Anti Meterpreter

written by Mert SARICA | 21 May 2010

Yaklaşık 4 gün önce Metasploit'in yeni sürümü, 3.4.0 yayınlandı. Sürüm notlarına baktığımızda Meterpreter ile ilgili bir çok değişiklik olduğunu görüyoruz. Meterpreter'ın hemen hemen her pentesterın eli, kolu olduğunu söyleyebilirim çünkü penetrasyon testlerinde (şayet core impact gibi bir aracı yoksa) hedef sistemi istismar ettikten sonra erişimini devam ettirebilmesi ve derinlemesine penetre edebilmesi için en çok ihtiyaç duyacağı yardımcı araçların başında gelir.

Bilmeyenleriniz için meterpreterdan kısaca bahsetmem gerekirse meterpreter, tamamen istismar edilen hedef processin içinde yani hafızada çalışabilen, hedef sistemin diski ile herhangi bir etkileşimde bulunmadığı içinde standart antivirüs yazılımları tarafından yakalanmayan, desteklediği modüller sayesinde hedef sistemdeki şifrelerin hashlerini toplamaktan, sniffer olarak çalışmaya, hedef sistemin ekranını kayıt etmekten, arka kapı olarak hizmet vermeye kadar bir çok özelliği üzerinde barındıran erişim sisteme erişim sağlayan yardımcı bir araç olarak düşünebilirsiniz.

Meterpreter ile ilgili bu zamana dek bir çok doküman, makale ve video hazırlandığı için bu yazımda meterpreter üzerine fazla birşey söylemeyeceğim. Meterpreter'ın nasıl çalıştığını, hangi yardımcı modüller ile geldiğini ve neler yapılabildiği ile ilgili olarak Irongeek sitesinde yer alan videoyu izlemenizi tavsiye ediyorum.

Yazımın asıl konusuna gelecek olursam, hafta içinde Türk Telekom'un istemcilere yüklettiği bir uygulamada bir güvenlik açığı keşfettim. Bu güvenlik açığını istismar eden art niyetli bir kişi, bu uygulama kullanıcısını kandırarak hazırlamış olduğu zararlı yazılımı bu kişiye göndererek çalıştırmasını sağlayabiliyor. Bu durumu simüle etmek için sanal makina üzerinde yer alan bir windows xp (kuzu) ile bir backtrack (kurt) arasında geçen ve zafiyetin nasıl istismar edilebileceğini konu alan ufak bir çalışma yaptım. Çalışma esnasında Backtrack üzerinde Metasploit ile meterpreter programını oluşturdum ve güvenlik zafiyetini istismar ederek windows xp'deki kullanıcıya gönderdim ve kullanıcının çalıştırmasını sağladım. Uygulama kullanıcısı meterpreter programını çalıştırdığı anda art niyetli kişinin sisteminde çalışan Metasploit'e bağlantı kuruyor ve art niyetli kişi artık uzaktan bu kullanıcının sisteminde kullanıcının yetkisi

ile yukarıda belirtmiş olduğum bir çok eylemi gerçekleştirebiliyor.

Penetrasyon testinde bir güvenlik zafiyeti keşfettiğinizde aklınızın bir köşesinde bu zafiyeti ortadan kaldıracak yollarıda düşünmeniz gerekiyor çünkü hazırlayacağınız raporda çözüm önerilerininde yer alması gerekiyor. Türk Telekom'un bu uygulaması için aklımda bir kaç çözüm yolu vardı henüz kendileri ile paylaşma fırsatım olmadı çünkü şu zamana kadar sadece kendilerine zafiyetin nerede olduğunu açıklayabildim.

