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.

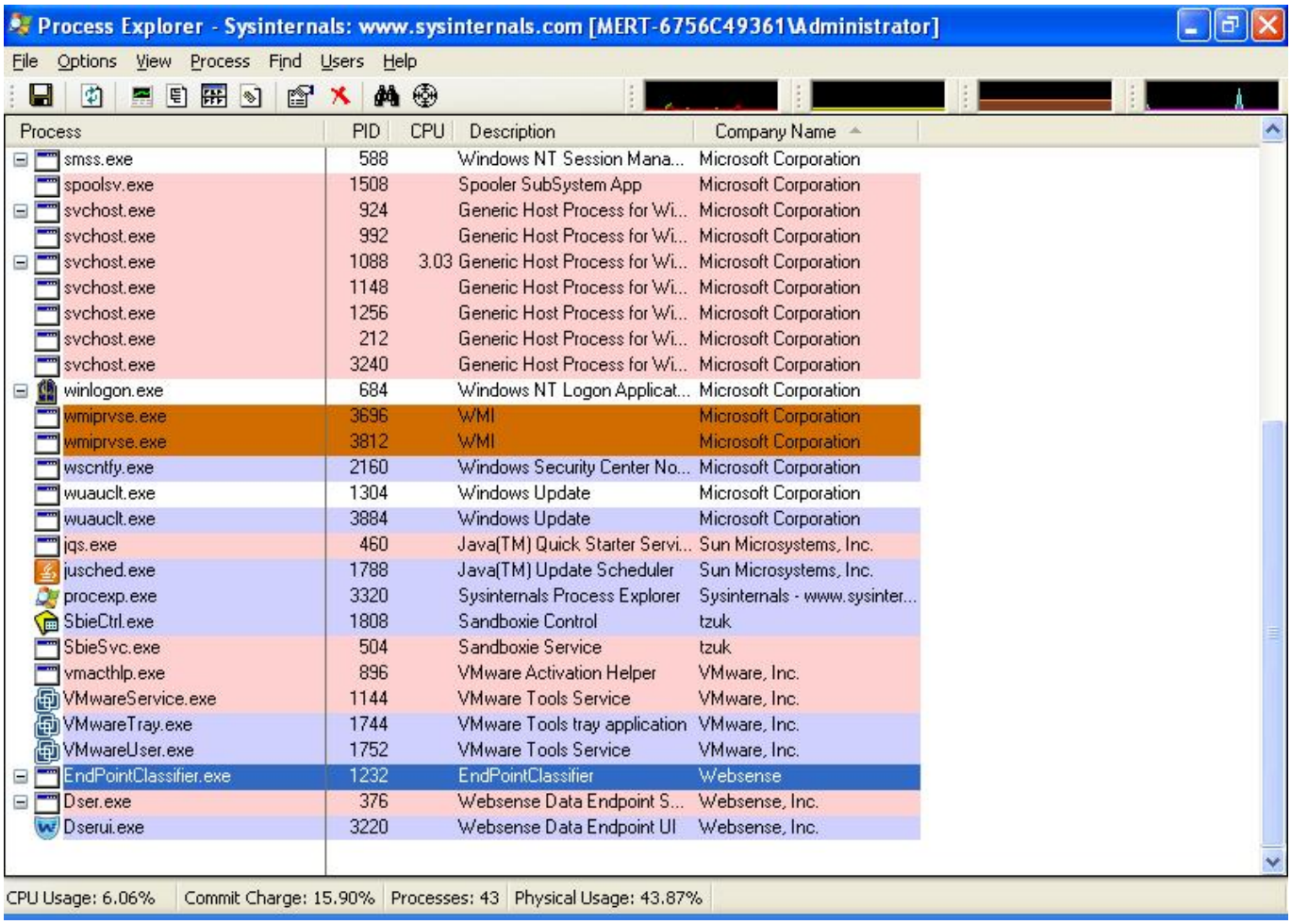
Günümüze gelecek olursak günümüz korsanları açık kaynak koda sahip olmayan yazılımlarda (Örneğin MS office uygulamaları) güvenlik açığı bulmak için tersine mühendislikten faydalanmaktadırlar. Hatta tersine mühendisliği otomatize ederek her ayın 2. haftasında Salı günü Microsoft firması tarafından yayınlanan 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.

