TÜBİTAK

Windows Güvenliği Eğitimi

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

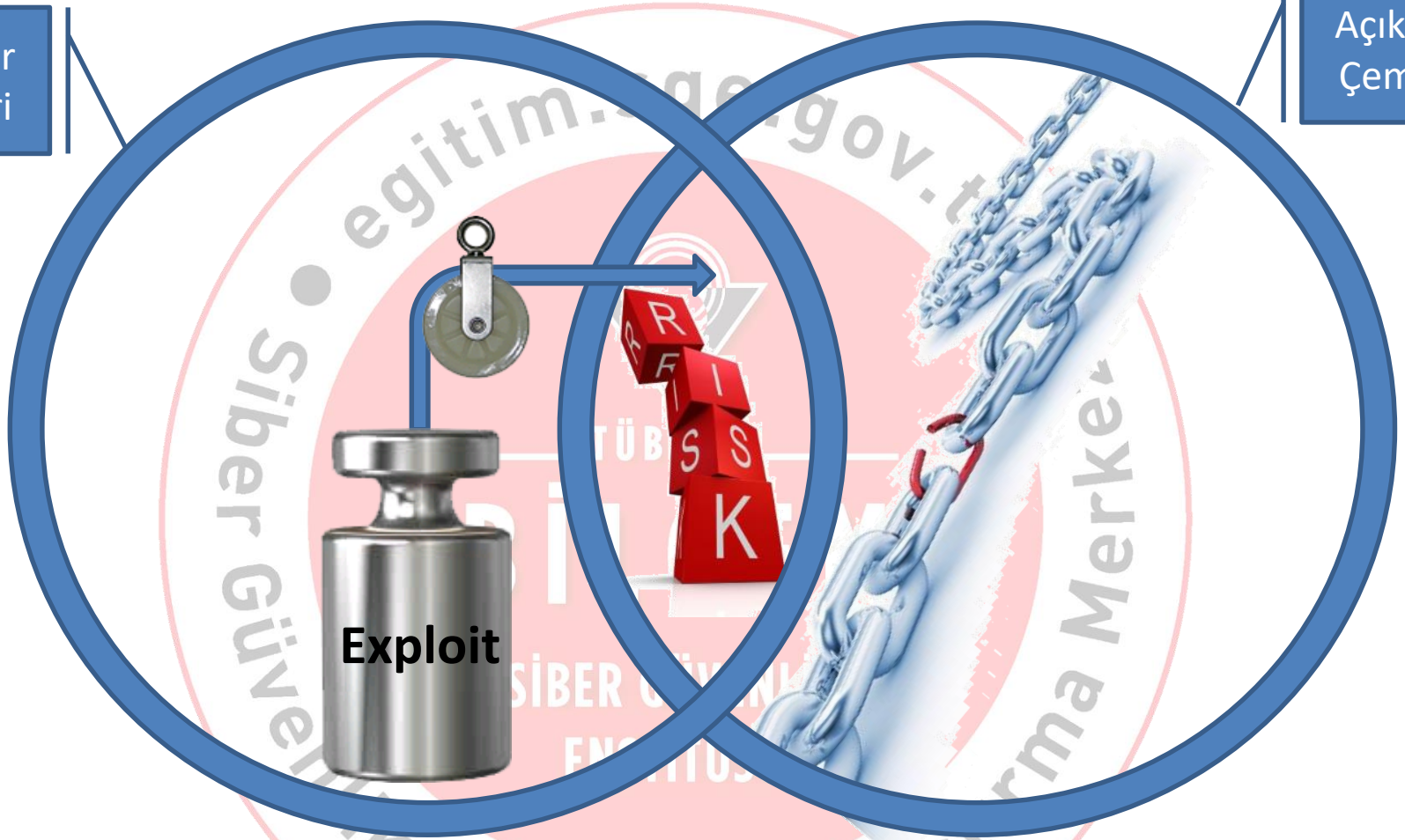
Eğitimin Genel İçeriği

- Temel Prensipler
- Temel Güvenlik Önlemleri
- Windows'ta Güvenlik Bileşenleri
- Kimlik Doğrulama
- Erişim Kontrolü
- Yedekleme
- Güncelleme
- Korunma Teknolojileri
- Güvenlik Denetimi ve Sıkılaştırma
- Faydalı Araçlar

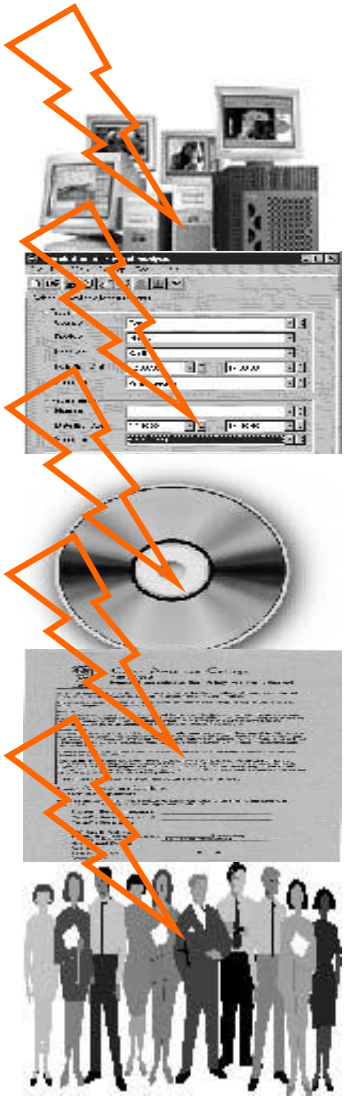
TÜBİTAK

Temel Prensipler

Açıklık, Tehdit, Sömürme ve Risk



Tehdit Örnekleri



- Donanımın bulunduğu ortamdaki toz, nem, güneş ışığı.
- Yazılımdaki açıklıkları kullanan bilgisayar korsanları.
- Verinin bulunduğu medyanın çalınması.
- Politikaların açık noktaların kullanılarak kötüye kullanılması.
- Bilgisayar virüsleri.

Çeşitli Bilgi Güvenliği Riskleri

Tehdit	Bilgi Varlığı / Açıklık	Risk
Servis dışı bırakma saldırıları	Kurumun WEB Sitesi	WEB sitesinin servis veremez duruma düşmesi - maddi kayıp
İnsani zayıflıklar	USB belleklere ilişkin politika ve eğitim eksiği / taşıma kolaylığı	Belleklerin kurum dışında kaybolması - kurumsal bilginin açığa çıkması
Sistem odası sıcaklığında ve nem düzeyinde dalgalanmalar	Sunucu sabit diskleri / sınırlı dayanıklılık	Sabit disk arızası - kurumsal bilginin kaybedilmesi
Sistem yöneticilerinin iş yoğunluğu / prosedürsüz çalışması	Güvenlik duvarı kural listesi	Personel hatası - sunucuların Internet'ten saldırıya açık hala gelmesi.

Pareto Prensibi

Alınabilecek önlemlerin %20'sinin alınması karşılaşılabilecek saldırıların %80'inden korunma sağlar.

Temel Güvenlik Önlemleri

Temel Güvenlik Önlemleri

- **Fiziksel Güvenlik Önlemleri**
- **Güncellemeler**
- **Yetkilendirme**
- **Yedekleme**
- **Denetleme ve İzleme**
- **Sıkılaştırma**
- **….**

Fiziksel Güvenlik

- **Kilitli Sistem Odası, Kilitli Sunucu Dolapları**
  - Anahtarlar kimde?
  - Kameralarla izleniyor mu?
  - Sunuculara cd veya usb bellek doğrudan takılabiliyor mu?
- **Kayıtları izleyen var mı?**
  - Kameralar nereyi izliyor?
- **Akıllı Kart, Manyetik Kart ve Biyometrik Sistemler**
  - Erişimi olanların listesi?
  - Kimden izin alınıyor?
  - Kayıtları inceleyen var mı?

Fiziksel Güvenlik

- **Sistem Yedekleri**
  - Güvenli bir yerde mi saklanıyor?
  - Aldığınız yedekler kullanılabilir durumda mı?
- **Hata Toleransı**
  - Oluşabilecek hatalara karşı diskler uygun şekilde yapılandırılmış mı?
  - Sunucular yedekli çalışacak şekilde yapılandırılmış mı?
  - Yangın, sel, deprem vb. durumlar düşünüldü mü?

Fiziksel Güvenlik

- **Fiziksel güvenlik önlemi alınmayan ortamlarda**
  - Yönetici şifresinin değiştirilmesi
  - Yönetici şifrelerinin çalınması
  - Önemli işletim sistemleri dosyalarının değiştirilmesi
  - Kritik bilgileri çalınması
  - Servis dışı bırakma
  - SID sahteciliği (SID Spoofing)
  - vb...

Uygulama – 'Ease of Access' Özelliği ile Bilgisayarın Ele Geçirilmesi

- Uygulama 1 dosyasını indiriniz.

Fiziksel güvenlik önlemleri alınmayan ortamlarda sisteme verilebilecek zararlardan birine örnek gösterilecektir.

Lütfen uygulamayı tamamlayınız!

TÜBİTAK

Windows'ta Güvenlik Bileşenleri

Windows İşletim Sistemi Ailesi

- **Biraz tarihçe…**
- **Mobil**
  - Windows Mobile 2002, 2003, 5.0, 6.5 → Phone 7, 8
- **İstemci**
  - Windows XP, Vista, 7, 8
- **Sunucu**
  - Windows Server 2000, 2003, 2008, 2012

Windows İstemci Sürümleri

- Windows XP
  - Home Edition
  - Professional
- Windows Vista & 7
  - Starter
  - Home Basic
  - Home Premium
  - Business
  - Enterprise
  - Ultimate
- Windows 8
  - RT
  - 8
  - 8 Pro
  - Enterprise
- Windows 10
  - Home
  - Pro
  - Education
  - Enterprise

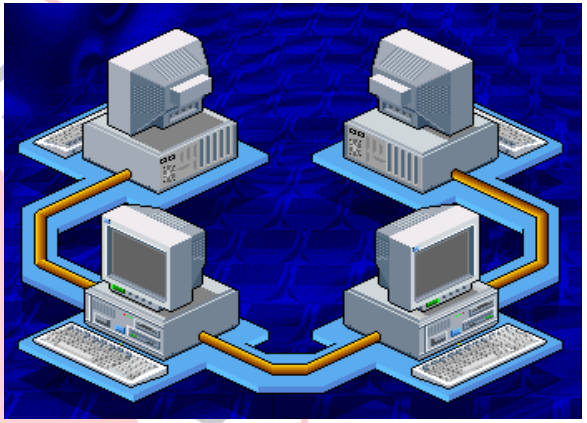
Windows Sunucu Sürümleri

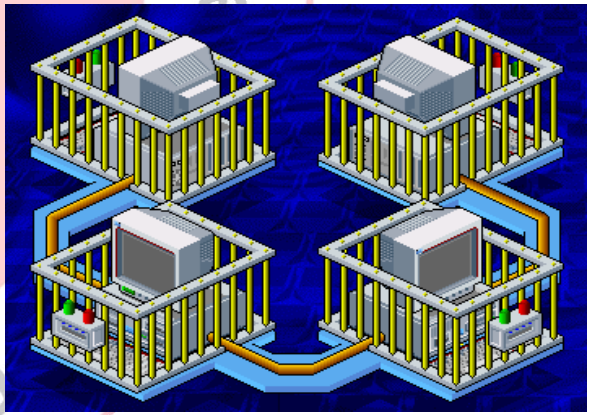
- Server 2003
  - Web
  - Standart
  - Enterprise
  - Datacenter
- Windows 2008 & R2
  - Foundation
  - Standart
  - Web
  - HPC
  - Enterprise
  - Datacenter
  - Itanium
- Windows 2012 & R2
  - Foundation
  - Essentials
  - Standart
  - Datacenter
- Windows 2016
  - Datacenter
  - Standart
  - Essentials
  - MultiPoint Premium Server
  - Storage Server
  - Hyper-V

