

Tersine Mühendisliğin Faydaları

written by Mert SARICA | 8 April 2010

Herkes gider Mersin'e biz gidelim tersine diyerek bu haftanın yazısında tersine mühendisliğin (reverse engineering) kullanım alanlarından kısaca bahsedeceğim. Öncelikle Tersine Mühendislik nedir diye Vikipedi'ye soracak olursak alacağımız yanıt aşağıdaki gibi olacaktır.

Tersine mühendislik (Reverse Engineering, RE) bir aygıtın, objenin veya sistemin; yapısının, işlevinin veya çalışmasının, çıkarımcı bir akıl yürütme analiziyle keşfedilmesi işlemidir. Bu yöntem, genellikle orijinalinden kopyalamadan onunla aynı şeyi yapan yeni bir alet veya yazılım yapmaya çalışır ve sıklıkla bir şeylerin (örneğin; makine veya mekanik alet, elektronik komponent, yazılım programı gibi) parçalarına ayrılması ve çalışma prensiplerinin detaylı şekilde analizini içerir.

Tersine mühendislik ile ilgili bilinen en meşhur hikaye ise 1980'li yılların ortasında rahmetli Compaq firmasının o zamanlar sadece IBM PC'lerde mevcut olan BIOS'u tersine mühendislikten faydalanarak kopyalaması ve Compaq PCler'i üretmesidir. Daha sonra Phoenix Teknoloji firması aynı yolla BIOS'u kopyalamış ve kendi PCler'ini üretmek yerine diğer PC üreticilerine BIOS'u satarak günümüzde her eve ucuz PC girmesine imkan tanımıştır.

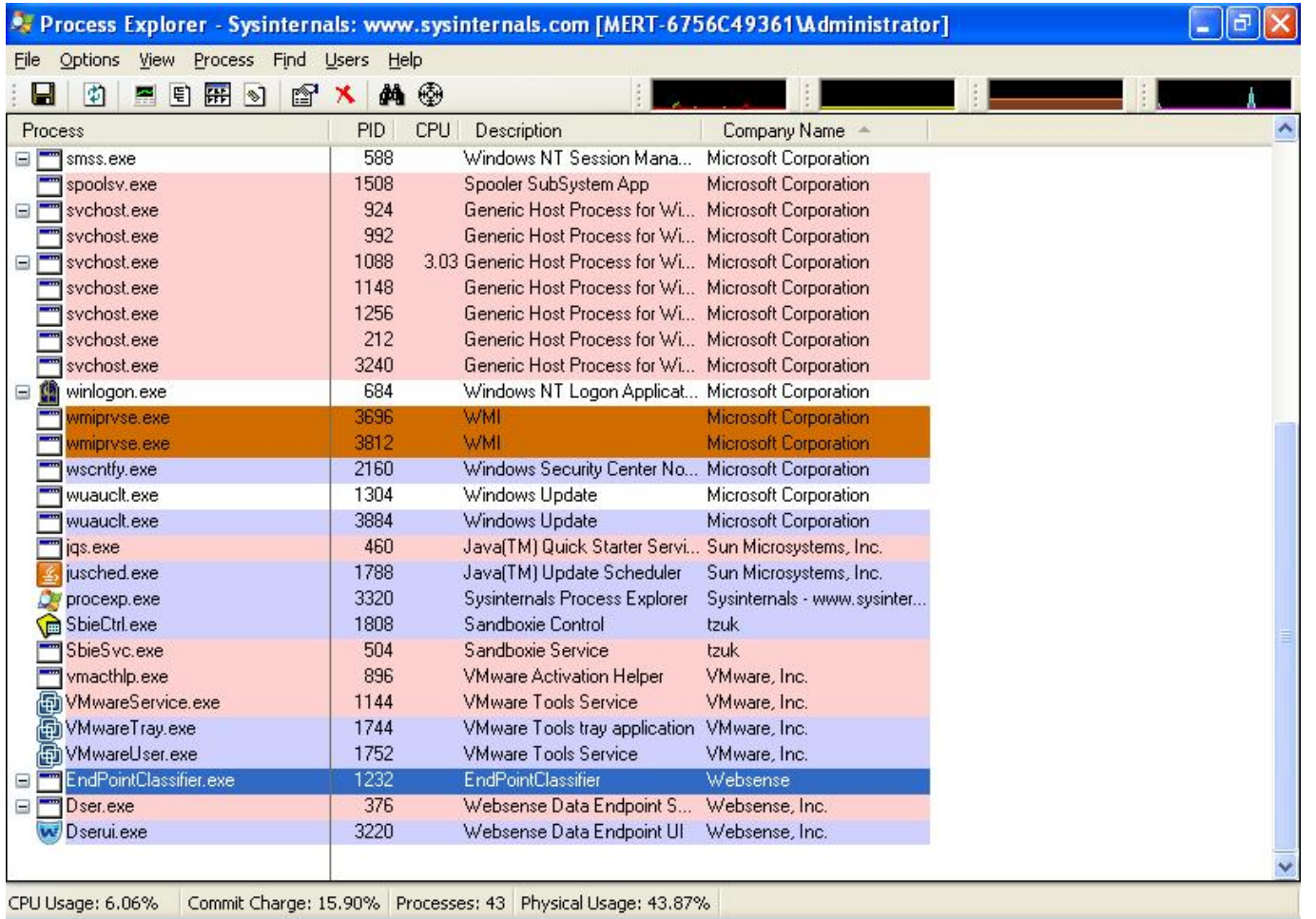
Günümüze gelecek olursak günümüz korsanları açık kaynak koda sahip olmayan yazılımlarda (Örneğin MS office uygulamaları) güvenlik açığı bulmak için tersine mühendislikten faydalanmaktadırlar. Hatta tersine mühendisliği otomatize ederek her ayın 2. haftasında Salı günü Microsoft firması tarafından yayınlanan yamalar tersine mühendislik ile analiz edilmekte ve 30 dakika ile 1 saat arasında istismar araçları (exploit) hazırlanabilmektedir.

