Microsoft Sysinternals AccessChk v.5.0

MUSTAFA SERHAT DÜNDAR, <SERHAT AT SERHATDUNDAR DOT COM>,
02/05/2010

Öncelikle Sysinternals nedir kısaca bahsedeyim.

Mark Russinovich ve Bryce Cogswell adında 2 yazılımcı 1996 yılından 2006 yılına kadar yani 10 sene boyunca Microsoft Windows için çeşitli ufak sistem yazılımları hazırladılar. Bu yazılımlar oldukça pratik ve kullanışlıydı ve birçok kişi tarafından beklenenin üzerinde sevildi. Tüm bu gelişmelerden sonra Microsoft 2006 yılında Sysinternals'i satın aldı.

Benim Sysinternals ile tanışmam ise sadece Windows üzerine geliştirilmiş, ufak, kurulum gerektirmeyen güvenlik pratiklerinde yardımcı programlar ararken oldu.

Kaldı ki benim sysinternals ile tanışmam seneler önceydi.. Bu grubun yazdığı yazılımlar ilgili 2 yazımda mevcut :

Folder and Registy Authorization

System Security And Microsoft Port Reporter

ACCESSCHK NEDİR?

AccessChk ufak bir sistem yazılımıdır. Sistem yöneticilerinin işini kolaylaştırmak için kodlanmıştır. Sistemde ki kullanıcıların veya kullanıcı gruplarının hangi dizinlere, kayıt anahtarlarına (regedit), global nesnelere ve Windows servislerine erişim hakları olduğunu görmelerini sağlar.

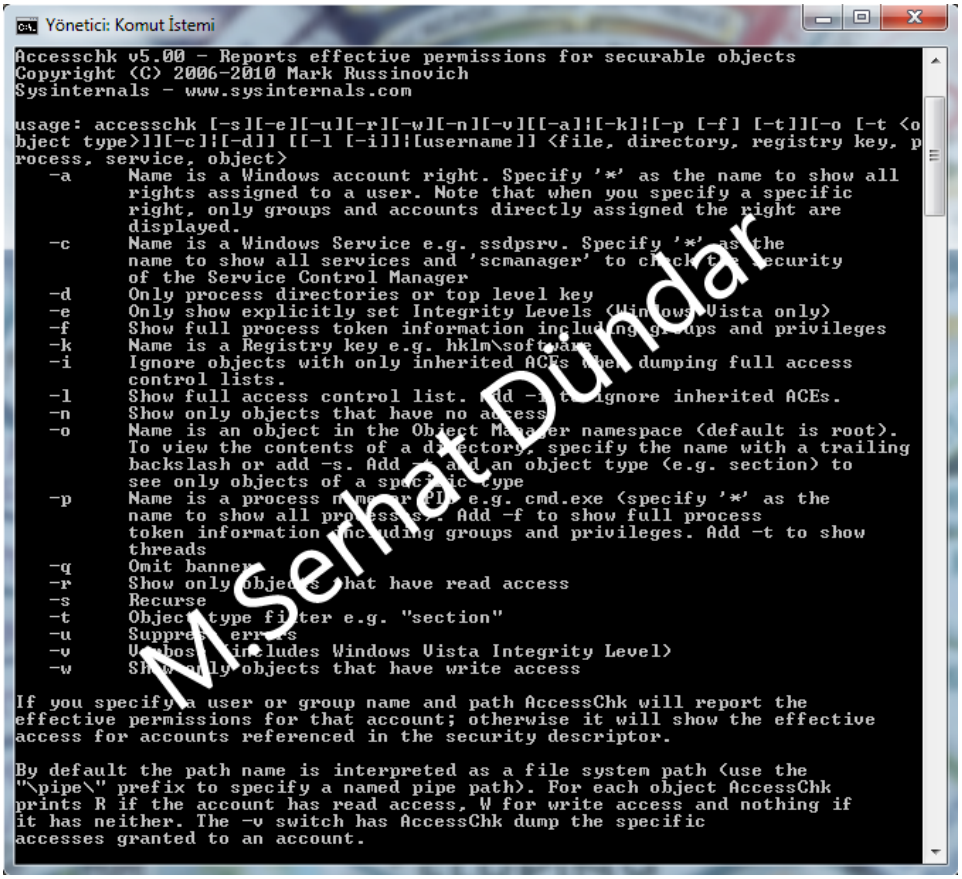
AccessChk 5.0 sürümünü bu adresten indirebilirsiniz.

AccessChk kurulumsuz, executable bir programdır. Kullanmak için .exe dosyalarını çalıştırdığınız dizine taşımanız yeterlidir.