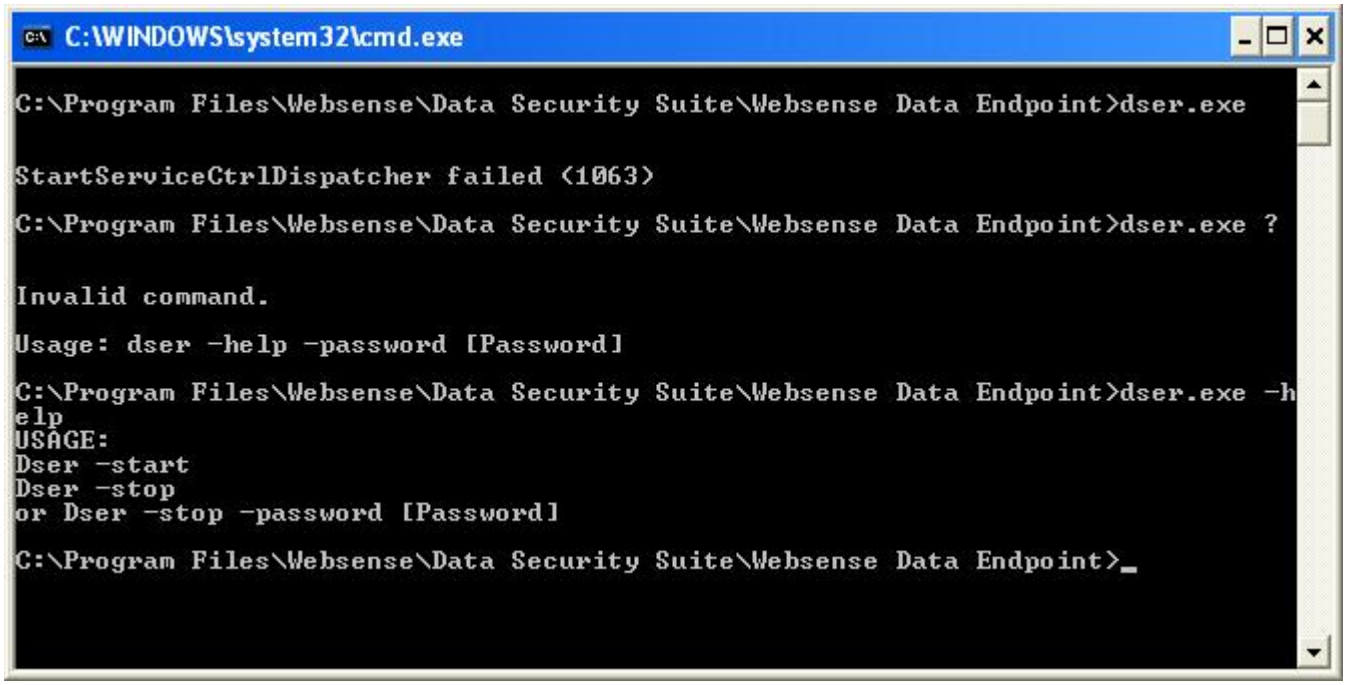
Ayrıca tersine mühendislik, programların içerisinde yer alan ancak dokümante edilmeyen gizli komutları/parametreleri ve özellikleri ortaya çıkarmak içinde kullanılmaktadır. Örneğin komut satırında programın desteklediği komutları listelediğinizde 2 komut olduğu gösterilirken, assembly debugger ile incelediğinizde 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.