Bunun dışında tersine mühendisliğe güvenlik testlerinde de yer verilmektedir. Hedef programın akışını değiştirmek kimi zaman programda yetkiniz olmayan bölümlere erişmenize imkan tanıyabilmektedir. Örneğin geçtiğimiz senelerde şifre saklamak için kullanılan bir programı incelemiştim. Program açıldığında sizden doğru kullanıcı adı ve şifre girmenizi istiyordu ve doğru ikili girildiği taktirde ana menüye yönlendirerek ana şifrenin görüntülenmesini

sağlıyordu. Programı assembly debugger ile kısa bir süre inceledikten sonra programın akışını değiştirerek doğrulama adımını bypass etmek ve ana şifreye ulaşmak mümkün olmuştu.

Ayrıca tersine mühendislik, programların içerisinde yer alan ancak dokümente edilmeyen gizli komutları/parametreleri ve özellikleri ortaya çıkarmak içinde kullanılmaktadır. Örneğin komut satırında programın desteklediği komutları listelediğinizde 2 komut olduğu gösterilirken, assembly debugger ile incelediğinizde gerçekte 4 komutun desteklendiğini görebilirsiniz. Hazır elimde bu konu ile ilgili bir örnek varken sizle paylaşmak istedim.

Elime geçtiğimiz günlerde üzerinde herhangi bir politika barındırmayan Websense Data Endpoint ajanı geçti. Yine canımın sıkıldığı bir akşam ajanı kurmaya ve göz atmaya karar verdim. Kurulum tamamlandıktan sonra ilk işim Process Explorer uygulaması ile ajan ile ilişkili programları keşfetmek olduk. Görebildiğim kadarıyla bu programlar Dser.exe, Dserui.exe, EndPointClassifier.exe ve kvoop.exe idi.

