

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 Registry 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 :



```
Accesschk v5.00 - Reports effective permissions for securable objects
Copyright (C) 2006-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

usage: 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 Name is a Windows account right. Specify '*' as the name to show all rights assigned to a user. Note that when you specify a specific right, only groups and accounts directly assigned the right are displayed.
-c Name is a Windows Service e.g. ssdpsrv. Specify '*' as the name to show all services and 'scmanager' to check the security of the Service Control Manager
-d Only process directories or top level key
-e Only show explicitly set Integrity Levels (Windows Vista only)
-f Show full process token information including groups and privileges
-k Name is a Registry key e.g. hklm\software
-i Ignore objects with only inherited ACEs (use -d to dump full access control lists)
-l Show full access control list. Add -i to ignore inherited ACEs.
-n Show only objects that have no access
-o Name is an object in the Object Manager namespace (default is root). To view the contents of a directory, specify the name with a trailing backslash or add -s. Add -t to add an object type (e.g. section) to see only objects of a specific type
-p Name is a process name or PID e.g. cmd.exe (specify '*' as the name to show all processes). Add -f to show full process token information including groups and privileges. Add -t to show threads
-q Omit banner
-r Show only objects that have read access
-s Recurse
-t Object type filter e.g. "section"
-u Suppress errors
-v Windows includes Windows Vista Integrity Level)
-w Show only objects that have write access

If you specify a user or group name and path AccessChk will report the effective permissions for that account; otherwise it will show the effective access for accounts referenced in the security descriptor.

By default the path name is interpreted as a file system path (use the "\pipe\" prefix to specify a named pipe path). For each object AccessChk prints R if the account has read access, W for write access and nothing if it has neither. The -v switch has AccessChk dump the specific accesses granted to an account.
```

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 sınavabilirsiniz.
- 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 gruplarından bilgi alan tüm işlemleri 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 izin 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
R BUILTIN\Users
RW BUILTIN\Administrators
RW NT AUTHORITY\SYSTEM
HKLM\software\Synthetic Aperture
R BUILTIN\Users
RW BUILTIN\Administrators
RW NT AUTHORITY\SYSTEM
HKLM\software\URUSoft
R BUILTIN\Users
RW BUILTIN\Administrators
RW NT AUTHORITY\SYSTEM
HKLM\software\VideoLAN
R BUILTIN\Users
RW BUILTIN\Administrators
RW NT AUTHORITY\SYSTEM
```

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