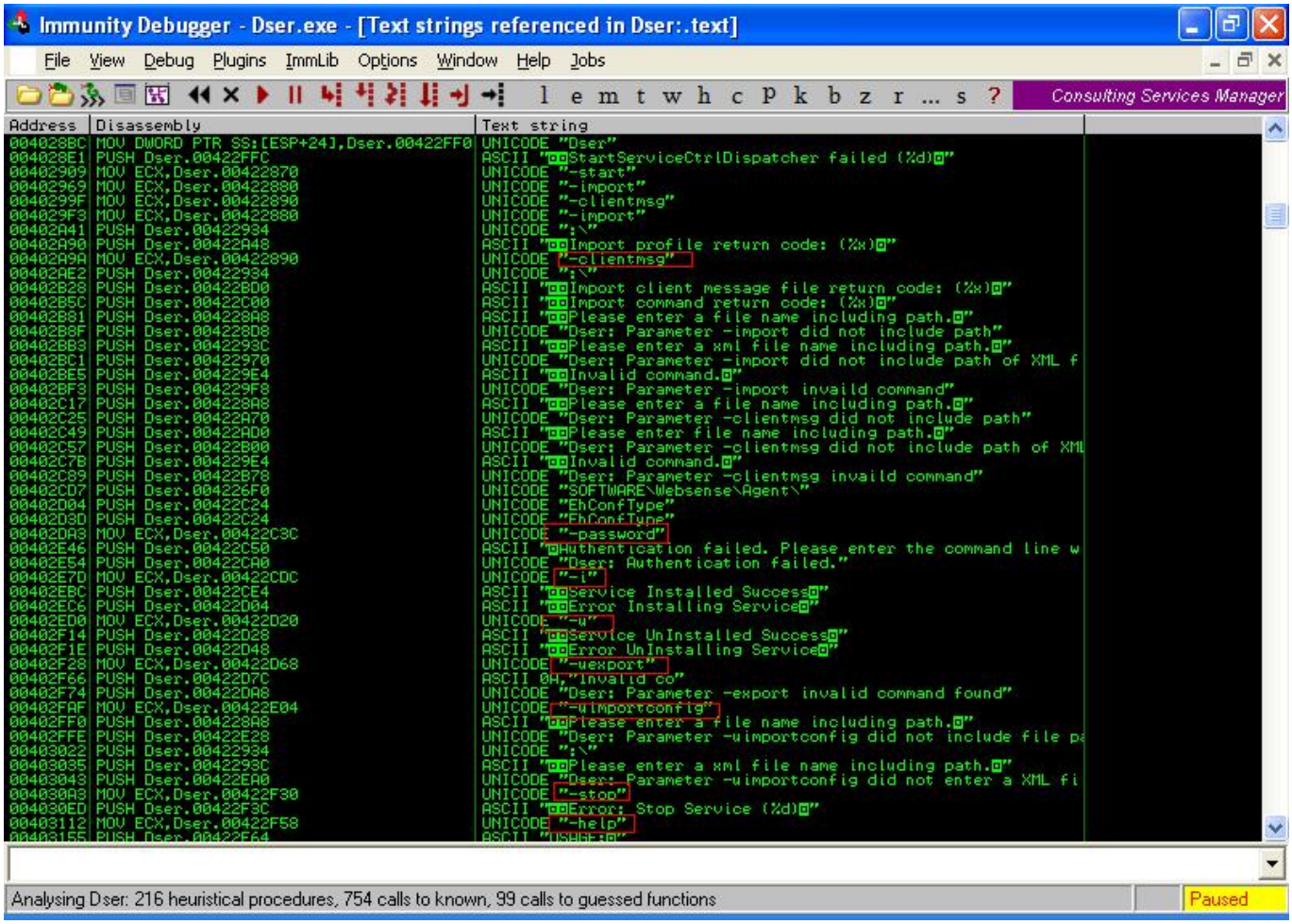
Process Explorer ile Dser.exe ve EndPointClassifier.exe programlarını kapattığımda otomatik olarak tekrar çalıştığını gördüm. Komut satırından