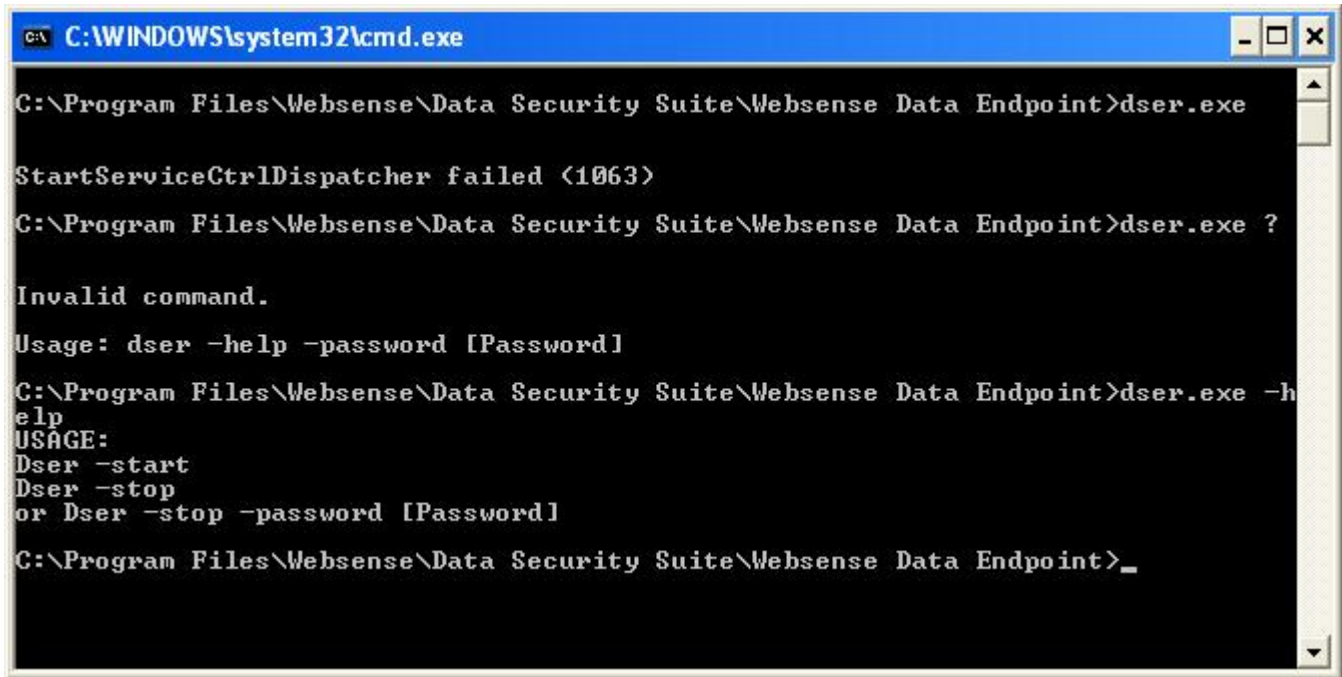


Process	PID	CPU	Description	Company Name
smss.exe	588		Windows NT Session Mana...	Microsoft Corporation
spoolsv.exe	1508		Spooler SubSystem App	Microsoft Corporation
svchost.exe	924		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	992		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1088	3.03	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1148		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1256		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	212		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	3240		Generic Host Process for Wi...	Microsoft Corporation
winlogon.exe	684		Windows NT Logon Applicat...	Microsoft Corporation
wmiprvse.exe	3696		WMI	Microsoft Corporation
wmiprvse.exe	3812		WMI	Microsoft Corporation
wscntfy.exe	2160		Windows Security Center No...	Microsoft Corporation
wuauclt.exe	1304		Windows Update	Microsoft Corporation
wuauclt.exe	3884		Windows Update	Microsoft Corporation
iqs.exe	460		Java(TM) Quick Starter Servi...	Sun Microsystems, Inc.
jtsched.exe	1788		Java(TM) Update Scheduler	Sun Microsystems, Inc.
procexp.exe	3320		Sysinternals Process Explorer	Sysinternals - www.sysinter...
SbieCtrl.exe	1808		Sandboxie Control	tzuk
SbieSvc.exe	504		Sandboxie Service	tzuk
vmacthlp.exe	896		VMware Activation Helper	VMware, Inc.
VMwareService.exe	1144		VMware Tools Service	VMware, Inc.
VMwareTray.exe	1744		VMware Tools tray application	VMware, Inc.
VMwareUser.exe	1752		VMware Tools Service	VMware, Inc.
EndPointClassifier.exe	1232		EndPointClassifier	Websense
Dser.exe	376		Websense Data Endpoint S...	Websense, Inc.
Dserui.exe	3220		Websense Data Endpoint UI	Websense, Inc.

CPU Usage: 6.06% Commit Charge: 15.90% Processes: 43 Physical Usage: 43.87%

Process Explorer ile Dser.exe ve EndPointClassifier.exe programlarını kapattığımda otomatik olarak tekrar çalıştığını gördüm. Komut satırından

Dser.exe uygulamasını çalıştırdığımda önce ufak bir hata mesajı aldım daha sonra ? parametresi ile çalıştırmayı denediğimde program desteklediği komutları listeledi.



```
C:\WINDOWS\system32\cmd.exe

C:\Program Files\WebSense\Data Security Suite\WebSense Data Endpoint>dser.exe

StartServiceCtrlDispatcher failed (1063)

C:\Program Files\WebSense\Data Security Suite\WebSense Data Endpoint>dser.exe ?

Invalid command.

Usage: dser -help -password [Password]

C:\Program Files\WebSense\Data Security Suite\WebSense Data Endpoint>dser.exe -h
elp
USAGE:
Dser -start
Dser -stop
or Dser -stop -password [Password]

C:\Program Files\WebSense\Data Security Suite\WebSense Data Endpoint>_
```

Sanıyorumki üzerinde herhangi bir politika yüklü olmadığı için dser.exe -stop yazarak çalışan servisi ve çalışan programları kapatabildim. Tahminimce politika bağlı olarak -password parametresi ve doğru şifre ile tüm programları ve servisleri kapatmak mümkün oluyor ancak dediğim gibi herhangi bir politika yüklü olmadığı için ve bu şekilde kapanabildiği için diğer ürünlerde olduğu gibi bypass etme girişiminde bulunmadım.