Minimum Önerilen

Çalışma Grupları (Workgroups)

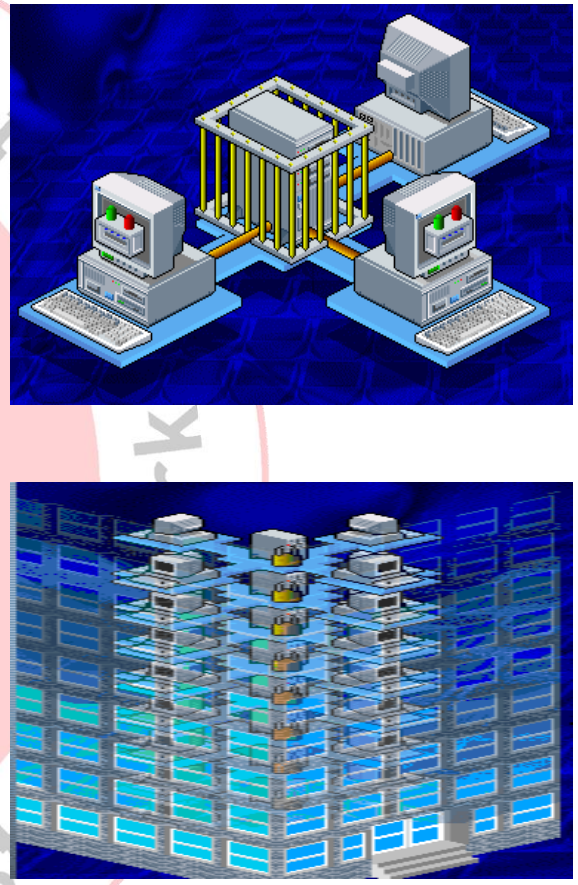
- Ağda komşu bilgisayarların bir ağ cihazı ile bağlanmasıyla oluşan yapıdır.
- Bilgisayara bir çalışma grubu ismi vererek bağlanılabilir.
- Kaynak paylaşımı vardır.
- Güvenlik fonksiyonları bulunmaz.
- Merkezi kontrol birimleri yoktur, yönetilemezler.





Etki Alanı (Domain)

- Merkezi yönetim ve merkezi güvenlik politikaları
- Microsoft, verimli kurum ağlarının oluşturulması için geliştirmiştir
- Kurum ağındaki nesnelerin (bilgisayar, kullanıcı, grup, yönetici, yazıcı …) bilgilerini tutan ortak bir veritabanıdır.



Kullanıcılar & Bilgisayarlar

- **İki tür kullanıcı**
  - Yerel Kullanıcı
    - SAM
  - Etki Alanı Kullanıcısı
    - NTDS.dit
- **Nasıl yönetilir**
  - Başlangıç > Yönetimsel Araçlar > Bilgisayar Yönetimi
  - Kontrol Paneli > Kullanıcı Hesapları
  - Komut istemi: net user
- Bilgisayar da bir kullanıcı türüdür.

Gruplar

- **Grup üyelikleri**
- **Erişim kontrolünün kolaylaştırılması**
  - **Scope:**
    - Domain Local
    - Global
    - Universal
  - **Type:**
    - Security
    - Distribution

Security Identifier (SID)

- **TC Kimlik No**
- S-1-5-21-4353520176-2898672217-036752055-1000
- **Her bir varlığa özeldir**
  - Kullanıcı
  - Grup
  - Bilgisayar
  - Servis
- **Bir kaynağa izin atanabilmesi esnasında göz önünde bulundurulur.**

Kullanıcı Hakları ve Ayrıcalıkları

- **Her bilgisayara özeldir.**
- **İki farklı kategori:**
  - Oturum Açma Hakları
  - Ayrıcalıklar
- **Security Access Token (SAT) içerisinde bulunurlar.**
- **Grup Politika İlkeleri ile yönetilebilirler.**

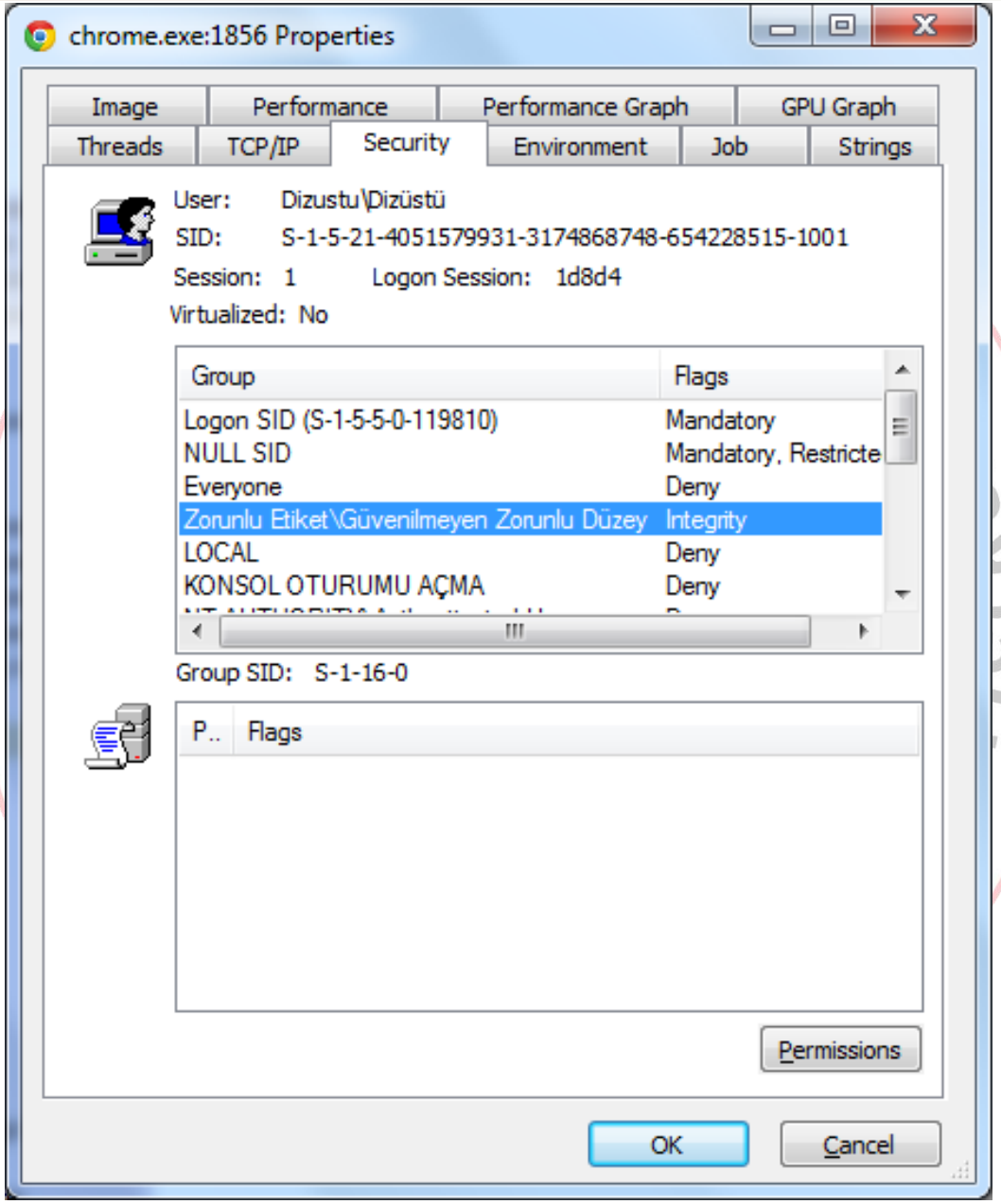
Security Access Token (SAT)

- **Ehliyet'e benzetilebilir.**
- **Bir bilgisayarda oturum açıldığında üretilir.**
- **Çalışan her prosese eklenir.**
- **İçerisinde:**
  - Kullanıcı SID değeri
  - Üye olunan gruplara ait SID değerleri
  - Kullanıcı ayrıcalıkları

Zorunlu Bütünlük Kontrolü (MIC)

- **Biba (Kenneth J. Biba) bütünlük kontrol modeli**
- **Bütünlük kontrolü *etiketler* ile sağlanır**
- **Windows'ta bütünlük Etiketi Seviyeleri:**
  - Mandatory Integrity Control - MIC (Vista+)
  - Biba kısmi gerçekleme, okuma var fakat yazma yok
  - Low, Medium, High ve System
- **NTFS izinlerinden önce ve bağımsız**
- **Okumaya ve çalıştırmaya engel olmaz**

Zorunlu Bütünlük Kontrolü (MIC)



Kullanıcı Hesap Denetimi (UAC)

- **İki farklı etiket:**
  - Standart Kullanıcı Hakları
    - Low veya Medium
  - Yönetici Hakları
    - High veya System
- **Yetkisiz değişiklikleri önler**
- **Zararlı yazılımlara karşı koruma sağlar**
- **Run As Administrator**

Uygulama – SID Değerlerinin Elde Edilmesi

- Uygulama 2 dosyasını indiriniz.

Lütfen uygulamayı tamamlayınız!

Uygulama – SAT Değerlerinin Elde Edilmesi

- Uygulama 3 dosyasını indiriniz.

Lütfen uygulamayı tamamlayınız!

Kimlik Doğrulama

Çok Aşamalı Kimlik Doğrulama

- **Bilinen (Something you know)**
  - Parola (*tahmin edilebilir, çalınabilir, paylaşılabilir*)
- **Sahip Olunan (Something you have)**
  - Akıllı Kart, Parola Üreteçleri (*çalınabilir*)
- **Sizin Olan (Something you are)**
  - Parmak İzi, Retina Taraması (*pahalı, bazen kopyalanabilir*)

Kimlik Doğrulama Protokolleri

- **Basit Kimlik Doğrulama (Basic Authentication)**
  - Telnet, FTP, POP, IMAP, vs..
  - Base64 ile kodlanıp gönderilebilir
- **Sınama/Yanıt Kimlik Doğrulama (Challenge Response Authentication)**
  - Kullanıcıdan sunucuya istek
  - Sunucudan kullanıcıya rastgele bir sayı
  - Sunucu, kullanıcı kimliğe uygun cevap oluştur
  - Kullanıcı, rastgele sayıyı alıp, şifreleyerek gönderir

Şifre Özetleri

- **Nerede Tutulur?**
  - **Yerel şifre veritabanı:** %systemroot%\system32\config\SAM
  - **Etki alanı denetçisi:** %SystemRoot%\ntds\NTDS.DIT
- **Bu dosyalara erişilebilir mi?**
  - Kullanıcılar (administrators grubu dahil) tarafından kopyalanmasına, silinmesine ve okunmasına izin vermez. (İşletim sisteminin varsayılan araçları ile erişilemez.)
  - Yönetim ve hacking araçları ile erişilebilir.

SAM ve SYSTEM

SAM: Yerel kullanıcı hesapları veritabanı

SYSTEM: Sistem verileri + SYSKEY

- Yeri: %SystemRoot%\System32\Config
- Sistem çalışırken değişiklik yapılamaz.