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

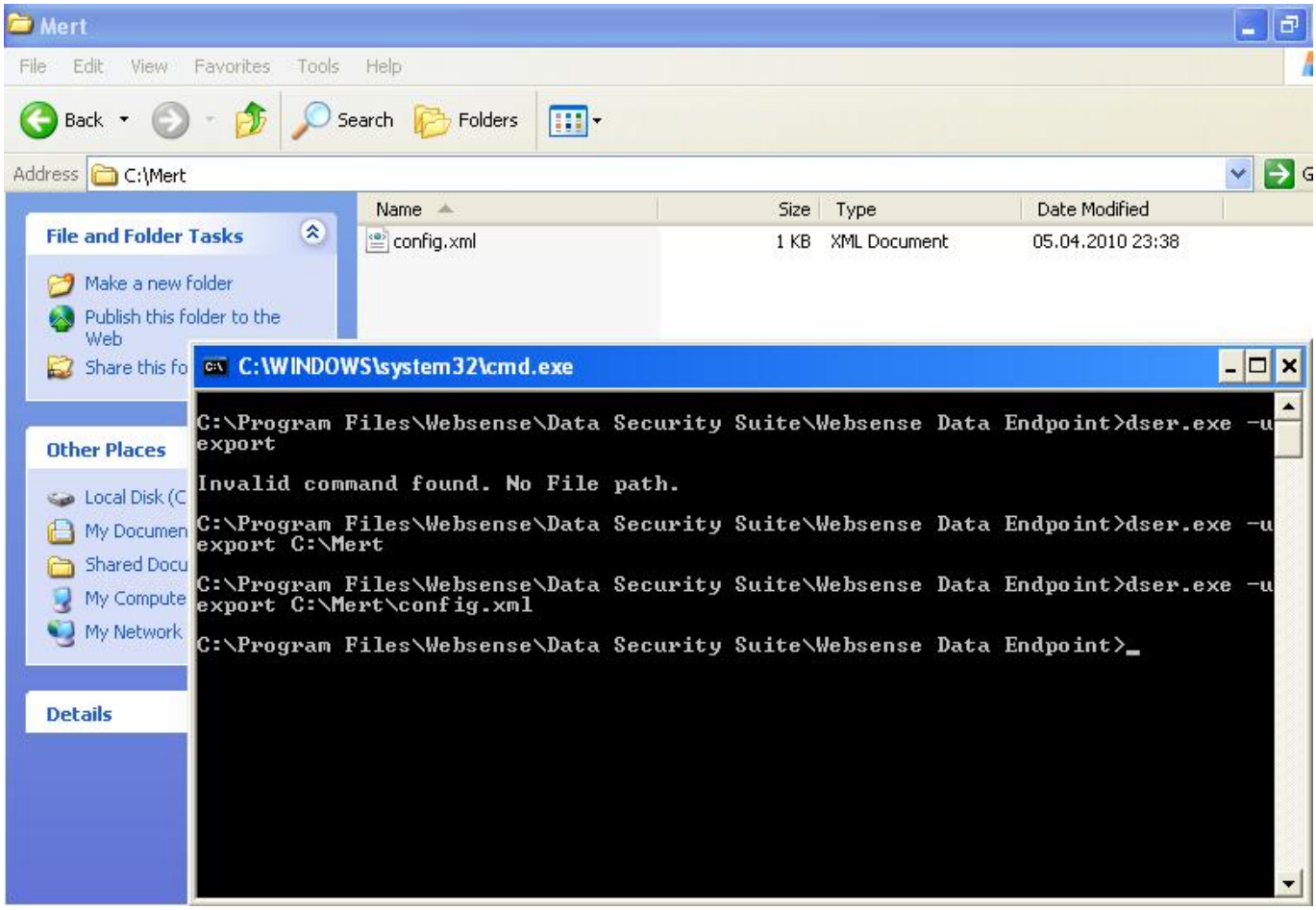


Sanıyorumki üzerinde herhangi bir politika yüklü olmadığı için dser.exe -stop yazarak çalışan servisi ve çalışan programları kapatabildim. Tahminimce politika bağlı olarak -password parametresi ve doğru şifre ile tüm programları ve servisleri kapatmak mümkün oluyor ancak dediğim gibi herhangi bir politika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

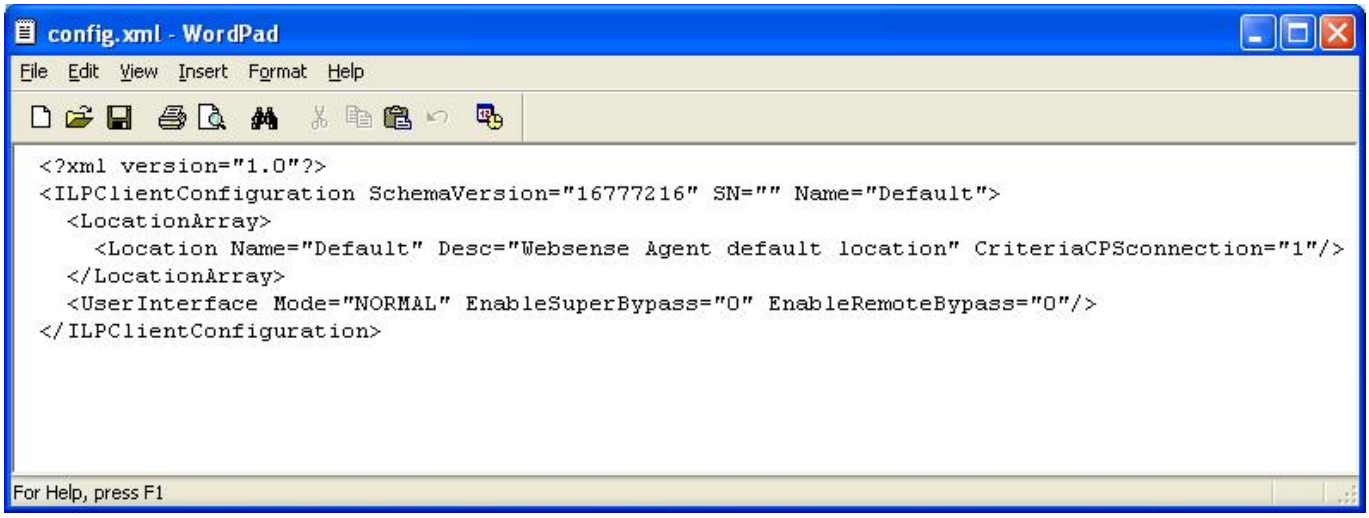
Immunity Debugger ile Dser.exe programına göz atıp program üzerinde yer alan metinleri listelediğimde listelenen komutların dışında 5 tane daha komut (parametre) olduğunu gördüm.



