
AscoS...	CloseK...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB	
AscoS...	Create...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB	Access: 0xF003F
AscoS...	CloseK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\LocalServer32	
AscoS...	OpenK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\InprocServer32	
AscoS...	OpenK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\InprocServerX86	
AscoS...	OpenK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\InprocHandler32	
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB\ASCOSiteName	"crackslatinos"
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB\ASCOSiteName	"crackslatinos"
AscoS...	CloseK...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB	
AscoS...	OpenK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\InprocHandlerX86	
AscoS...	OpenK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\LocalServer32	Access: 0x2000000
AscoS...	Query...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\LocalServer32\(Default)	""C:\Archivos de programa\SiPass\AscoS...
AscoS...	Create...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB	Access: 0xF003F
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB\ASCOValidityCheck	"AAAAAAAAAAAAAAAAAAAAAAAA"
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB\ASCOValidityCheck	"AAAAAAAAAAAAAAAAAAAAAAAA"
AscoS...	CloseK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}\LocalServer32	
AscoS...	CloseK...	HKLM\Software\Classes\CLSID\{039E6362-8611-11D3-9043-00105A6E778D}	
AscoS...	OpenK...	HKLM\System\CurrentControlSet\Control\ComputerName	Access: 0x20019
AscoS...	CloseK...	HKLM\SOFTWARE\Landis & Staefa\Advantage\Version4\Server\ServerConfigurations\JELB	
AscoS...	Create...	HKLM\SOFTWARE\Landis & Staefa\ADVANTAGE\Version4\AdvantageLog\AscoServer	Access: 0xF003F
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\ADVANTAGE\Version4\AdvantageLog\AscoServer\Level	0x0
AscoS...	OpenK...	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	Access: 0x20019
AscoS...	Query...	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName\ComputerName	"JELB"
AscoS...	CloseK...	HKLM\System\CurrentControlSet\Control\ComputerName\ActiveComputerName	
AscoS...	CloseK...	HKLM\SOFTWARE\Landis & Staefa\ADVANTAGE\Version4\AdvantageLog\AscoServer	
AscoS...	Create...	HKLM\SOFTWARE\Landis & Staefa\ADVANTAGE\Version4\AdvantageLog\AscoServer	Access: 0xF003F
AscoS...	Query...	HKLM\SOFTWARE\Landis & Staefa\ADVANTAGE\Version4\AdvantageLog\AscoServer\LogFile	"C:\TEMP\AscoServer.EVT"
AscoS...	CloseK...	HKLM\System\CurrentControlSet\Control\ComputerName	

Vemos que accesa el SiteName, veamos las Apis:

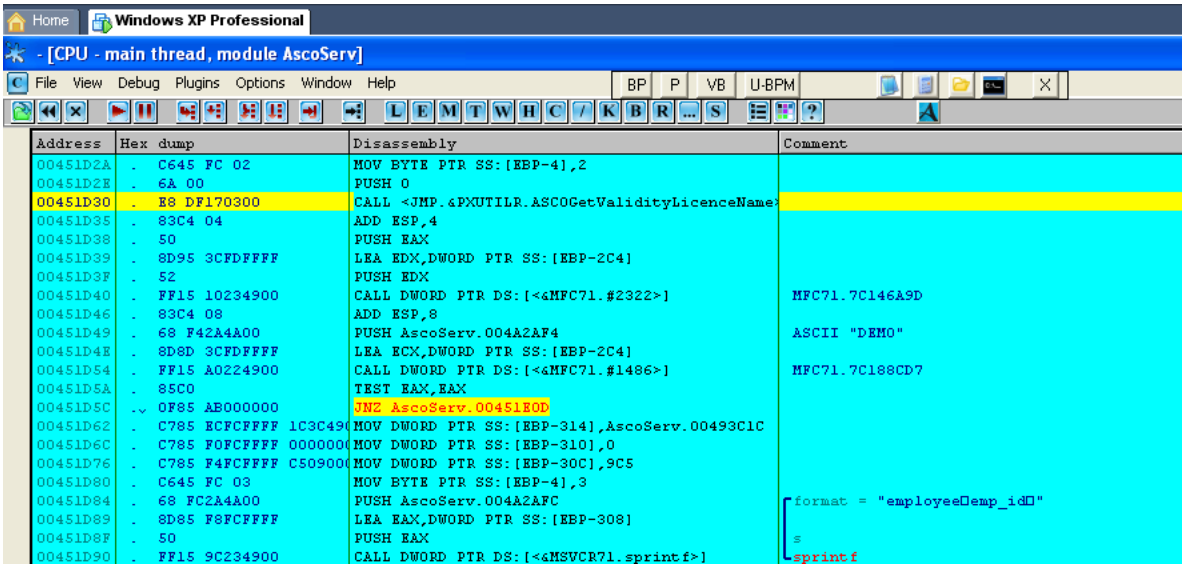


```
00480B02 CALL <JMP.&PXUTILR.ASCOGetSMsgRPCEndPoi PXUTILR.ASCOGetSMsgRPCEndPoint
00480A94 CALL <JMP.&PXUTILR.ASCOGetSMsgRPCProtoS PXUTILR.ASCOGetSMsgRPCProtoSeq
00480B0D CALL <JMP.&PXUTILR.ASCOGetSMsgRPCProtoS PXUTILR.ASCOGetSMsgRPCProtoSeq
00451E5B CALL <JMP.&PXUTILR.ASCOGetSSMessageOrig PXUTILR.ASCOGetSSMessageOriginator
00451E7A CALL <JMP.&PXUTILR.ASCOGetSSMessageRece PXUTILR.ASCOGetSSMessageReceiver
00451D30 CALL <JMP.&PXUTILR.ASCOGetValidityLicen PXUTILR.ASCOGetValidityLicenceName
004516FA CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
004517DE CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
004518C4 CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
0048098E CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
00480A24 CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
00480BAD CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
00482323 CALL <JMP.&PXUTILR.ASCOGetValidityModul PXUTILR.ASCOGetValidityModule
00451CDD CALL <JMP.&PXUTILR.ASCOGetValidityNumbe PXUTILR.ASCOGetValidityNumberOfCCTV
004502B6 CALL <JMP.&PXUTILR.ASCOGetValidityNumbe PXUTILR.ASCOGetValidityNumberOfClients
00451CCD CALL <JMP.&PXUTILR.ASCOGetValidityNumbe PXUTILR.ASCOGetValidityNumberOfClients
0048B037 CALL <JMP.&PXUTILR.ASCOSetServerName>   PXUTILR.ASCOSetServerName
004717A5 CALL <JMP.&PXUTILR.?AsyncSend@AsyncQueu PXUTILR.?AsyncSend@AsyncQueueCommand@@SAXPAV1@@Z
0043CE13 CALL DWORD PTR DS:[<&MSVCR71._atoi64>]  MSVCR71._atoi64
0043CE6C CALL DWORD PTR DS:[<&MSVCR71._atoi64>]  MSVCR71._atoi64
0041ED4D CALL DWORD PTR DS:[<&MSVCR71.atoi>]     MSVCR71.atol
```