Parolaların saklanması:

SYSKEY [LM/NTLM(Parola)] → SAM

SAM ve SYSTEM

Örnek:

testuser1:"":0F20048EFC645D0A179B4D5D6690BDF3
:1120ACB74670C7DD46F1D3F5038A5CE8:::

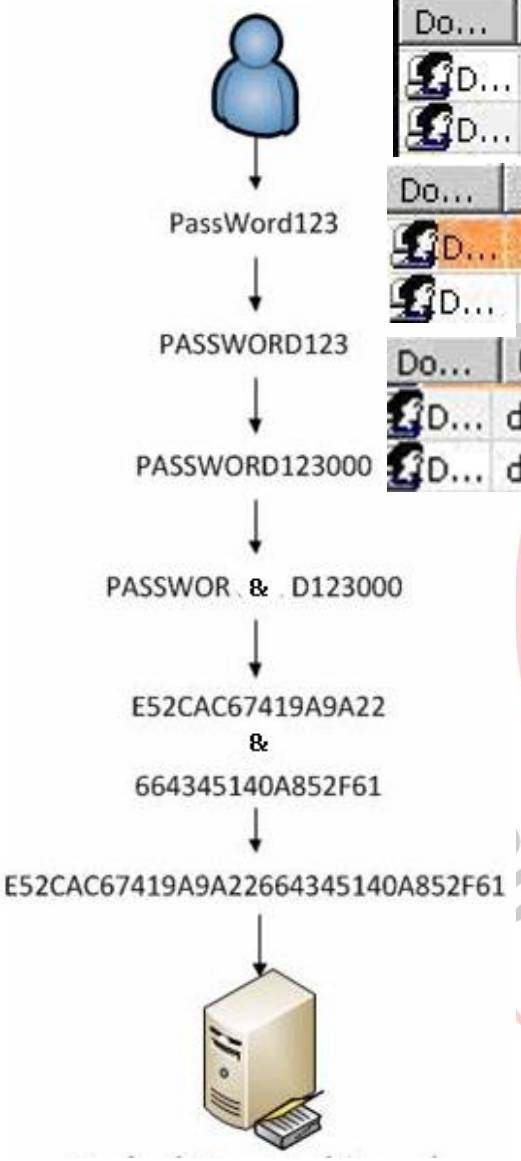
Kullanıcı Adı

İpucu-parola hatırlatıcı

NTLM-Hash değeri

LM-Hash değeri

LM



Do...	User Name	LM Password	<8	Password	LM Hash
D...	test1	PASSWORD		password	E52CAC67419A9A224A3B108F3FA6CB6D
D...	test2	PASSWORD		PassWord	E52CAC67419A9A224A3B108F3FA6CB6D

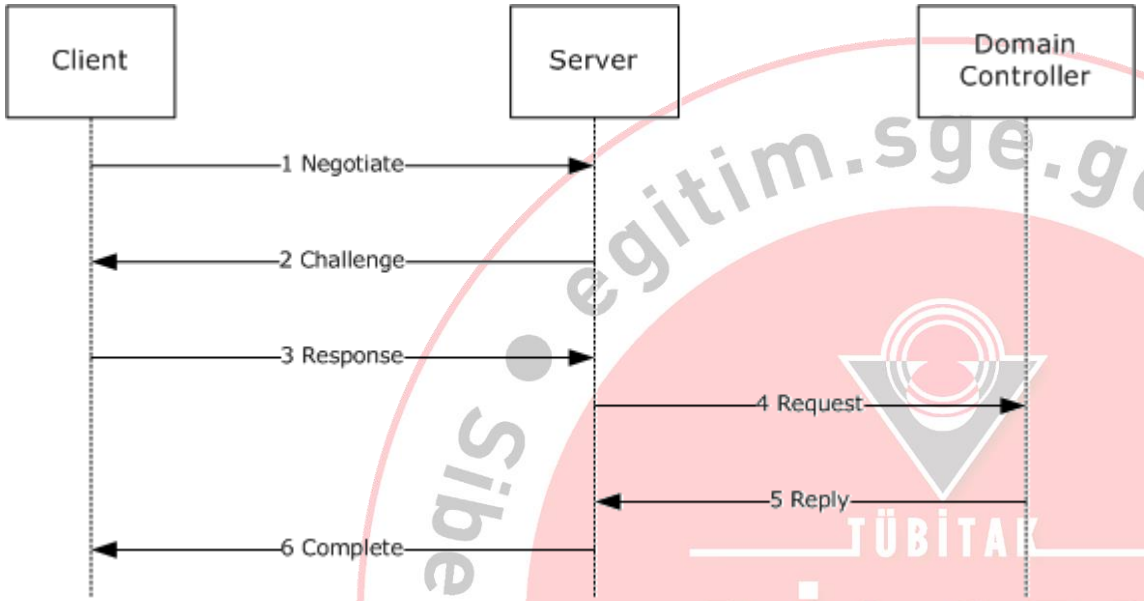
Do...	User Name	LM Password	<8	Password	LM Hash
D...	test	* empty *	x	* empty *	AAD3B435B51404EEAAD3B435B51404EE
D...	test	* empty *			AAD3B435B51404EEAAD3B435B51404EE

Do...	User Name	LM Password	<8	Password	LM Hash
D...	deneme2	???????6			9E85E206249EB46FC81667E9D738C5D9
D...	deneme3		x		9E85E206249EB46FAAD3B435B51404EE

Eksikleri

- Büyük/küçük harf duyarsız. İlk 14 karakter
- (L>14) == (L=0)
- Sabit katar ile DES & SALT kullanmaz
- Boş şifre: “AAD3B435B51404EE”
- Aynı parola parçaları --> Aynı özet parçaları
- Ağ üzerinden transfer

NTLM



Adımları

1. Erişim talebi
2. Tek kullanımlık sayı
3. Sayıyı şifreleme
4. Doğrulama talebi
5. Doğrulama sonucu
6. Talep sonucu

3. Adım

1. MD4 (Parola) = NTLM Özeti
2. NTLM özeti + 5 byte (‘0’)
3. 7’Şer byte 3 parça = K1, K2, K3
4. R = DES(K1,c) + DES(K2,c) + DES(K3,c)
5. R: Cevap

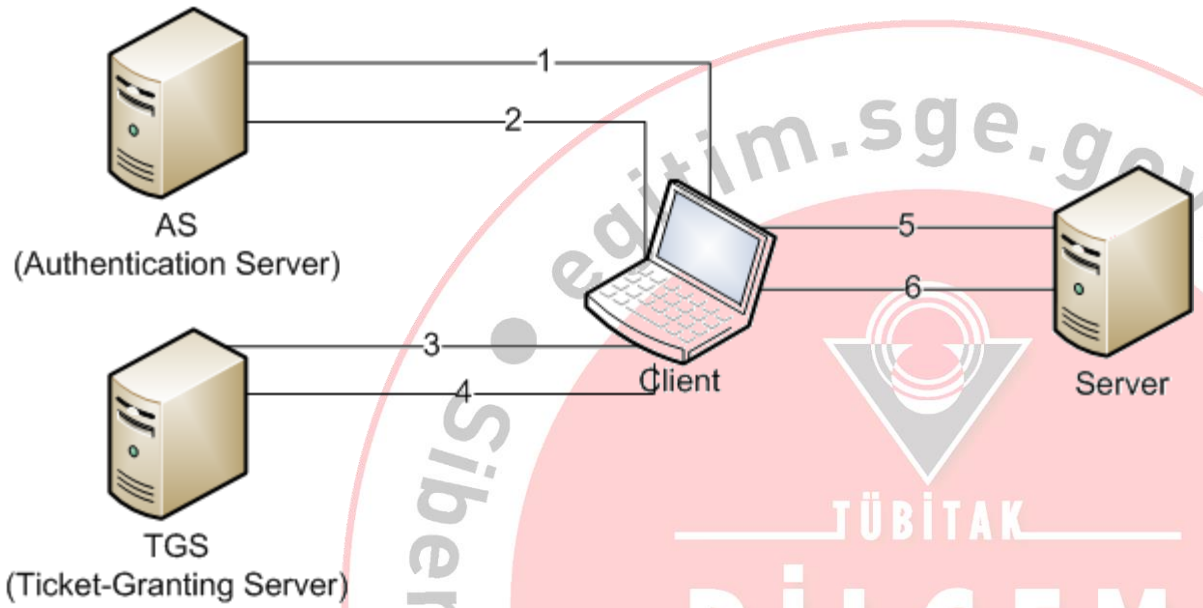
Eksikleri

1. Zayıf algoritma: MD4, DES
2. SAM dosyası: PTH, Cain&Abel
3. Tuzlama yok
4. Bilinen açık metin (MITM)

NTLMv2

- **NTLM'den daha kuvvetli**
  - Tekrarlama saldırılarına karşı dayanıklı
  - Zaman Damgası (Timestamp) değeri
  - Özetleme (Hash) işlemleri
  - Yalnızca NT-Hash kullanılması

Kerberos



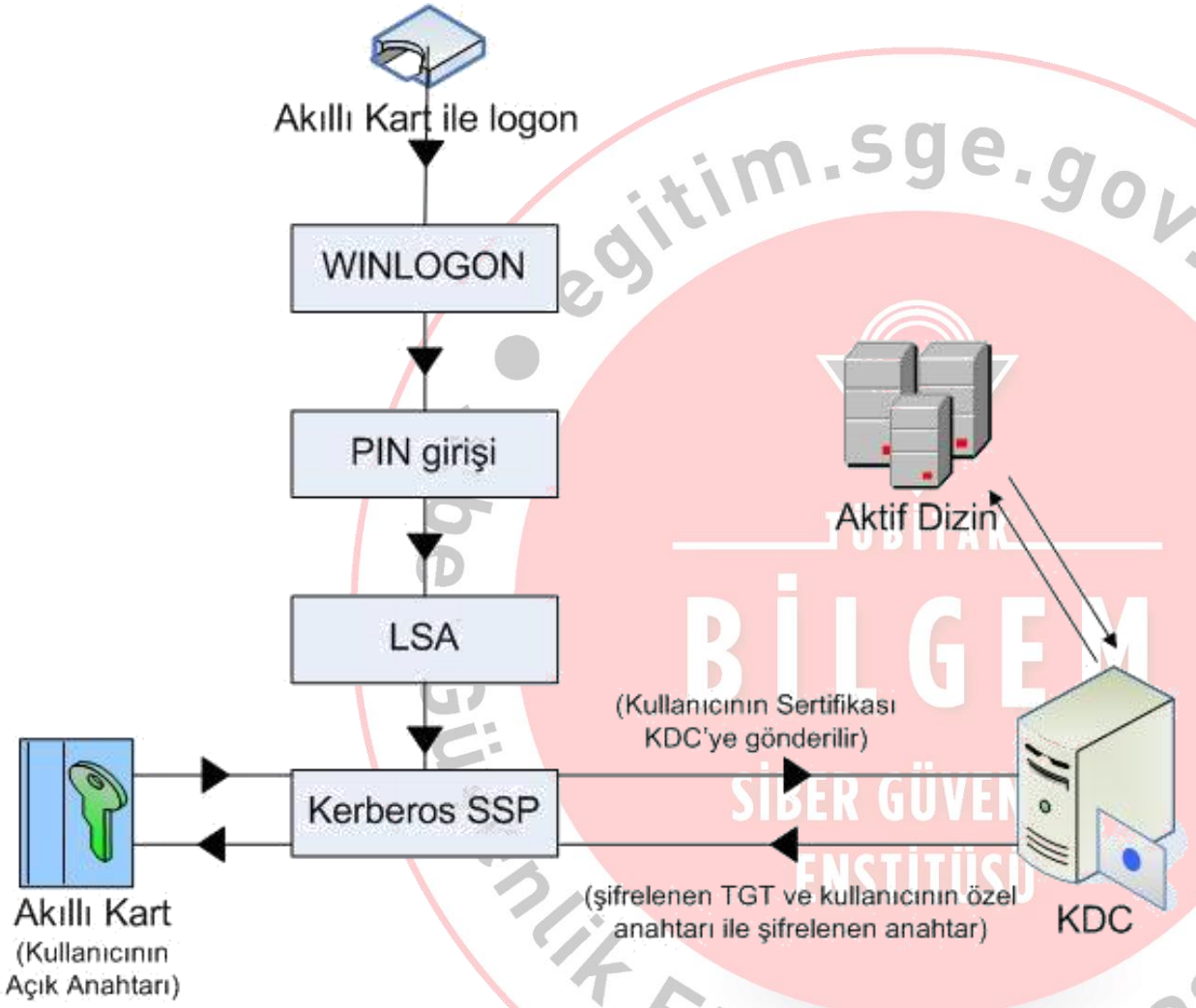
Adımları

1. TGT talebi
2. Şifreli TGT & SK1 cevabı
3. TGT ile asıl bilet talebi
4. Asıl bilet & SK2 cevabı
5. Asıl biletin iletilmesi
6. Onay