Immunity Debugger ile Dser.exe programına göz atıp program üzerinde yer alan metinleri listelediğimde listelenen komutların dışında 5 tane daha komut (parametre) olduğunu gördüm.

Immunity Debugger - Dser.exe - [Text strings referenced in Dser:.text]

File View Debug Plugins Immlib Options Window Help Jobs

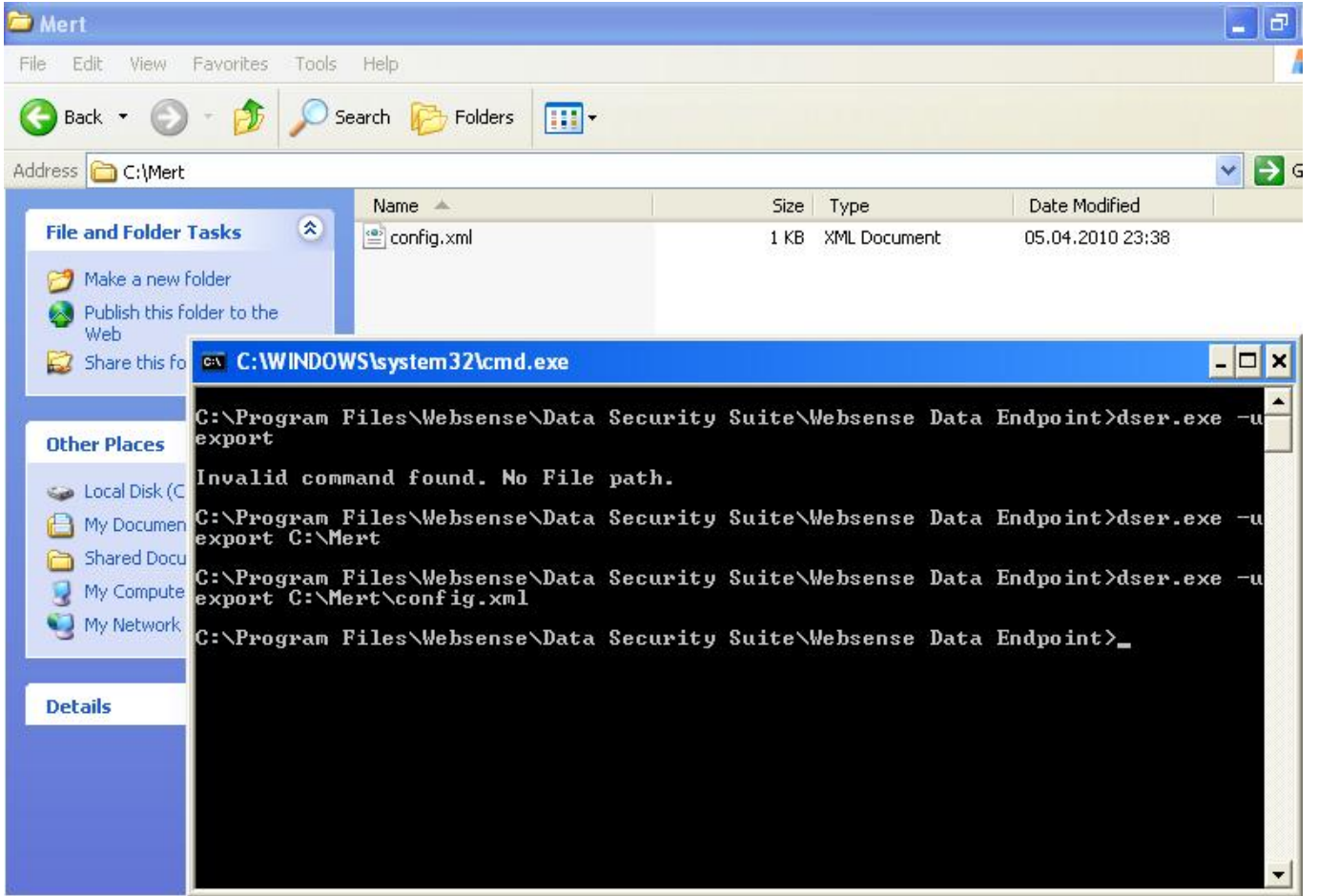
l e m t w h c P k b z r ... s ? Consulting Services Manager