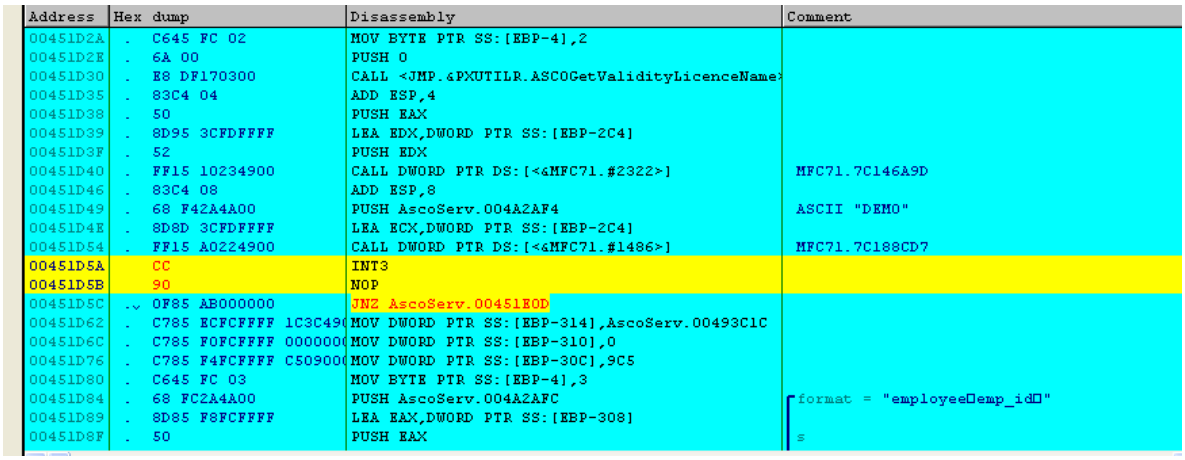
ValidityLicenceName es una candidata que resalta.

Veamos la zona a la llamada:

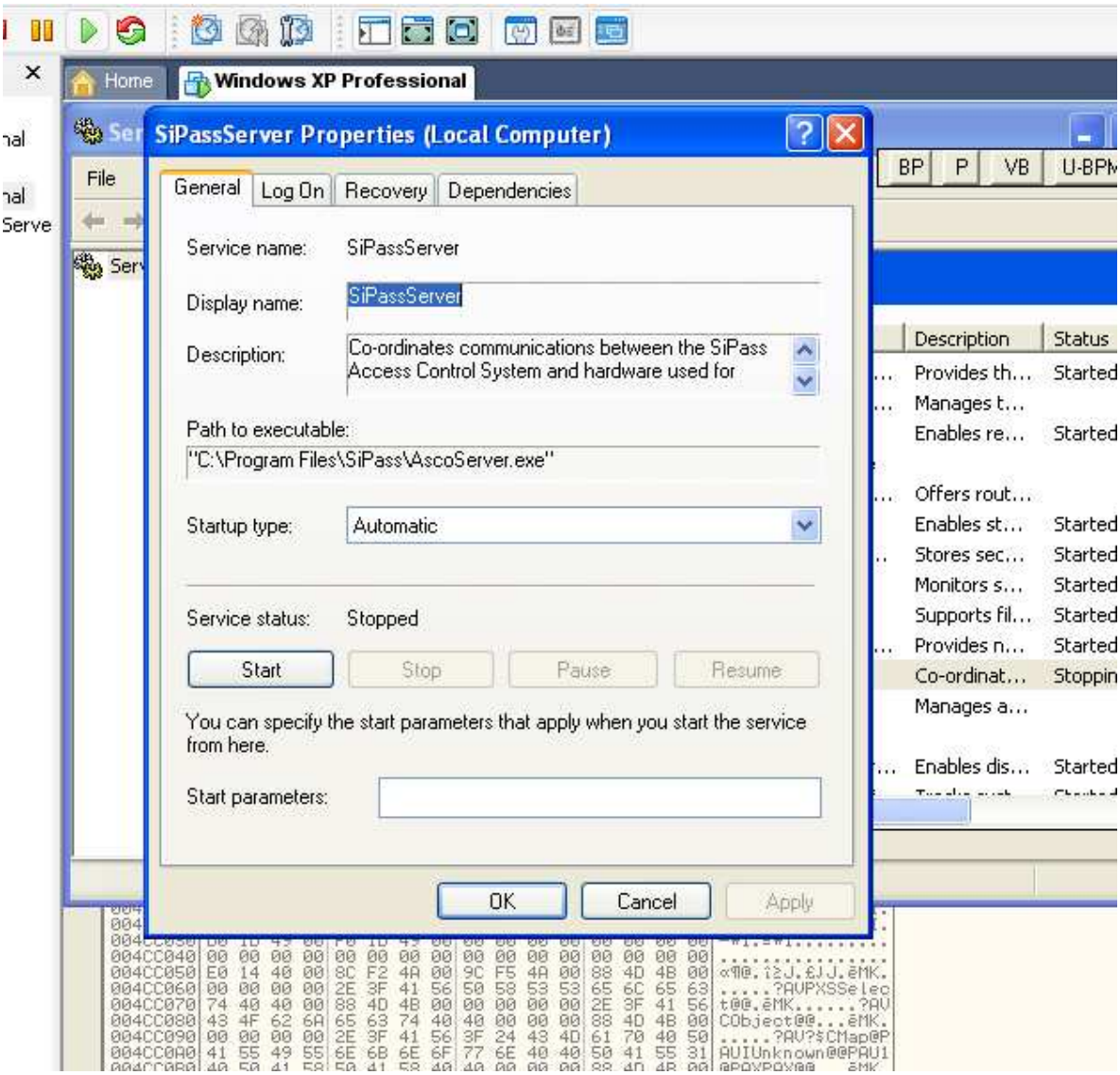
Cls2007



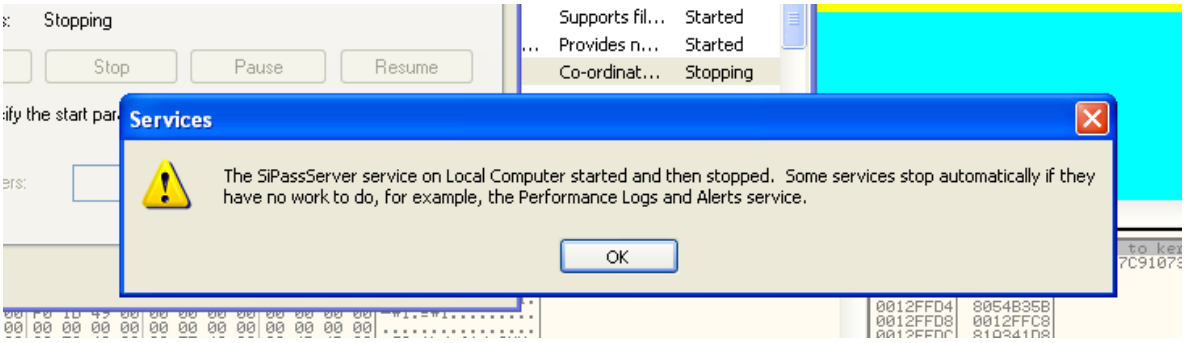
Pues ahí valida que no sea demo, ponemos el int3 en 451d5a, guardamos el exe y rearrancamos el servicio:



Cls2007

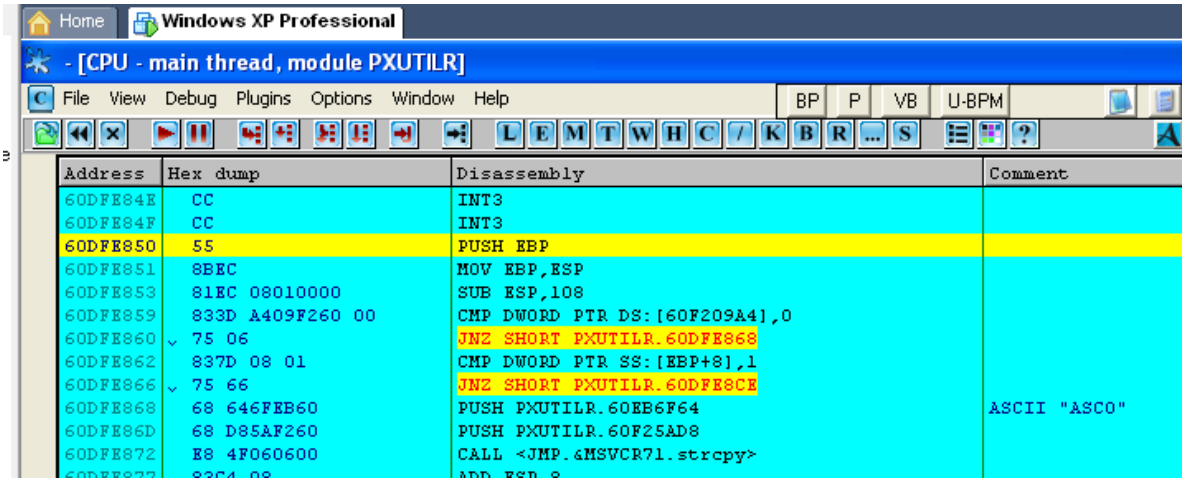


Al darle start:

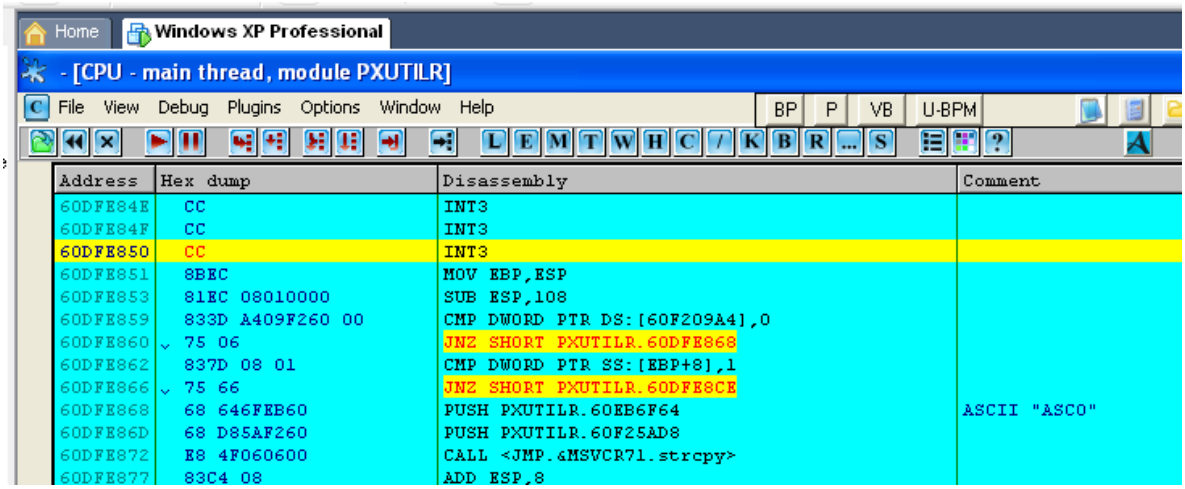


Pues no hubo interrupción, el código del exe del servicio no pasa por ahí, veamos si alguien mas usa la api, pondremos el int3 dentro de la dll asi:

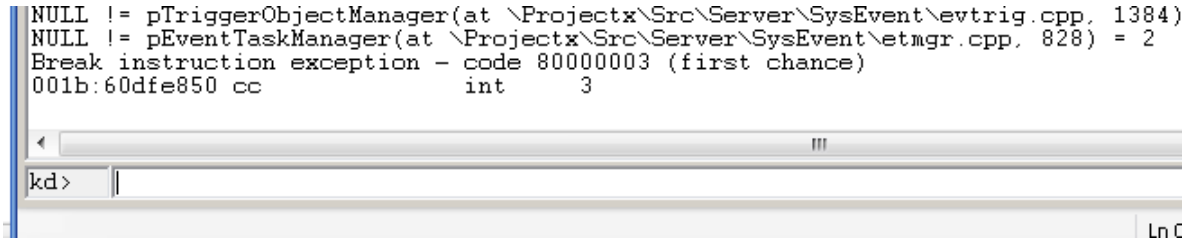
Cls2007



Ahí en ValidityLicenceName, luego:



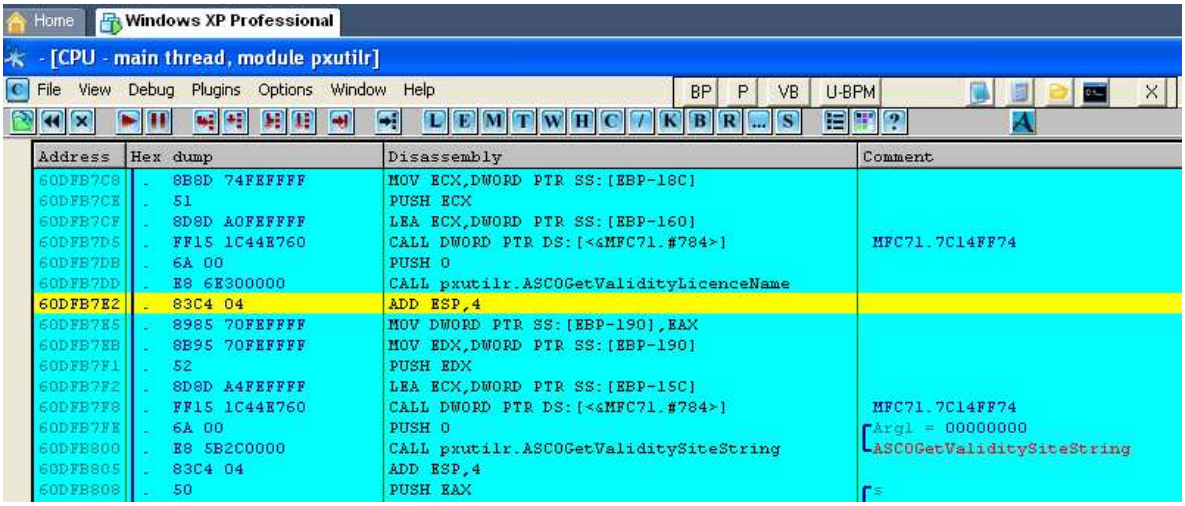
Reiniciamos el servicio y:



Ahí salto el debugger, no es ascoserver.exe el primero en accesar el registro, es alguien mas, veamos quien es:

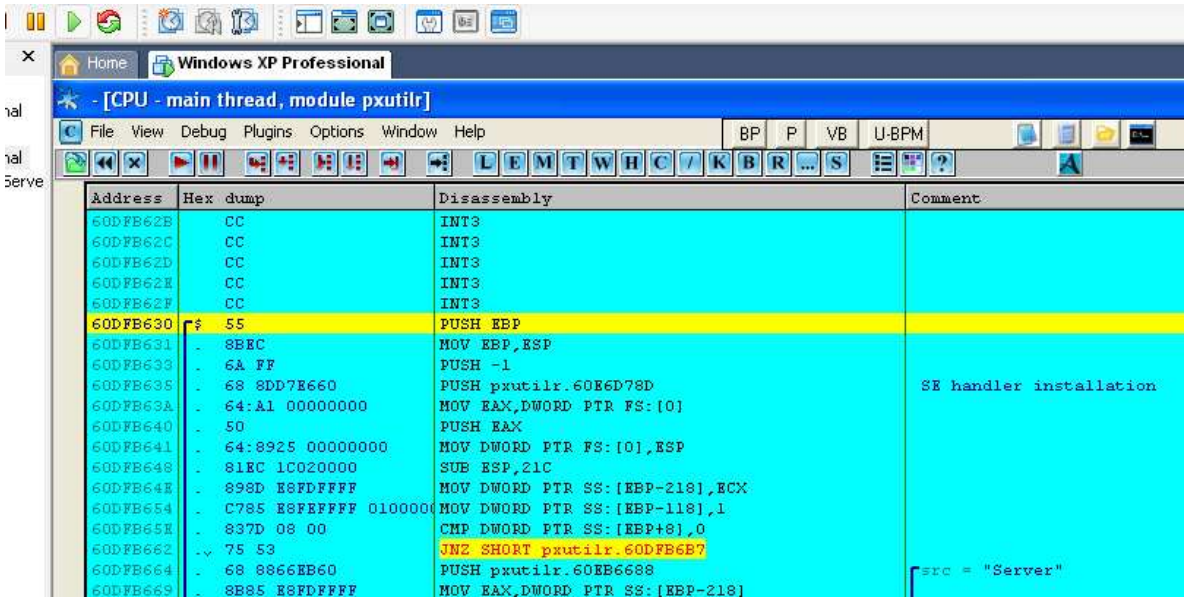
```
Break instruction exception - code 80000003 (first chance)
001b:60dfe850 cc              int     3
kd> eb eip 55
kd> u
001b:60dfe850 55              push    ebp
001b:60dfe851 8bec            mov     ebp,esp
001b:60dfe853 81ec08010000    sub     esp,108h
001b:60dfe859 833da409f26000  cmp     dword ptr ds:[60F209A4h],0
001b:60dfe860 7506            jne     60dfe868
001b:60dfe862 837d0801        cmp     dword ptr [ebp+8],1
001b:60dfe866 7566            jne     60dfe8ce
001b:60dfe868 68646feb60      push    60EB6F64h
kd> d esp
00aafa94  e2 b7 df 60 00 00 00 00-00 00 00 00 04 5d 88 8a  ...`.........]..
00aafaa4  48 00 00 00 2a 54 de 77-58 66 f2 60 03 00 00 00  H...*T.wXf.`....
00aafab4  38 54 de 77 50 fd aa 00-00 00 00 00 00 00 00 00  8T.wP...........
00aafac4  24 54 de 77 f2 1d de 77-00 00 00 00 00 00 00 00  $T.w...w........
00aafad4  00 00 00 00 00 00 00 00-10 fb aa 00 00 00 3f 00  ..............?.
00aafae4  32 07 91 7c 06 00 00 00-a8 07 3f 00 00 00 3f 00  2..|......?...?.
00aafaf4  00 00 00 00 e8 fa aa 00-00 00 00 00 2c fd aa 00  ............,...
00aafb04  18 ee 90 7c 38 07 91 7c-ff ff ff ff 32 07 91 7c  ...|8..|....2..|
```

Ahí se ve el código de la api, y la pila, donde esta la dirección de retorno, 60dfb7e2, damos g al windbg y veamos en el olly de la vm esa dirección que al parecer es de la dll:

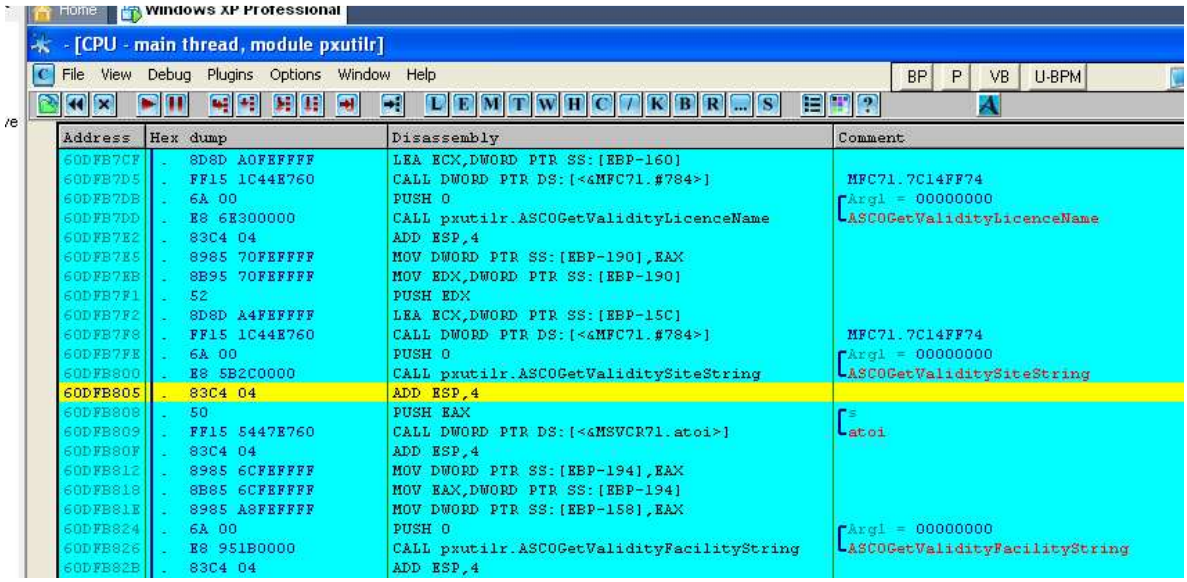


Pues ahí esta, vemos que la llamada es parte de una subrutina muy larga, buscamos el inicio:

Cls2007

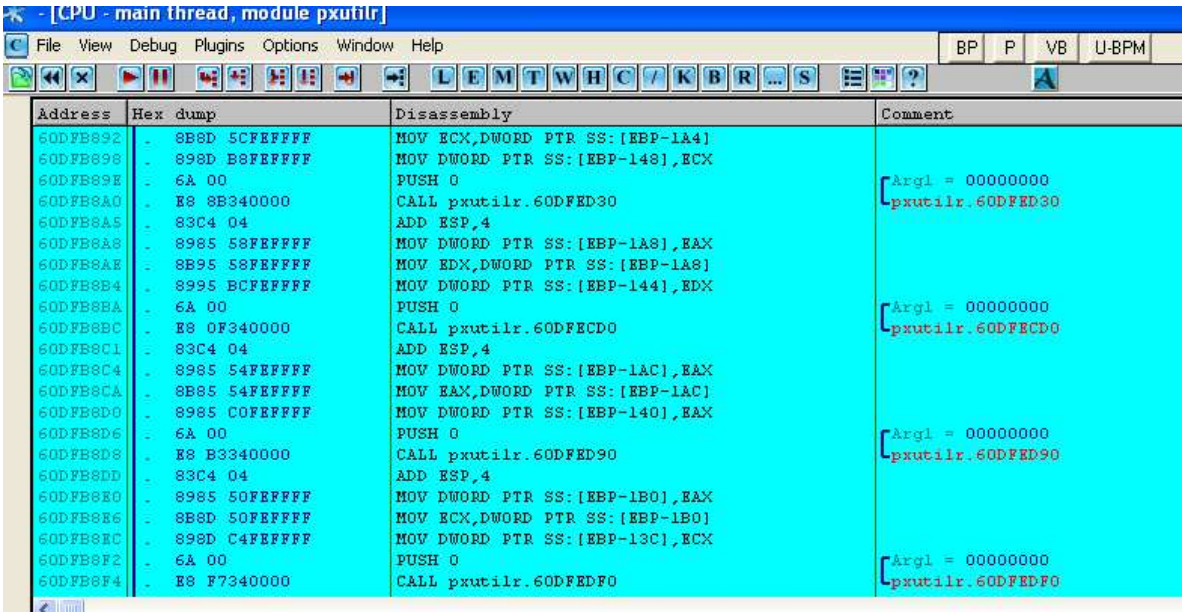


Ahora si analizamos la rutina hacia abajo, podemos ver como va accesando los campos del registro:

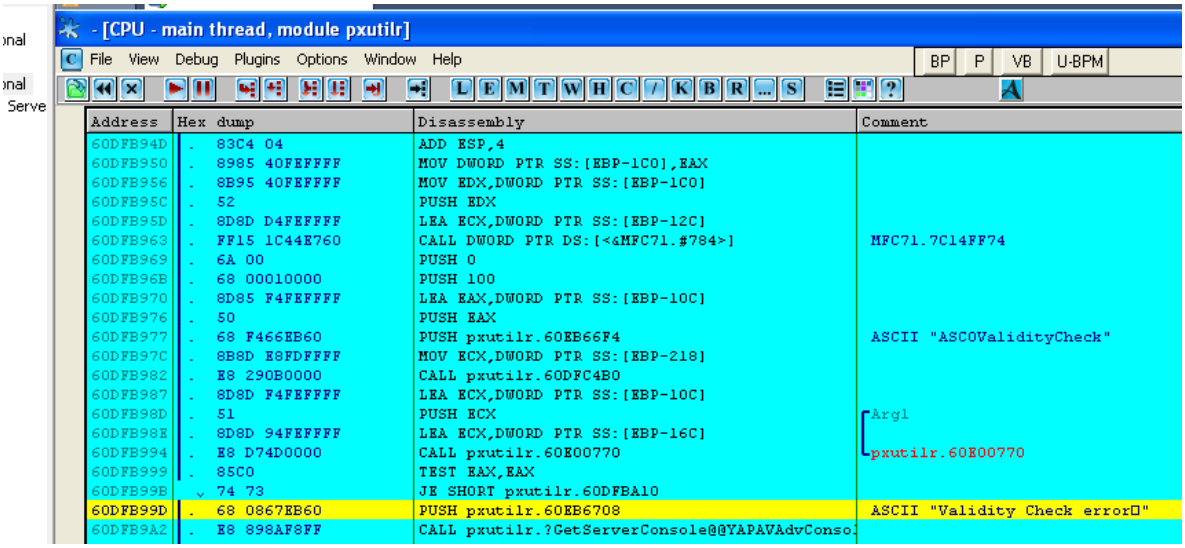


Luego vean como empieza a escribir los datos en una tabla, probablemente de donde el servicio leera luego:

Cls2007



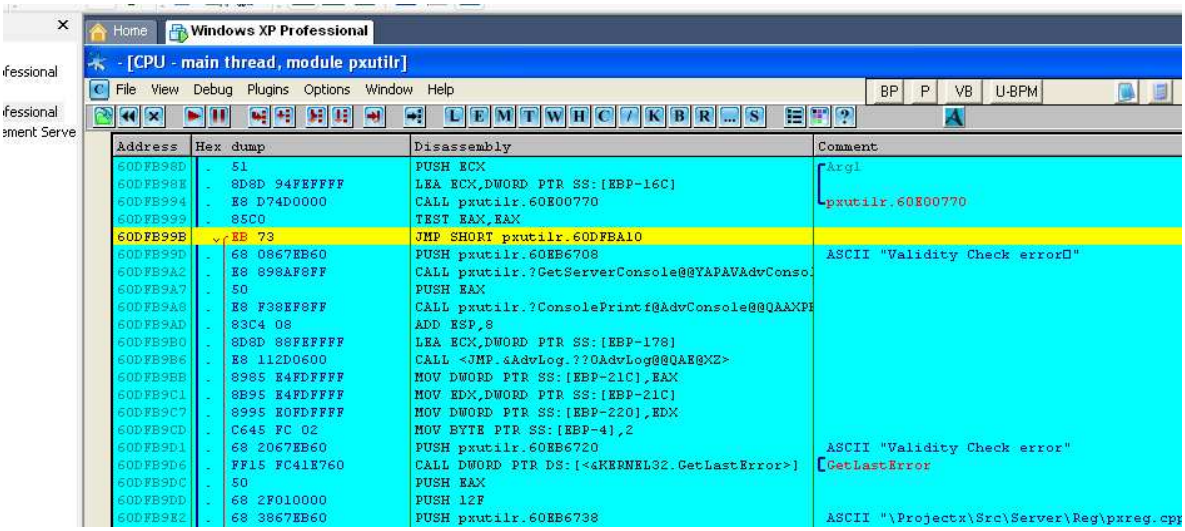
Lo interesante es al final de esta rutina:



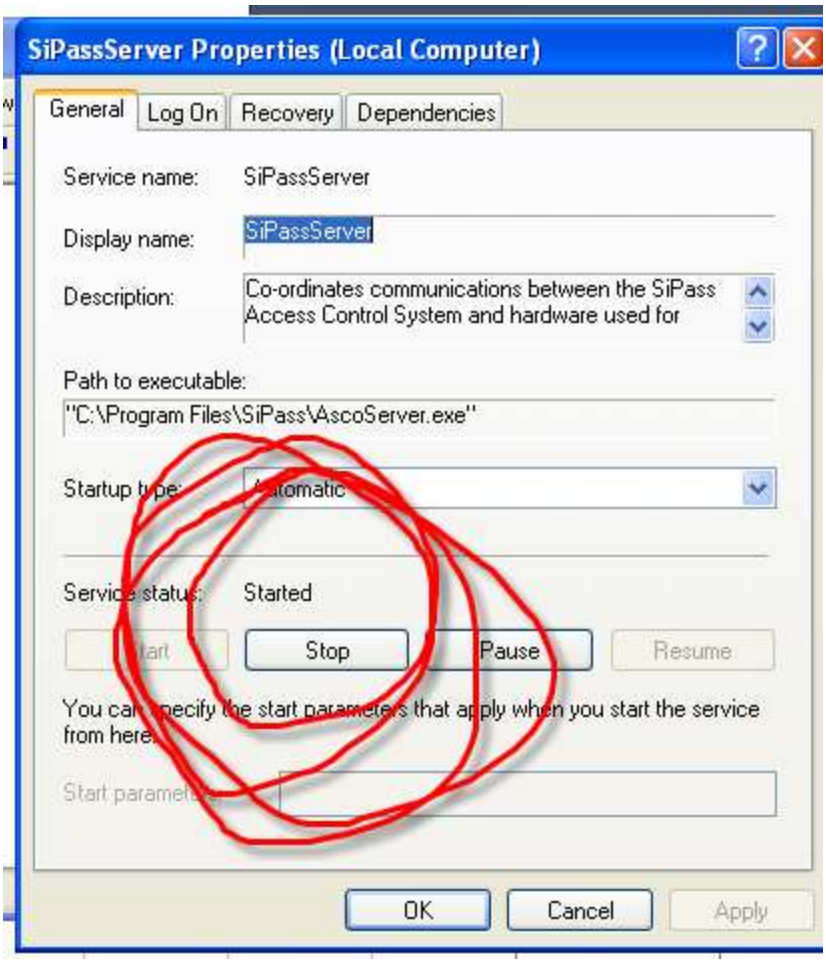
Bueno, ahí un salto mágico en 60dfb99d.

Con olly lo cambiamos para que siempre salte:

Cls2007



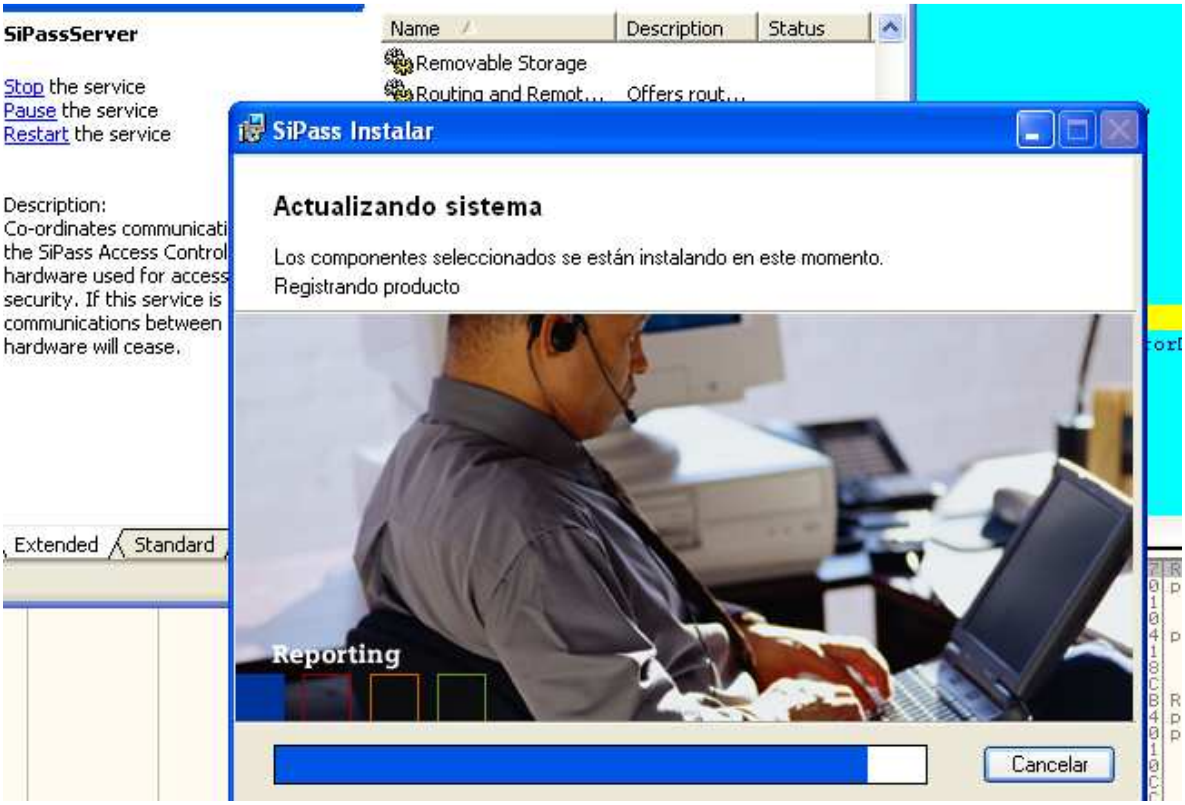
Y ahora reintentamos de nuevo arrancar el servicio:



Cls2007

Yes yes yes!!!!!!!!!!!!!!!!!

Volvamos al instalador, y le damos reintentar:



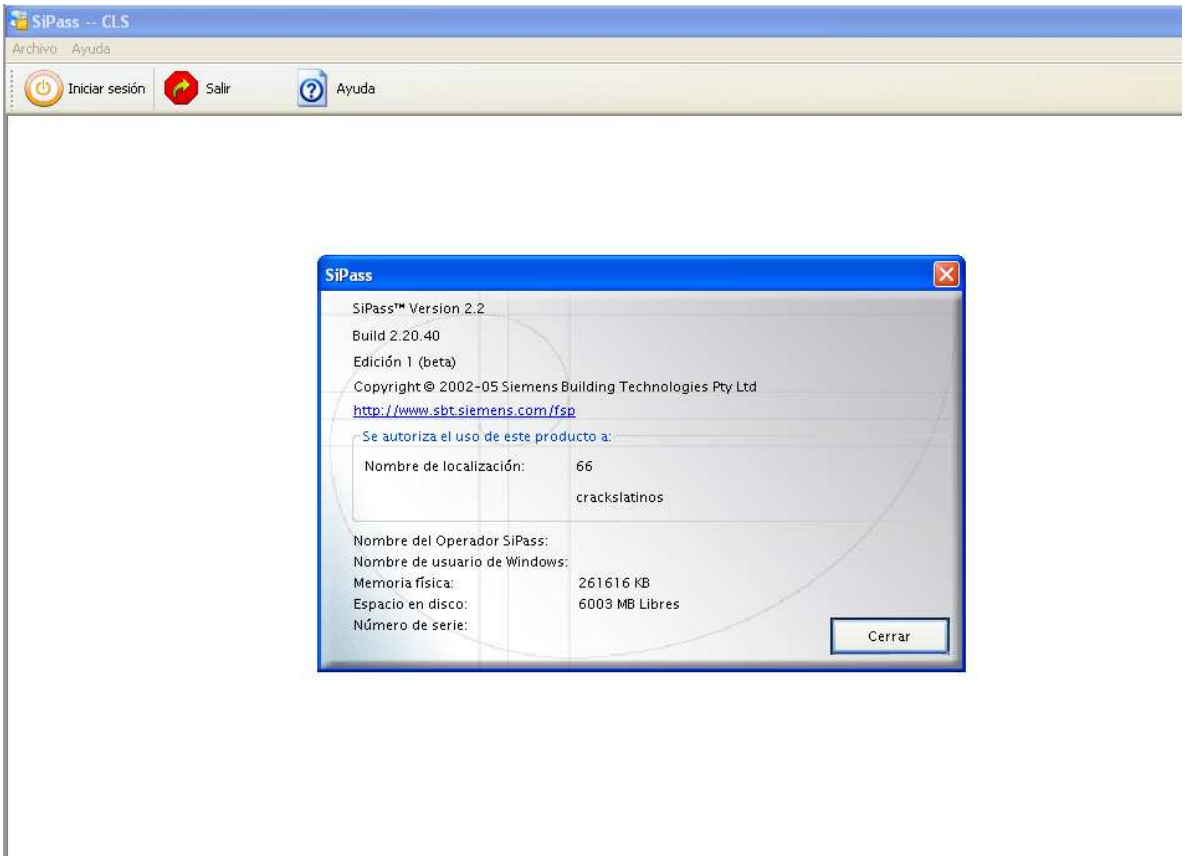
Yes yes ¡!!!!!!!!

Y Luego:

Cls2007

Solo falta verificar si arranca registrado:}

Cls2007



Sip.

Ahí esta, después de mucho pensar y trabajar.

Estuvo difícil, pero lo aprendido es muuchisiiisisisismo, eso es lo que importa.

Esto no hubiese podido llegar a feliz termino sin la ayuda y sabiduría de crackslatinos, un saludo a todos los listeros y gracias mil por el apoyo y sobre todo la amistad.

CRACKSLATINOS 2007

Joref.