Güvenlik Özellikleri

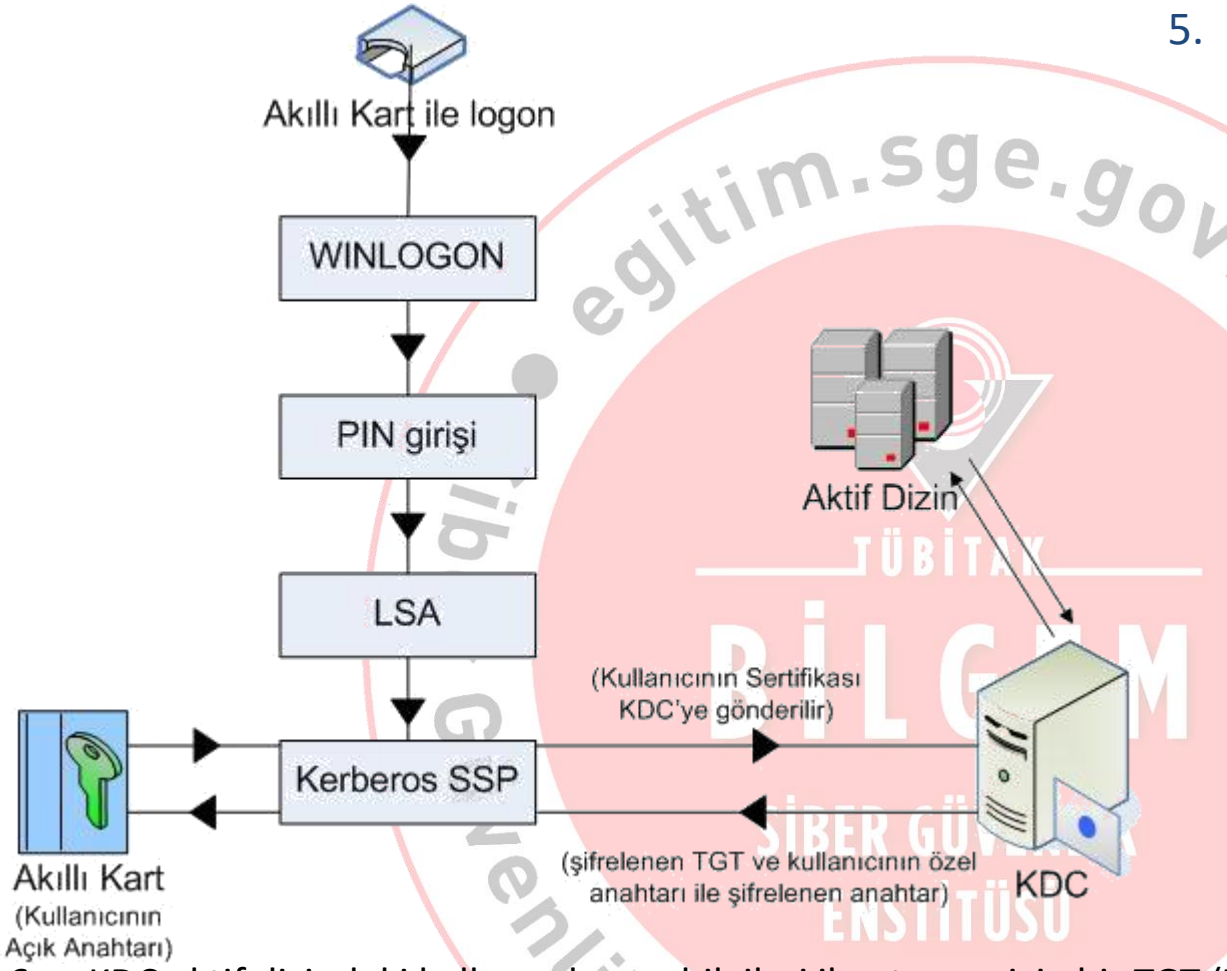
- Biletler kısa sürelidir.
- Özel anahtarlar ağdan gönderilmez. KDC'de özeti saklanır.
- Oturum anahtarları oturum sonunda silinir.
- SSO desteği, Merkezi sistem, Tekrarlama saldırılarına karşı dayanıklı, İki taraflı Kimlik doğrulama desteği,…

Akıllı Kart ile Kimlik Doğrulama (1)



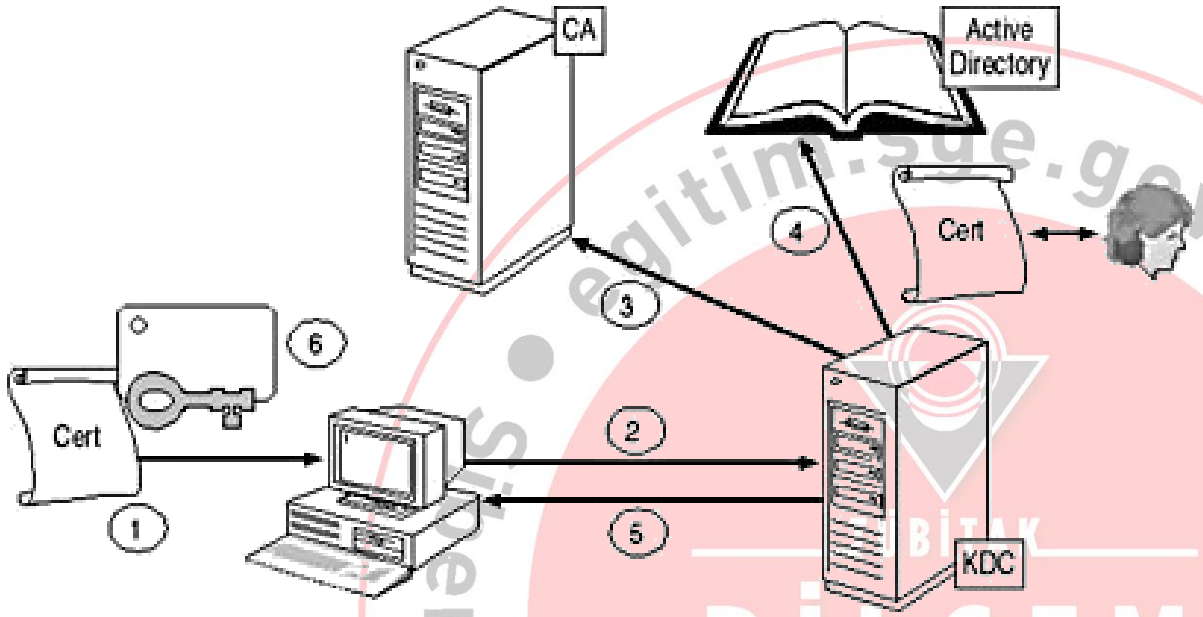
1. Kullanıcı akıllı kartını kart okuyucuya yerleştirdiğinde Windows Oturum Açma Servisi (Winlogon) kullanıcıdan PIN (Personal Identification Number) girmesini ister.
2. Kullanıcı tarafından girilen PIN, Local Security Authority (LSA) ya gönderilir.
3. LSA girilen PIN i kullanarak akıllı karta erişir ve kullanıcının sertifikasını açık anahtarı ile birlikte çeker ve Kerberos servis sağlayıcısına gönderir.
4. Kerberos kimlik doğrulama servis isteğini (X.509 sertifikası ile birlikte) Domain Controller (DC) üzerindeki KDC (Key DistributionCenter) servisine gönderir.

Akıllı Kart ile Kimlik Doğrulama (2)



5. KDC ilk olarak sertifikasyon yolunu doğrular. Bunun için KDC CryptoAPI kullanarak kullanıcı sertifikasından Kök Sertifika Makamı Sertifikasına kadar doğrulama yapar. Bu doğrulama sırasında KDC kullanıcı sertifikasındaki Konu Diğer Adı (Subject Alternative Name) ile Aktif Dizindeki kullanıcı UPN (User Principal Name) ile karşılaştırır. Aynı zamanda kullanıcı sertifikasındaki imzanın yetkili Sertifika Makamı tarafından verildiği de doğrulanmış olur.
6. KDC aktif dizindeki kullanıcı hesap bilgileri ile oturum için bir TGT (Ticket Granting Service) oluşturur. KDC oluşturduğu TGT'yi rastgele oluşturduğu bir anahtar ile şifreler. Bu anahtar kullanıcın açık anahtarı ile şifrelenir ve bu şifrelenmiş anahtar da KDC'nin veri alanına eklenir. Böylece sadece istemcinin kendi özel anahtarı ile şifresini çözebileceği bir oturum açma anahtarı oluşturulmuş olur.
7. İstemci kendi özel anahtarı ile oturum açma anahtarının şifresini çözer ve TGT'yi doğrulama servisine (ticket granting service) sunar.

Akıllı Kart ile Kimlik Doğrulama (Özet)



Adımları

1. PIN ile sertifika temini
2. Sertifikanın yollanması
3. Sertifika kontrolü
4. Kullanıcı kontrolü
5. TGT &SK1 iletilmesi
6. SK1 elde edilmesi

Özellikleri

1. Genel & Özel anahtar çifti
2. Kimlik doğrulama & Sayısal İmza
3. Kerberos'tan daha güvenilir.

Zayıflıkları

1. Özel bilet iyi saklanmalı
2. Donanımsal & Maliyetli
3. Bilet hala istemci makinede

Parola Saldırıları

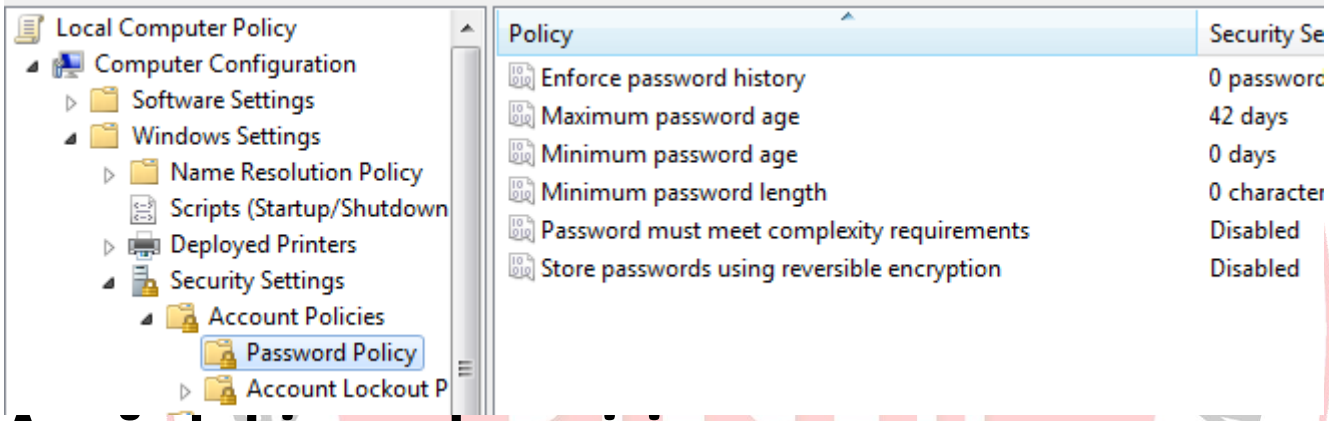
- **Parolaları elde etme**
  - Doğrudan sorarak
  - Key-logger ile
  - Kimlik doğrulanırken (challenge-response)
  - Hash'ler elde edilerek
  - Tahmin ederek
- **Eldekilerin kullanılması**
  - Parolalar kırılarak
  - Önceden hesaplanmış hash değerleri
  - Pass-the-Hash saldırıları

Parola Korunumu

- **Parola politikası**
  - Karmaşıklık vs Uzunluk
  - Yerel Hesaplar vs Etki Alanı Hesapları
- **Fine-Grained parola politikası**
  - Yöneticiler vs Kullanıcılar
- **Çok aşamalı kimlik doğrulama**
  - Parola, Akıllı Kart, Parmak İzi
- **Parolaların güvenli saklanması**
  - Şifreleme

Yerel Parola Politikası

- **Başlat > gpedit.msc yazın ve çalıştırın**
- **Bilgisayar Konf. > Windows Ayar. > Güvenlik Ayarları > Hesap Politikaları > Şifre Politikası yolunu takip edin**



- **Aşağıdaki ayarları girin:**
  - Minimum parola uzunluğu: 10 karakter
  - Karmaşık parola: Etkin
- **Yeni kullanıcı oluşturarak politikayı test et**
  - Net user testuser abcd123456 /add

Uygulama – Parolanın Elde Edilmesi

- Uygulama 4 dosyasını indiriniz.