Bilgisayar:/SistemBirimi:/Windows şeklinde dizine taşıyın.

Komut istemi'ni açıp, accesschk yazmanız programı çalıştırmak için yeterli.

Program çalıştığı zaman karşınıza aşağıda ki resimde gördüğünüz gibi program komutlarının listesi gelecek :



KULLANIMI

accesschk [-s][-e][-u][-r][-w][-n][-v][[-a]|[-k]|[-p [-f] [-t]][-o [-t <object type>]][-c]|[-d]] [[-l [-i]]|[username]] <file, directory, registry key, process, service, object>

-a	Bir Windows hesap yetkisi ismini belirtir. * karakterini bütün kullanıcı hesap yetkilerini kapsamasını istediğiniz zaman kullanın. Bir yetki ismi girdiğinizde sadece bu yetkiye sahip kullanıcı veya kullanıcı gruplarının listeleneceğini unutmayın.
-c	SSdpsrv gibi herhangi bir Windows servisinin ismini belirtir. Yıldız (*) karakterini kullanarak tüm servis isimlerini belirtebilir ve servis yöneticisinin de (scmanager) güvenlik yetkilerini sınayabilirsiniz.
-d	Sadece işlem birimlerini veya üst düzey anahtarları belirtir.
-e	Sadece net bir şekilde set-Integrity seviyelerini gösterir. (Sadece Windows Vista'da geçerli)
-f	Kullanıcı grupları ve ayrıcalıklı gruplarırdan bilgi alan tüm işlermleri gösterir.
-i	Tüm erişim kontrollerinin listesi ekrana dökülürken, ACE'den miras alınan nesnelerin gösterilmesini engeller.
-k	Bir kayıt defteri satırının ismini belirtir. hklm\software
-l	Tüm erişim kontrol listesini gösterir. -i ile ACE'den miras alınanların gösterilmesini engelleyebilirsiniz.
-n	Sadece erişimin engelli olduğu nesneleri gösterir.
-o	Nesne Yöneticisi isim uzayındaki ana dizin ismidir.

	(Default olarak root). -t ve -s kullanılabilir.
-p	İşlem veya PID ismidir. cmd.exe gibi. Yıldız (*) karakteri ile tüm işlemleri kapsatabilirsiniz. -f ve -t kullanabilirsiniz. Bunlarında açıklamaları mevcut zaten.
-q	Sembolleri görmezden gelir.
-r	Sadece okuma iznine sahip dosyaları gösterir.
-s	Recurse
-t	Nesne tipi filtresidir.
-u	Hataları engeller.
-v	Verbose
-w	Sadece yazma izni olunan nesneleri gösterir.

ÖRNEKLER

Aşağıda ki komut ile Windows\System32 içerisinde ki sistem dosyalarından hangilerine power userların erişebileceğini listeler.

accesschk "power users" c:\windows\system32

Bu komut ile hangi Windows servislerinin kullanıcı grup üyelerinde yazma izni olduğunu görebilirsiniz.

accesschk users -cw *

HKLM\CurrentUser altında ki hangi kayıt defteri anahtarlarının, belirtilen kullanıcıya göre erişim izni olmadığını gösterir.

accesschk -kns msdundar\mruss hklm\software

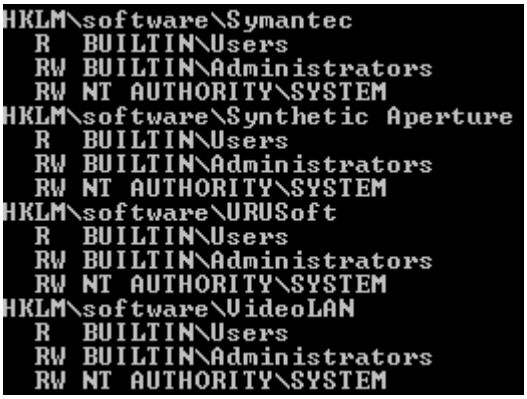
HKLM\Software anahtarının güvenlik yapılandırmasını gösterir.

accesschk -k hklm\software

Herkesin değiştirebileceği global yani evrensel nesneleri gösterir.

accesschk -wuo everyone \basednamedobjects

Örnek olarak HKLM\Software anahtarının güvenlik yapılandırmasının bir kısmına bakalım :



HKLM\software\Symantec anahtarına ;

Users grubu R iznine yani READ (okuma) izniyle sahip,

Administrators grubu RW iznine yani Rewrite (yazma) izniyle sahip.

Default sistem kullanıcısı doğal olarak RW izniyle sahip.

Çeşitli örnekler ve denemeler ile keşfedilmesi kolay bir yazılım.

M.SERHAT DÜNDAR