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.

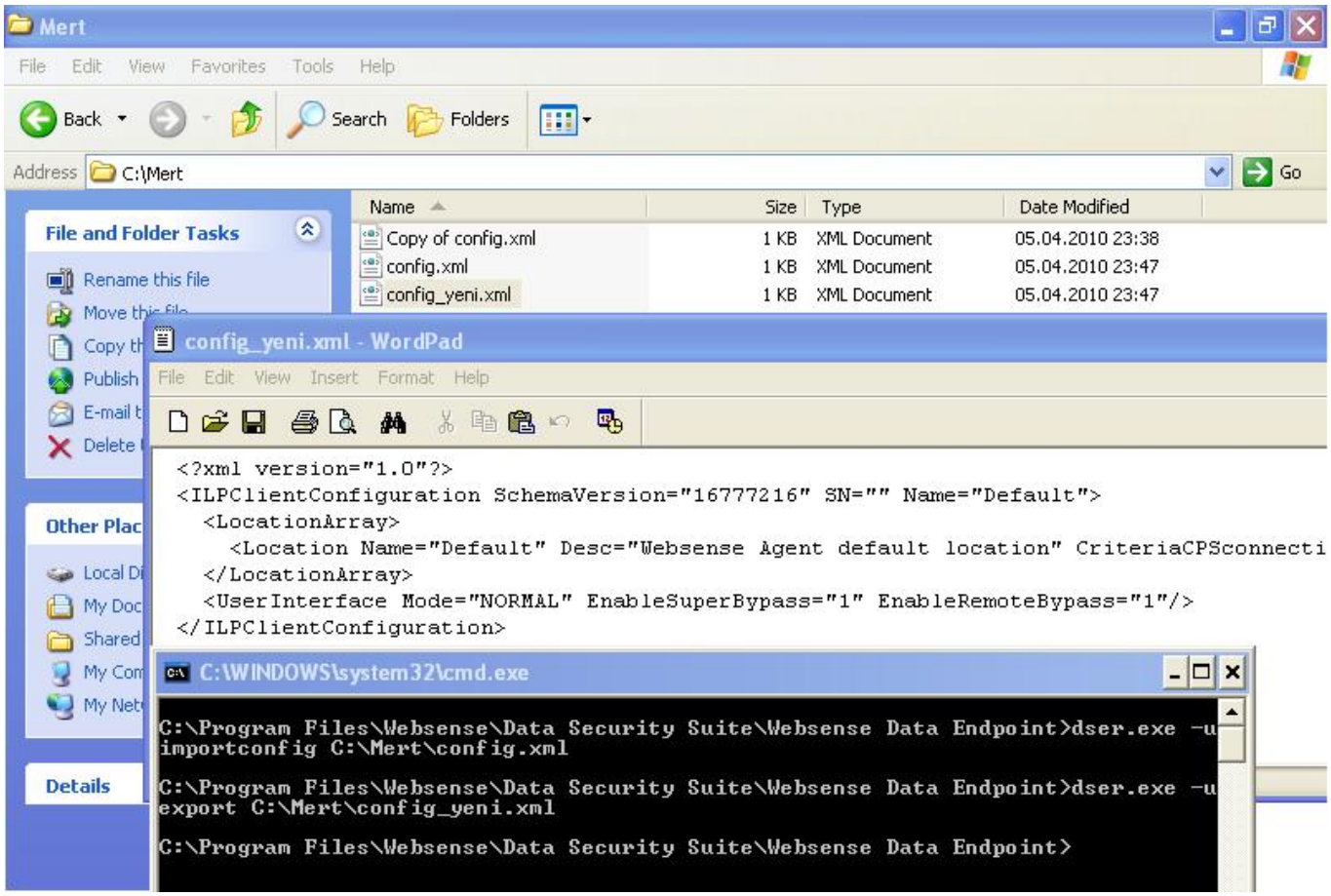


Evet aynen benimde sizin gibi satırı dikkatimi çekti. SuperBypass ve EnableRemoteBypass değerlerini 1 yaparsam ve bu konfigürasyonu programa geri yükleyebilirsem programı GUI üzerinden kapatmak mümkün olabilir mi sorusuna yanıt aramaya karar verdim.