Lütfen uygulamayı tamamlayınız!

Erişim Kontrolü

Windows Dosya Sistemleri

- **CDFS**
- **FAT**
- **exFAT**
- **NTFS**
  - İzinler (ACL)
  - Denetleme
  - Şifreleme
  - Sıkıştırma

Windows Erişim Kontrol Modeli

İki temel parçadan oluşur:

- Erişim Bileti (Access Token)
  - SID
  - Grup SID
  - Ayrıcalıklar
- Güvenlik Tanımlayıcıları (Security Descriptors)
  - Erişim Kontrol Listesi (ACL)
    - DACL
    - SACL

    } ACE
  - Nesne Sahibi SID
  - Bazı kontrol bit değerleri.

Erişim Kontrol Kayıtları (ACE)

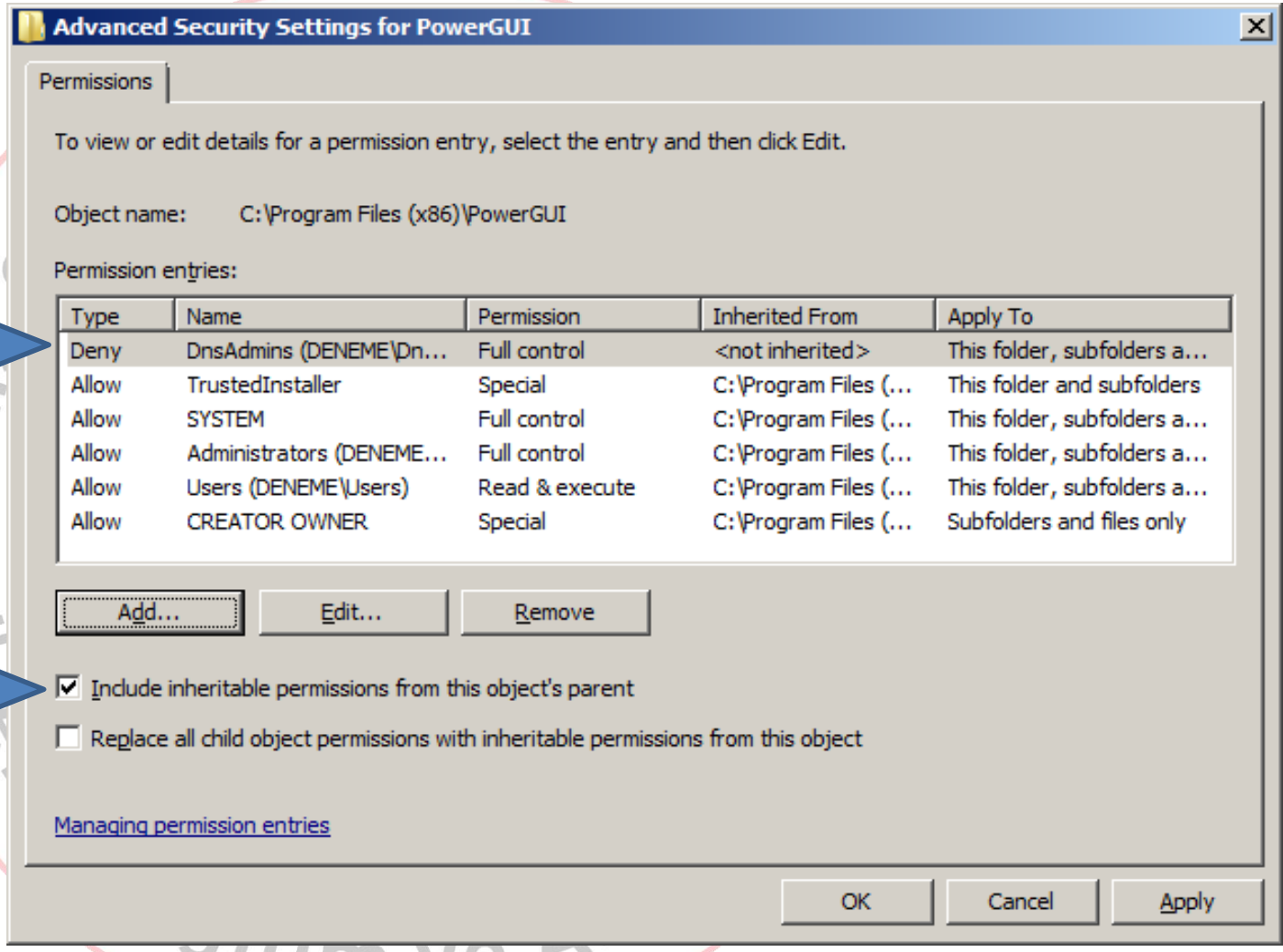
- Erişim Kontrol Listelerinin (ACL) bir elementidir.
- Erişim veya denetim kontrolü.
- Kullanıcı veya gruba
- İzin ver veya engelle
- Üst dizinden kalıtım
- Farklı şekilde alt dizinlere uygulanma

Erişim Kontrol Kayıtları (ACE)

TÜBİTAK

Deny izni Allow iznini ezer.

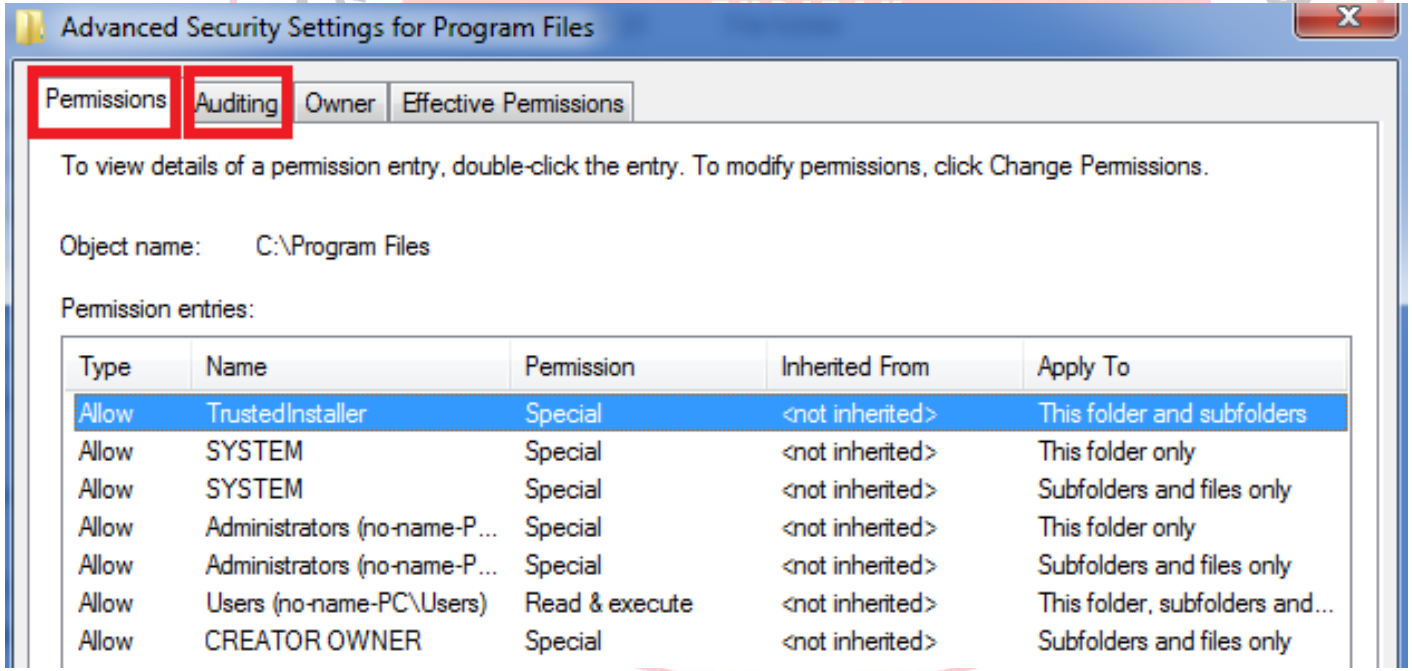
İzinler kalıtsal olarak aktarılabilir.



Erişim Kontrol Listeleri (ACL)

- ACL
  - DACL
  - SACL
- ACE

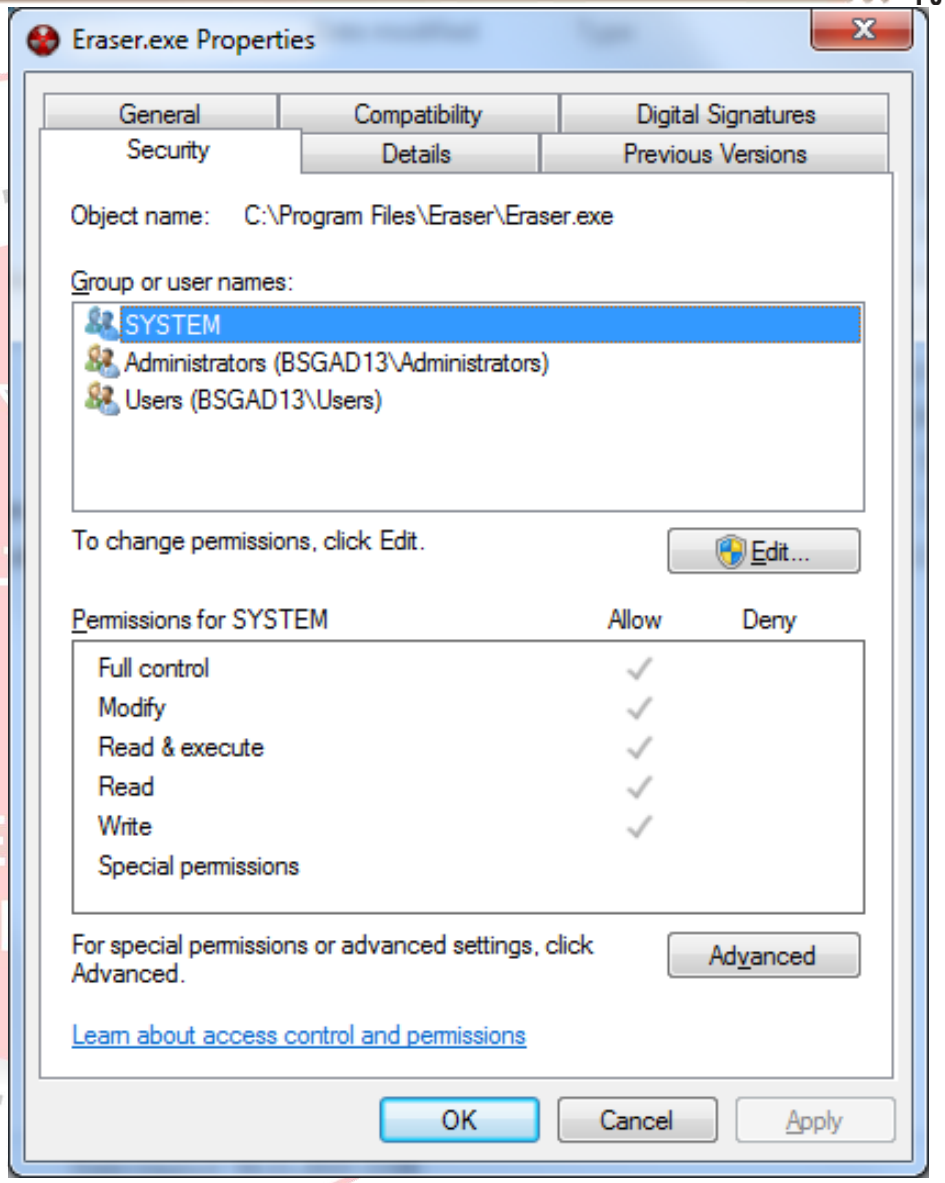
nesnelerinin bir araya gelmesi ile oluşur.