Address	Disassembly	Text string
004028BC	MOV DWORD PTR SS:[ESP+24],Dser.00422FF0	UNICODE "Dser"
004028E1	PUSH Dser.00422FFC	ASCII "StartServiceCtrlDispatcher failed (%d)"
00402909	MOV ECX,Dser.00422870	UNICODE "-start"
00402969	MOV ECX,Dser.00422880	UNICODE "-import"
0040299F	MOV ECX,Dser.00422890	UNICODE "-clientmsg"
004029F3	MOV ECX,Dser.00422880	UNICODE "-import"
00402A41	PUSH Dser.00422934	UNICODE ":\\"
00402A90	PUSH Dser.00422A48	ASCII "Import profile return code: (%x)"
00402A9A	MOV ECX,Dser.00422890	UNICODE "-clientmsg"
00402AE2	PUSH Dser.00422934	UNICODE ":\\"
00402B28	PUSH Dser.00422B00	ASCII "Import client message file return code: (%x)"
00402B5C	PUSH Dser.00422C00	ASCII "Import command return code: (%x)"
00402B81	PUSH Dser.004228A8	ASCII "Please enter a file name including path."
00402B8F	PUSH Dser.004228D8	UNICODE "Dser: Parameter -import did not include path"
00402BB9	PUSH Dser.0042293C	ASCII "Please enter a xml file name including path."
00402BC1	PUSH Dser.00422970	UNICODE "Dser: Parameter -import did not include path of XML f"
00402BE5	PUSH Dser.004229E4	ASCII "Invalid command."
00402BF3	PUSH Dser.004229F8	UNICODE "Dser: Parameter -import invalid command"
00402C17	PUSH Dser.004228A8	ASCII "Please enter a file name including path."
00402C25	PUSH Dser.00422A70	UNICODE "Dser: Parameter -clientmsg did not include path"
00402C49	PUSH Dser.00422A00	ASCII "Please enter file name including path."
00402C57	PUSH Dser.00422B00	UNICODE "Dser: Parameter -clientmsg did not include path of XML"
00402C7B	PUSH Dser.004229E4	ASCII "Invalid command."
00402C89	PUSH Dser.00422B78	UNICODE "Dser: Parameter -clientmsg invalid command"
00402CD7	PUSH Dser.004226F0	UNICODE "SOFTWARE\\Websense\\Agent\\"
00402D04	PUSH Dser.00422C24	UNICODE "EhConfType"
00402D3D	PUSH Dser.00422C24	UNICODE "EhConfType"
00402DA3	MOV ECX,Dser.00422C3C	UNICODE "-password"
00402E46	PUSH Dser.00422C50	ASCII "Authentication failed. Please enter the command line w"
00402E54	PUSH Dser.00422CA0	UNICODE "Dser: Authentication failed."
00402E7D	MOV ECX,Dser.00422C0C	UNICODE "-i"
00402EBC	PUSH Dser.00422CE4	ASCII "Service Installed Success"
00402EC6	PUSH Dser.00422D04	ASCII "Error Installing Service"
00402E08	MOV ECX,Dser.00422D20	UNICODE "-u"
00402F14	PUSH Dser.00422D28	ASCII "Service UnInstalled Success"
00402F1E	PUSH Dser.00422D48	ASCII "Error Uninstalling Service"
00402F28	MOV ECX,Dser.00422D68	UNICODE "-export"
00402F66	PUSH Dser.00422D7C	ASCII "Invalid co"
00402F74	PUSH Dser.00422DA8	UNICODE "Dser: Parameter -export invalid command found"
00402FAF	MOV ECX,Dser.00422E04	UNICODE "-uimportconfig"
00402FF0	PUSH Dser.004228A8	ASCII "Please enter a file name including path."
00402FFE	PUSH Dser.00422E28	UNICODE "Dser: Parameter -uimportconfig did not include file pa"
00403022	PUSH Dser.00422934	UNICODE ":\\"
00403035	PUSH Dser.0042293C	ASCII "Please enter a xml file name including path."
00403043	PUSH Dser.00422EA0	UNICODE "Dser: Parameter -uimportconfig did not enter a XML fi"
004030A3	MOV ECX,Dser.00422F30	UNICODE "-stop"
004030ED	PUSH Dser.00422F3C	ASCII "Error: Stop Service (%d)"
00403112	MOV ECX,Dser.00422F58	UNICODE "-help"
00403155	PUSH Dser.00422F64	ASCII "USAGE:"