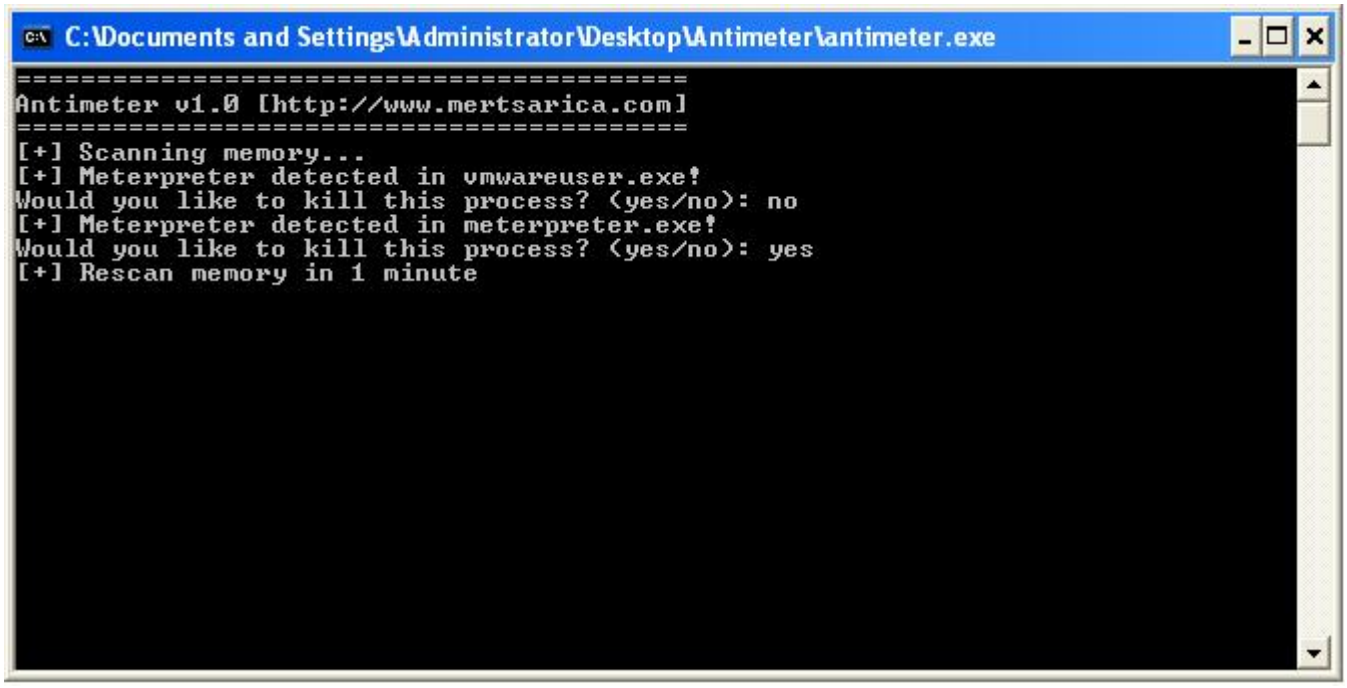
Diğer bir yandan meterpreter'ın bu kadar popüler olması ve bu ve benzer bir çok güvenlik zafiyetinde kullanılması nedeniyle meterpreterı tespit etmek için standart antivirüsler faydalı olmuyorsa nasıl bir çözüm olabilir diye düşünmeye başladım. Madem hafızada çalışıyor o zaman belli zaman aralıklarında hafızayı tarayan ve meterpreter'in izini süren ufak bir program hazırlasam işe yarar mı sorusuna yanıt aramaya karar verdim ve ortaya hemen hemen her yazıda olduğu gibi yine bir program çıkıverdi, Antimeter.

Antimeter programını zaman aralığı parametresi belirtmeden çalıştırmanız durumunda her 1 dakikada bir hafızayı taramakta ve meterpreter'a ait iz bulduğu taktirde sizi uyarmakta ve bu processi kapatmanıza imkan tanımaktadır. Zaman aralığı parametresi ile programı çalıştırmak için ise yapmanız gereken antimeter.exe <dakika cinsinden zaman aralığı>

Örnek kullanım: antimeter.exe 5

Programı yukarıdaki gibi çalıştırmanız durumunda antimeter her 5 dakikada bir hafızayı tarayacak ve meterpreter'a ait iz sürecektir.

Meterpreter'a ait iz bulması durumunda aşağıdaki gibi bir mesaj ve ses efekti ile sizi uyaracaktır.



Özellikle internet cafelerde, yurtlarda ve toplu internet kullanılan yani saldırıya açık olan mekanlarda bu uygulamanın kullanılması meterpreter korkusu olanlar için faydalı olabilir :) Bir sonraki yazıda görüşmek dileğiyle herkese iyi haftasonları dilerim.

Antimeter programına buradan ulaşabilirsiniz.