Discretionary Access Control List (DACL)

Nesne erişim kontrolü

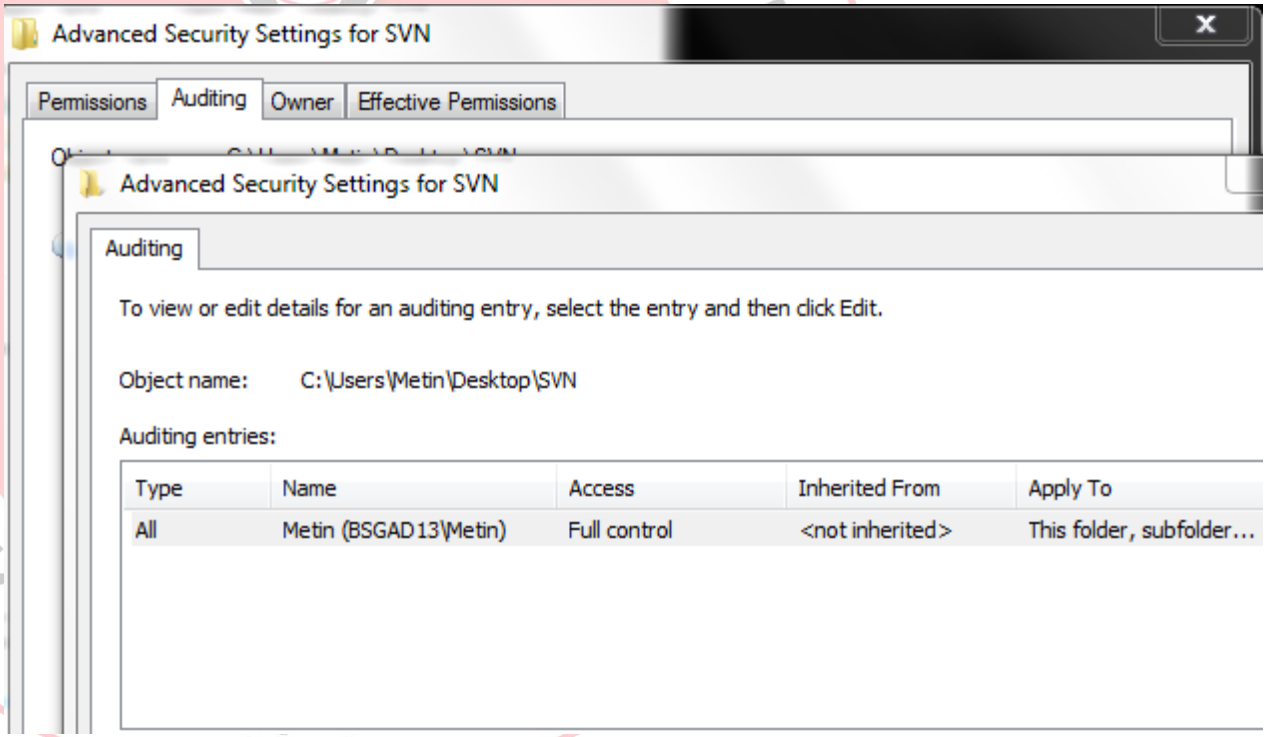
- İzin ver (Allow)
- Engelle (Deny)



System Access Control List (SACL)

Nesne erişim denetimi

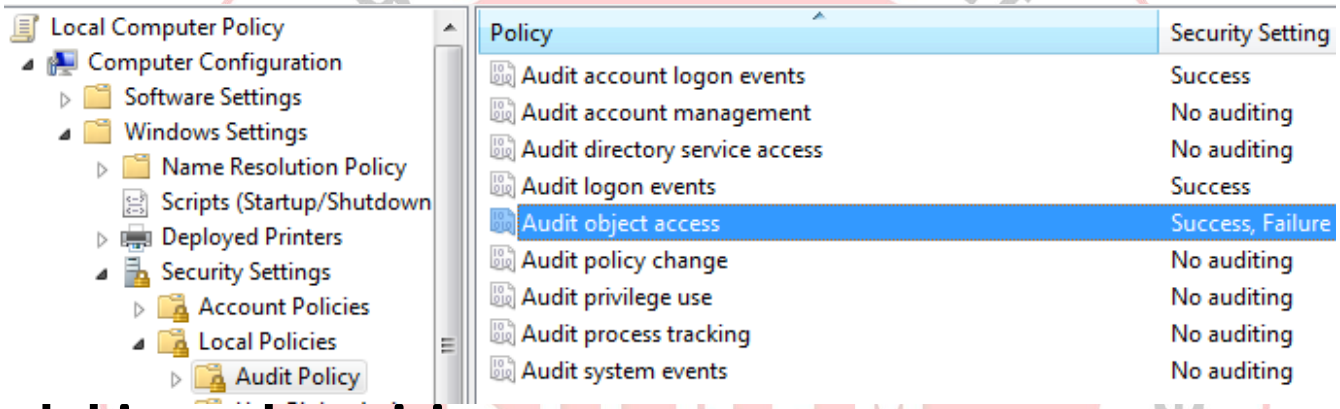
- Başarılı
- Başarısız
- Her ikisi de



Nesne erişim denetimi grup politikası ile açılmalıdır.

Uygulama - Güvenlik ACL (SACL)

- Başlat > gpedit.msc yazınız ve çalıştırınız.
- Bilgisayar Konf. > Windows Ayar. > Güvenlik Ayarları > Yerel Politikalar > Denetim Politikası yolunu takip ediniz.

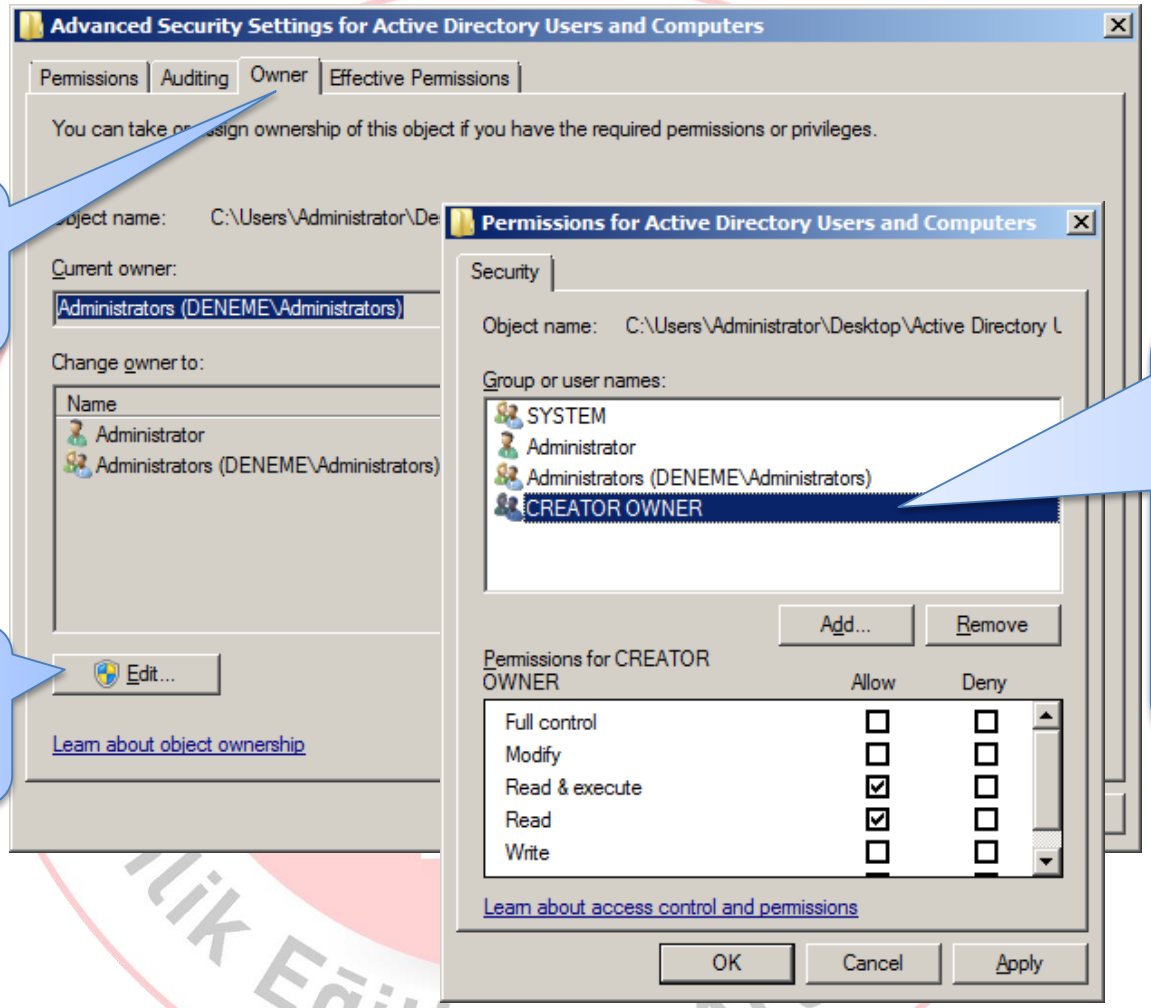


- Aşağıdaki ayarları girin:
  - Erişim Denetimi: Başarılı, Başarısız
- C:\ altında DenetimliKlasör adında klasör oluşturunuz.
- Klasöre SACL tanımlayın (Create ve Delete için)
- Yeni bir metin dosyası oluşturun
- Güvenlik olay kayıtlarından 560 ID nolu kayıt arayın

Sahiplik (Owners)

Her nesnenin bir sahibi vardır.

Sahiplik değiştirilebilir.