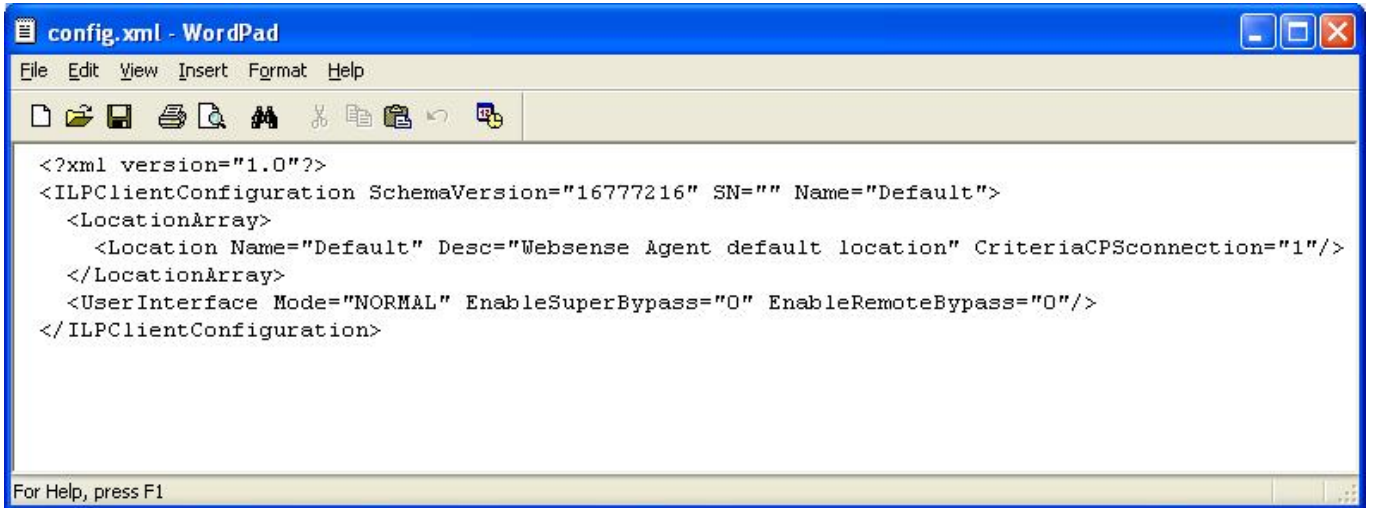
Analysing Dser: 216 heuristical procedures, 754 calls to known, 99 calls to guessed functions

Paused

Herhangi bir politika yüklü olmadan programları ve servisleri kapatmak mümkün oluyorsa servisi kaldırmak (uninstall) her türlü mümkün olur diye düşünerek - u parametresi yerine -uexport ve -uimportconfig parametrelerine göz atmaya karar verdim. Olsa olsa bu parametrelerden biri var olan konfigürasyon dosyasını export eder diğeri ise import eder varsayımından yola çıkarak dser.exe programını bu iki parametre ile çalıştırdım.



3 deneme sonrasında başarıyla yüklü olan konfigürasyonu export etmeyi başardım.