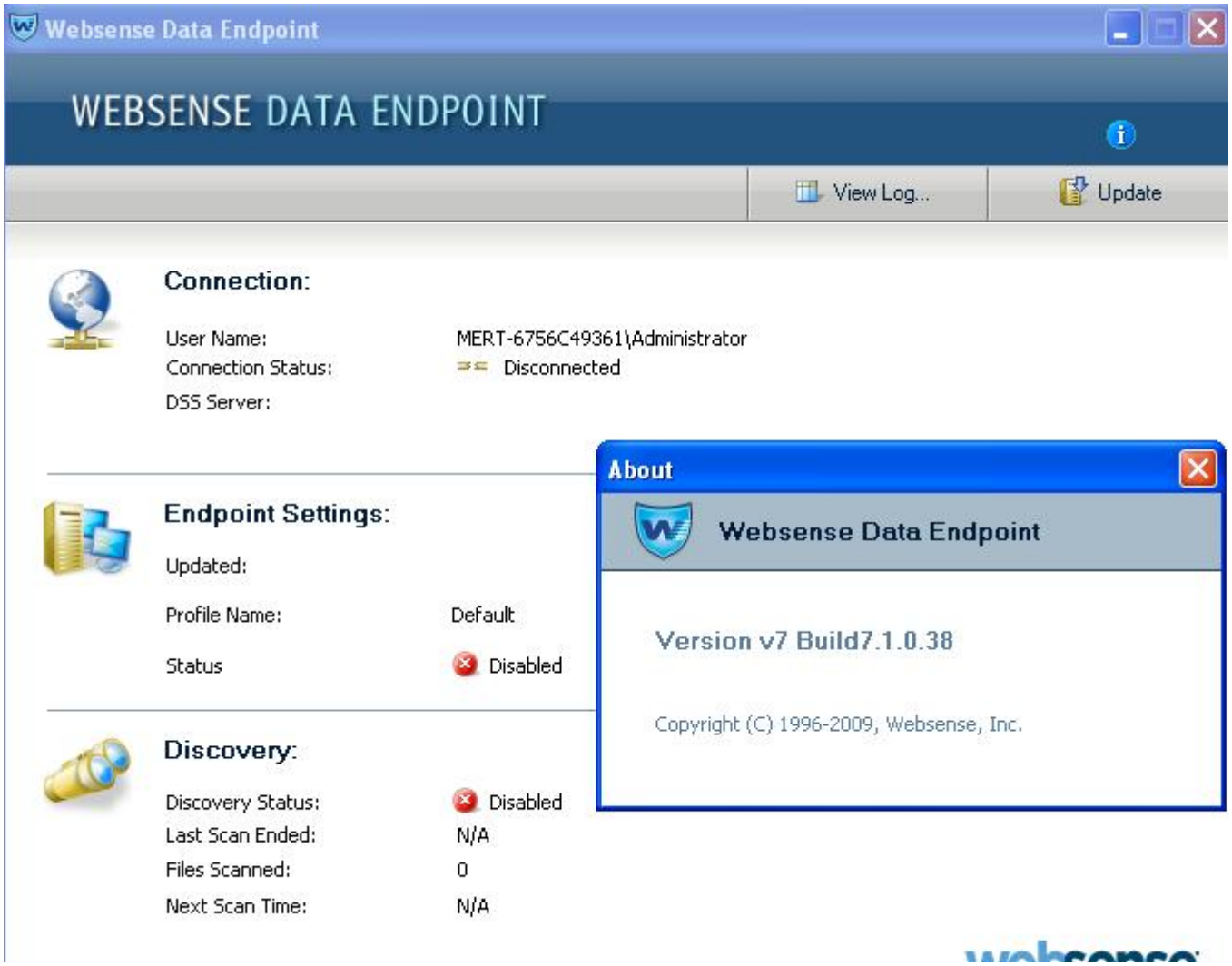
Değerleri değiştirip kayıt ettim ve programa geri yüklemek için şu komutu çalıştırdım:

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

Bu komutu çalıştırdıktan sonra işlemin başarıyla veya başarız 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 miydim 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.