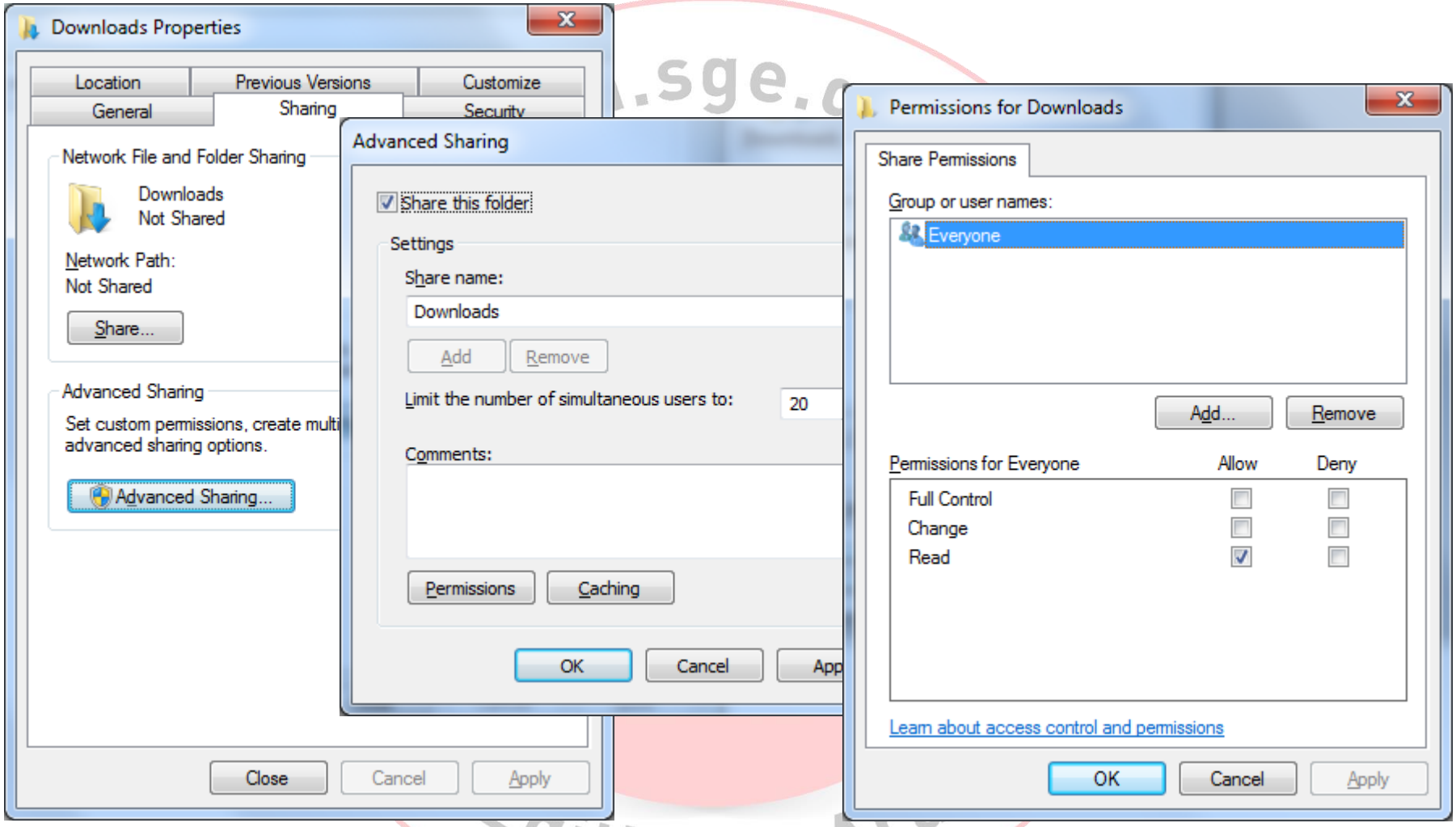


Creator Owner grubuna atanan izinler dosyanın o anki sahibine atanan izinlerdir.

Paylaşım İzinleri

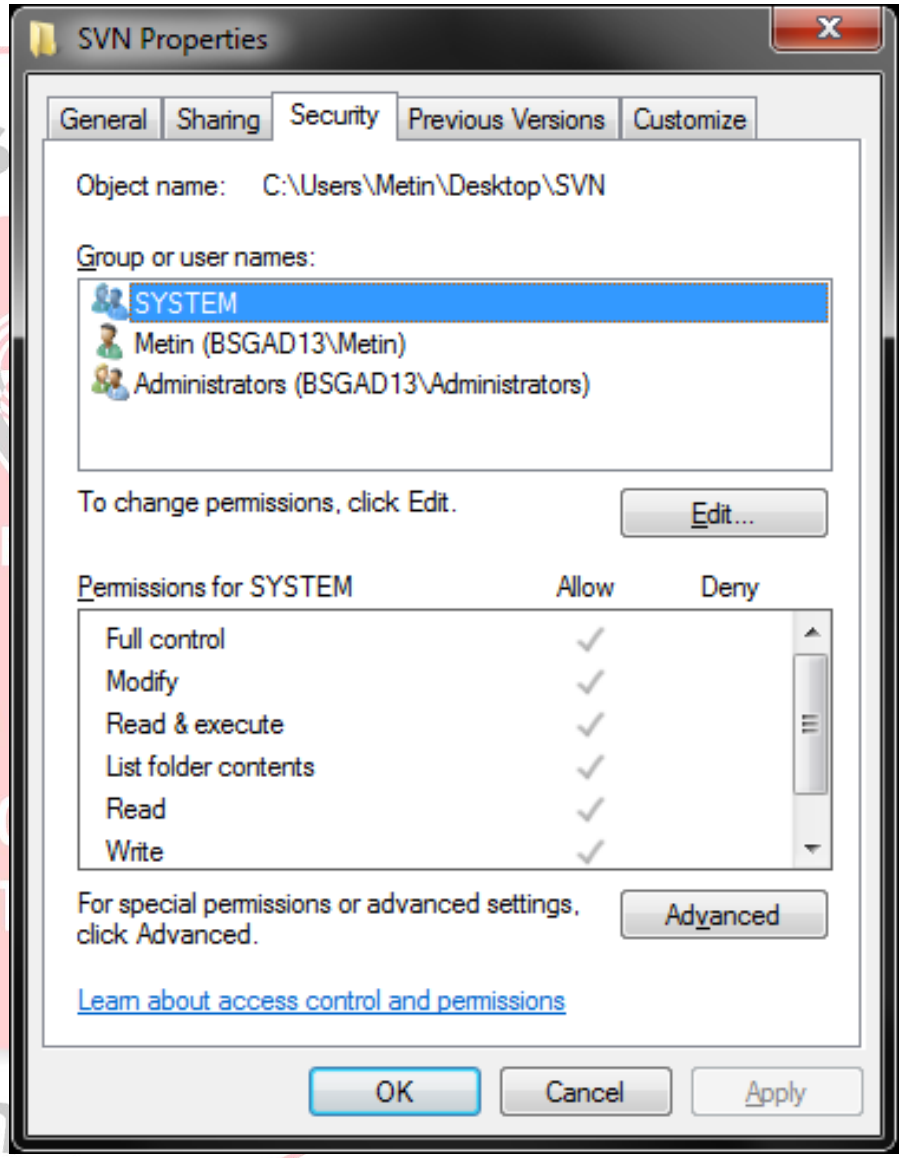
- **Ağ üzerinden erişimlerde kullanılır.**
- **NTFS izinlerine göre daha sadedir.**
- **NTFS izinlerine bağımlıdır.**
- **Kullanıcı veya grup bazında yetkilendirme**
  - Full Control
  - Change
  - Read
- **Farklı izinlerde çok sayıda paylaşım ismi**

Paylaşılan Klasör İzinleri



Dosya & Klasör İzinleri

- NTFS'e bağımlı
- Paylaşım izinlerinden daha detaylı
- Hem ağ üzerinden hem de yerel erişimlerde
- Yöneticiler ve sahipler izinleri değiştirebilir



Erişim Kontrol Süreci

Paylaşım İzinleri

- **Ahmet**
  - Satış Grubu - Modify
  - Ahmet – Full Control
  - Authenticated Users - Read

NTFS İzinleri

- **Ahmet**
  - Authenticated Users – Read
  - Satış – Read
  - Ahmet – Read,Write

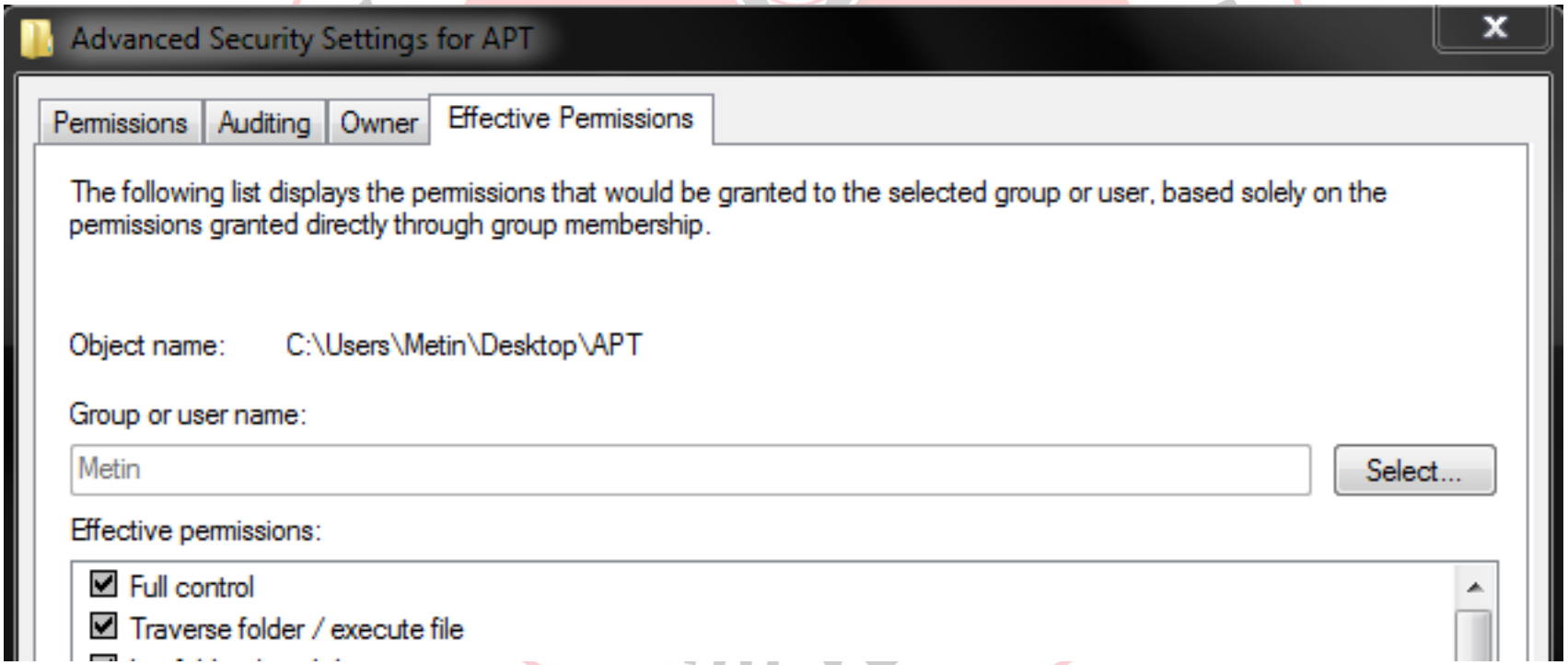
DENY: Her zaman öncelikli olarak uygulanır!

Etkili İzinler (Effective Permissions)

Ahmet birden fazla gruba üyeyse…

Bu grupların izinleri nelerdir?

Ahmet'in bir dizin üzerinde geçerli izni nedir?



En Az Hak Prensibi

- **Yetkilendirme Yöntemi**
  - Çalışılabilir olmalı
  - Tüm haklar kısıtlı olmalı
  - İhtiyaç duyulduğu kadar izin verilmeli
  - Ne daha az ne daha fazla yetki

Gizli Paylaşımlar

Gizli paylaşımları kapatmak için!