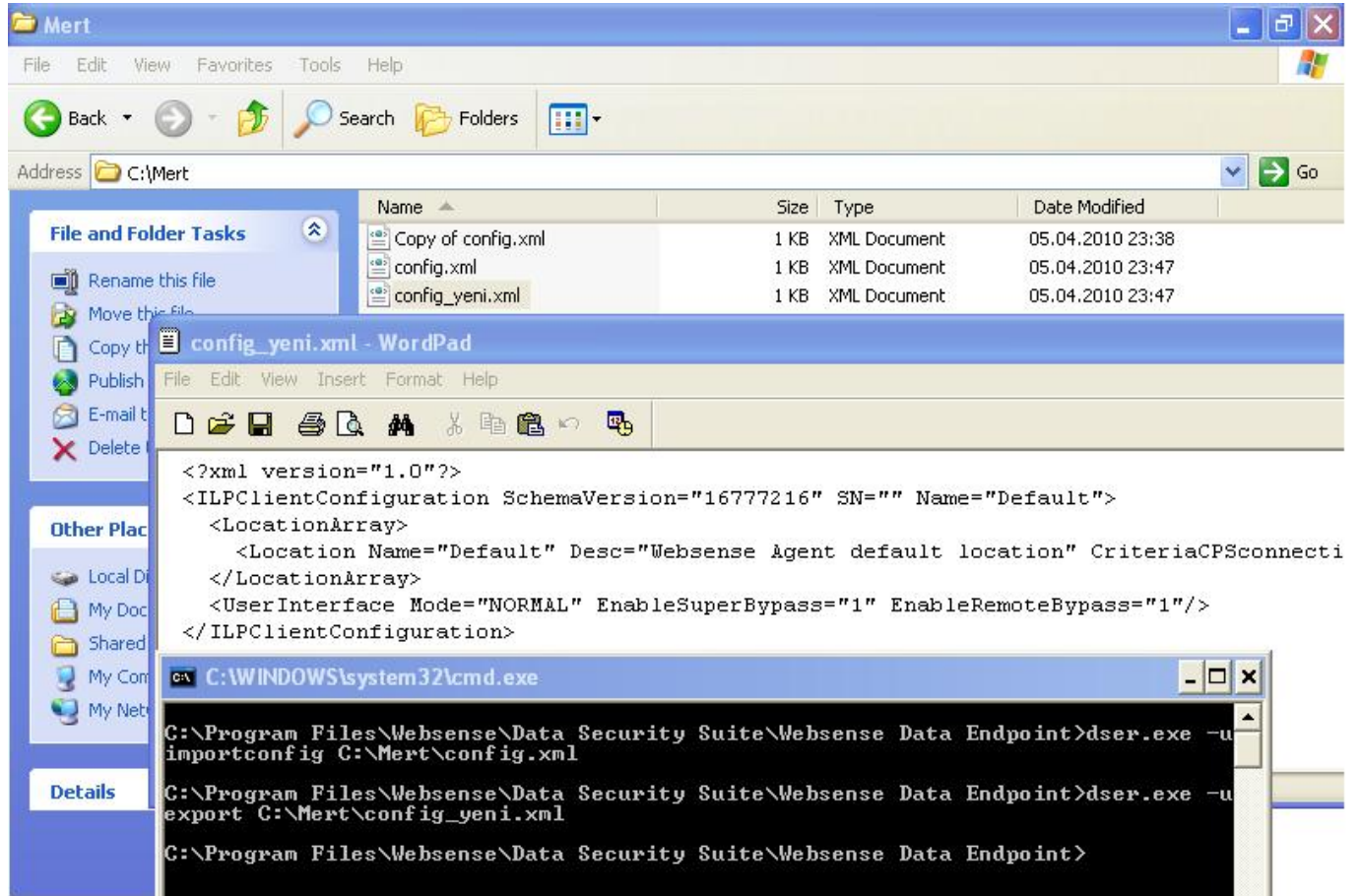


Evet aynen benimde sizin gibi satırını dikkatimi çekti. SuperBypass ve EnableRemoteBypass değerlerini 1 yaparsam ve bu konfigürasyonu programa geri yükleyebilirim programı GUI üzerinden kapatmak mümkün olabilir mi sorusuna yanıt aramaya karar verdim.

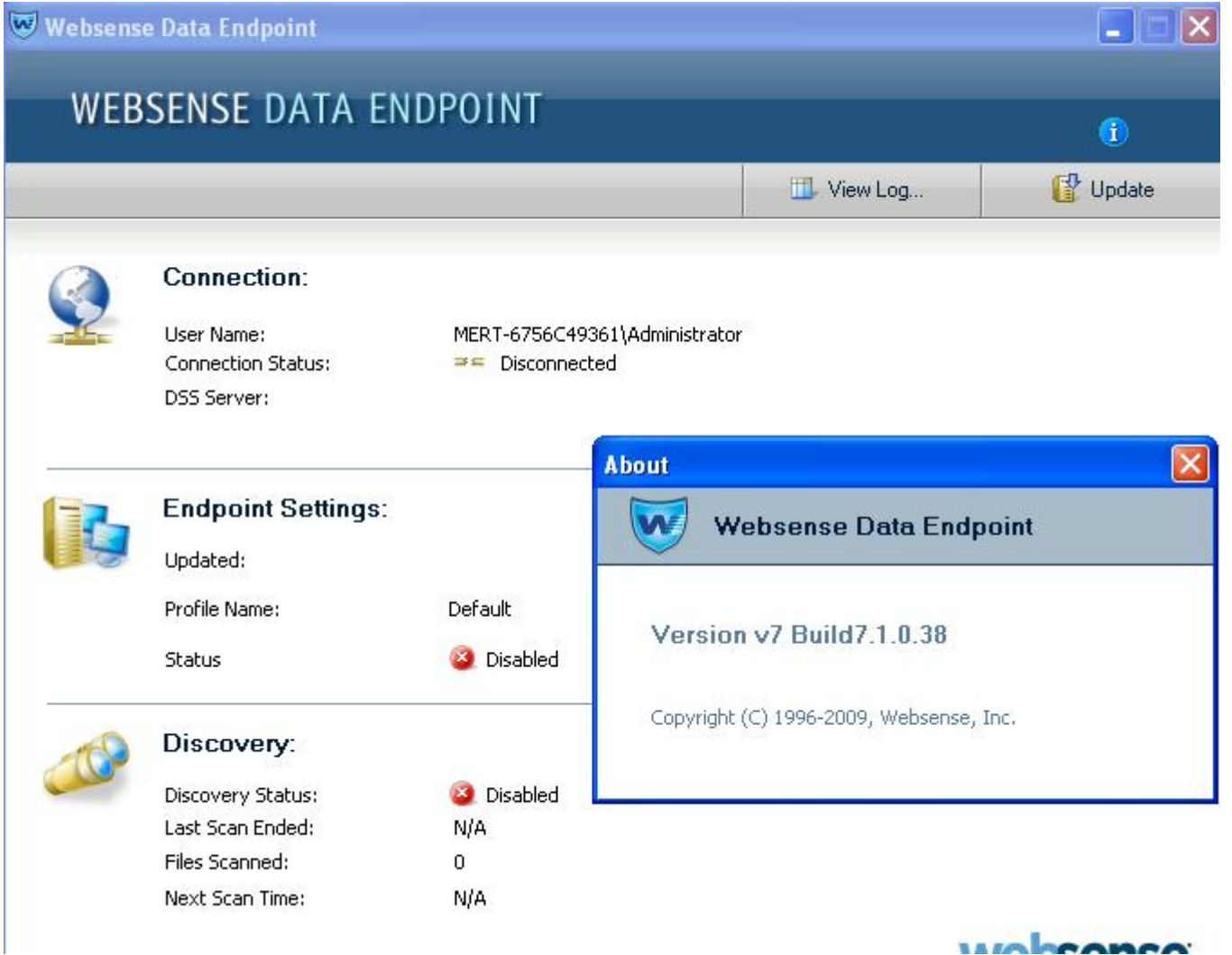
Değerleri değiştirip kayıt ettim ve programa geri yüklemek için şu komutu çalıştırdım:

```
dser.exe -uimportconfig C:\Mert\config.xml
```

Bu komutu çalıştırdıktan sonra işlemin başarıyla veya başarısız gerçekleştirildiğine dair herhangi bir yanıt almadım bu nedenle -uexport komutunu tekrar çalıştırarak güncel konfigürasyonu export ederek teyit etmeye karar verdim, sonuç konfigürasyonum başarıyla yüklenmişti.



Ancak GUI'ye baktığımda herhangi bir değişiklik ile karşılaşmadım.



Ajanda politika yüklü olsaydı farklı bir ekran ile karşılaşabilir miydik sorusunun cevabını üzerinde politika yüklü olan Websense Data Endpoint ajanı kullanan ve yönetici yetkisine sahip olan meraklı ziyaretçilerimize bırakıyorum. (Assembly kodundan anladığım kadarıyla şifre koruması var ise bu işlemi gerçekleştirebilmeniz için sizden doğru şifreyi girmeniz istenecek fakat bu adımda diğer ürünlerde olduğu gibi tersine mühendislik ile kolaylıkla bypass edilebilir gibi duruyor)

Sonuç olarak bu yazımızda, her ne kadar assembly seviyesinde hedef programa müdahalede bulunmamış olsakta tersine mühendislikten azda olsa faydalanarak programda, listelenen 3 komutun (parametre) dışında 5 komut (parametre) daha olduğunu tespit ettik ve bu komutlardan 1 tanesi ile uygulamanın güncel konfigürasyonunu export edebildik, diğeri ile ise dilediğimiz konfigürasyonu import edebildik.

Bir sonraki yazıda görüşmek dileğiyle herkese şimdiden iyi haftasonları dilerim.

Not: Üretici firma (veya dağıtıcı firma) yetkilileri dilediği taktirde

ziyaretçilerimizi konu ile ilgili aydınlatmak, hatalı veya eksik kısımları düzeltmek kısaca cevap hakkını kullanmak isterse seve seve yazımda yer verebilirim.