Baslat > regedit

Domain yöneticileri için:

- Hive: HKEY_LOCAL_MACHINE
- Key: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
- Name: AutoShareServer
- Data Type: REG_DWORD
- Value: 0

Yerel yöneticiler için:

- Hive: HKEY_LOCAL_MACHINE
- Key: SYSTEM\CurrentControlSet\Services\LanManServer\Parameters
- Name: AutoShareWks
- Data Type: REG_DWORD
- Value: 0

Uygulama - Gizli Paylaşımlar

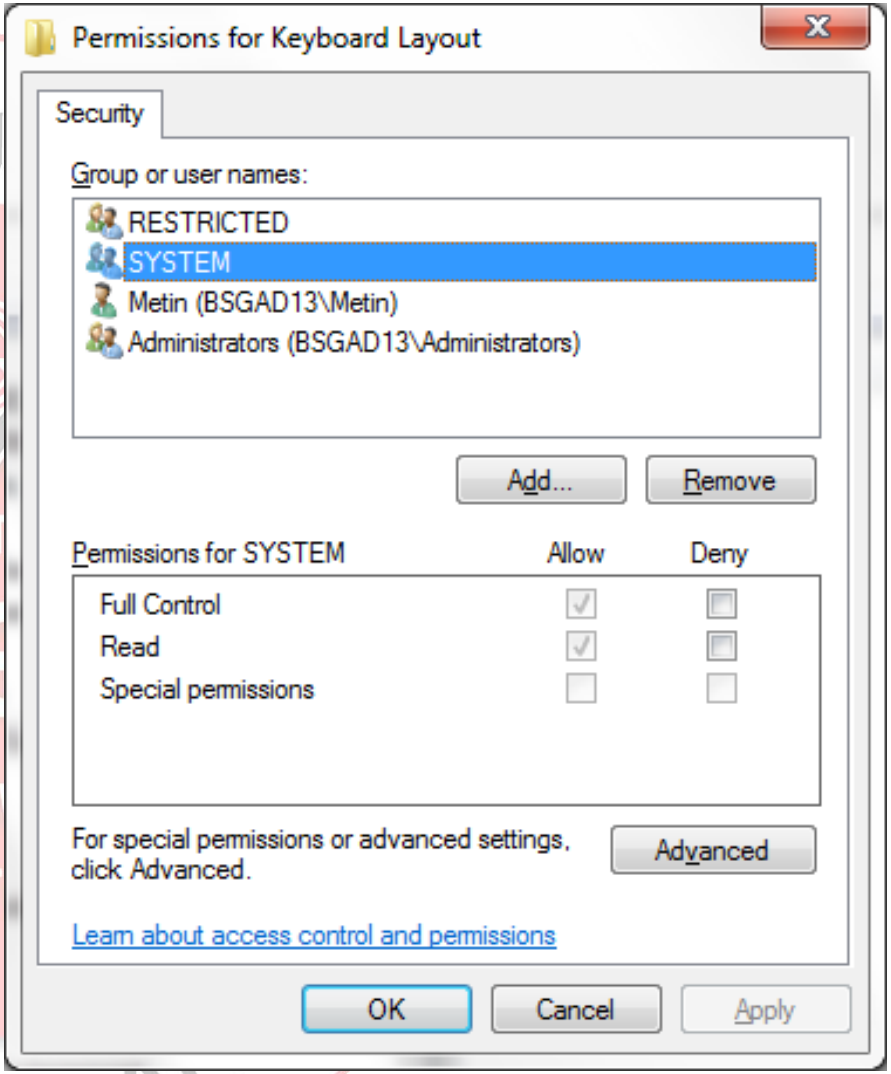
- **$ - gizleme karakteri**
- **Varsayılanlar:**
  - ADMIN$
  - C$ ve x$
  - FAX$
  - IPC$
  - PRINT$

Ortak Alan İzin Yapılandırması

- **Klasör İzinleri**
  - SYSTEM - Full Control
  - Domain Admins - Full Control
  - Creator Owners - Full Control
  - Authenticated Users - Read || Modify
- **Paylaşım İzinleri**
  - Domain Admins – Full Control
  - Authenticated Users – Read & Change
- **Access Based Enumeration**

Kayıt Defteri (Registry) İzinleri

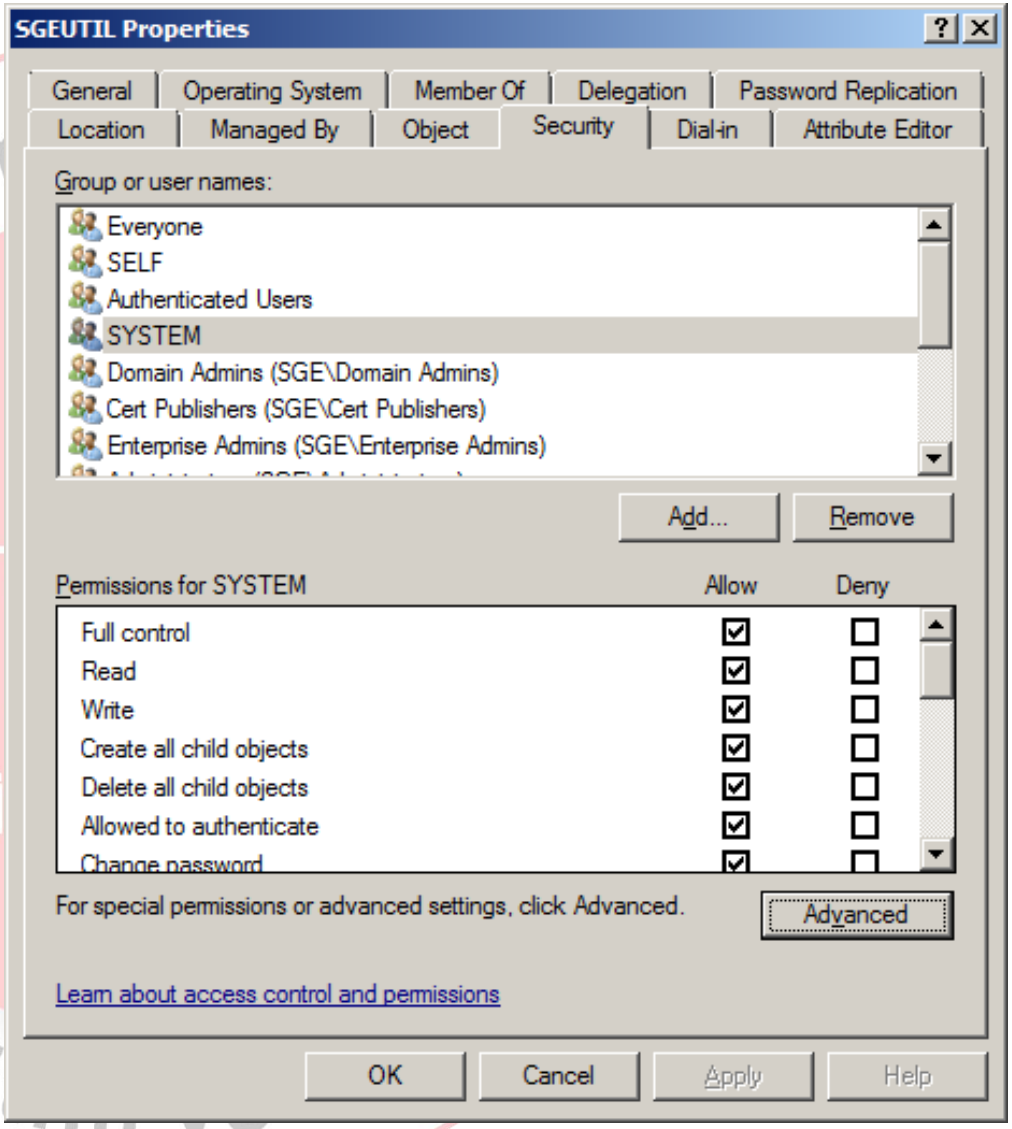
- Denetim
- Sahiplik
- Kalıtım
- Etkili İzinler
- Remote Registry Service
- Paylaşım İzinleri - Winreg



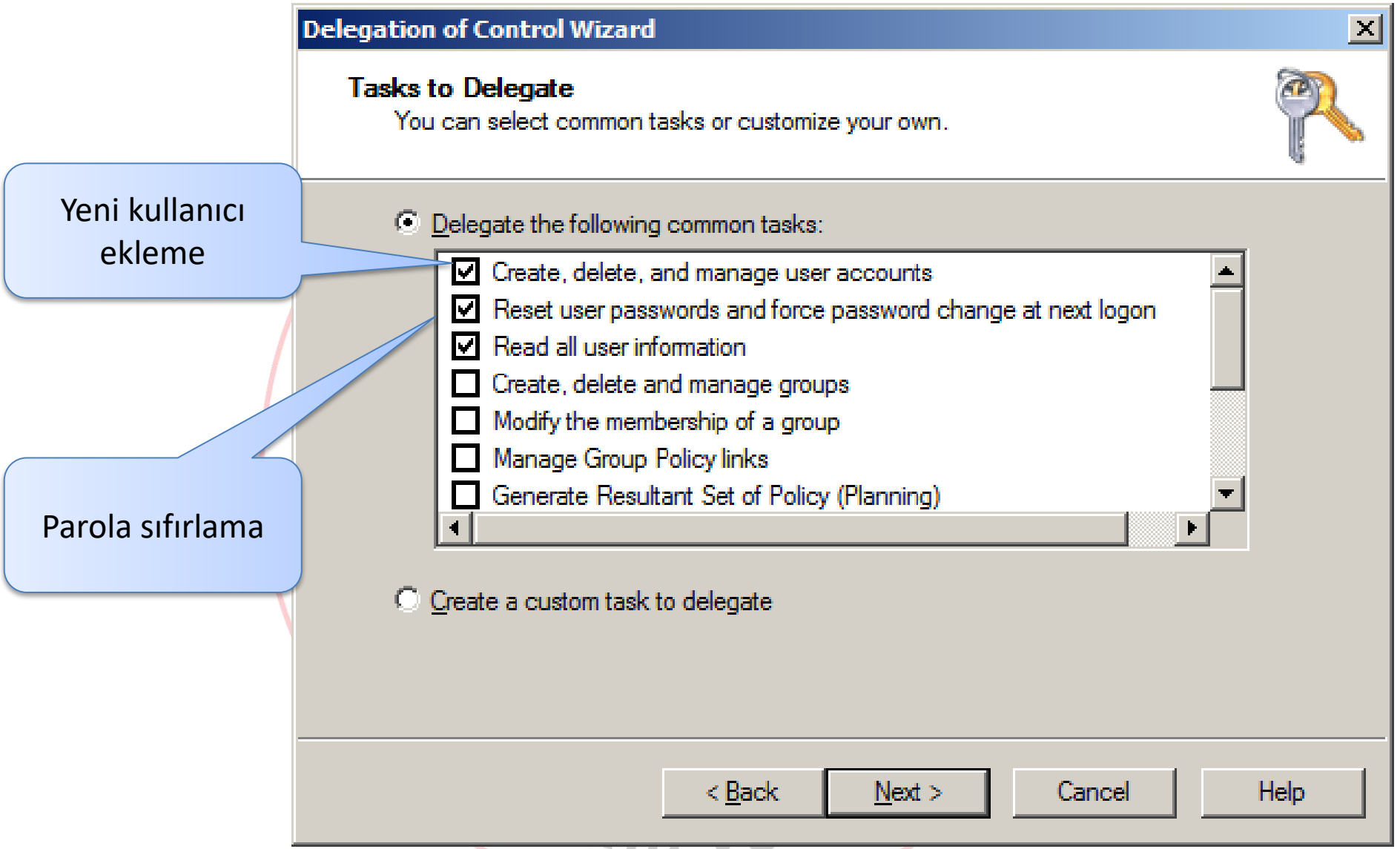
HKLM\System\CurrentControlSet\Control\SecurePipeServers\winreg

Aktif Dizin İzinleri

- Denetim
- Sahiplik
- Kalıtım
- Nesne ve Özellikler



Aktif Dizin Yetki Devri



Güncelleme

Yama Yönetimi

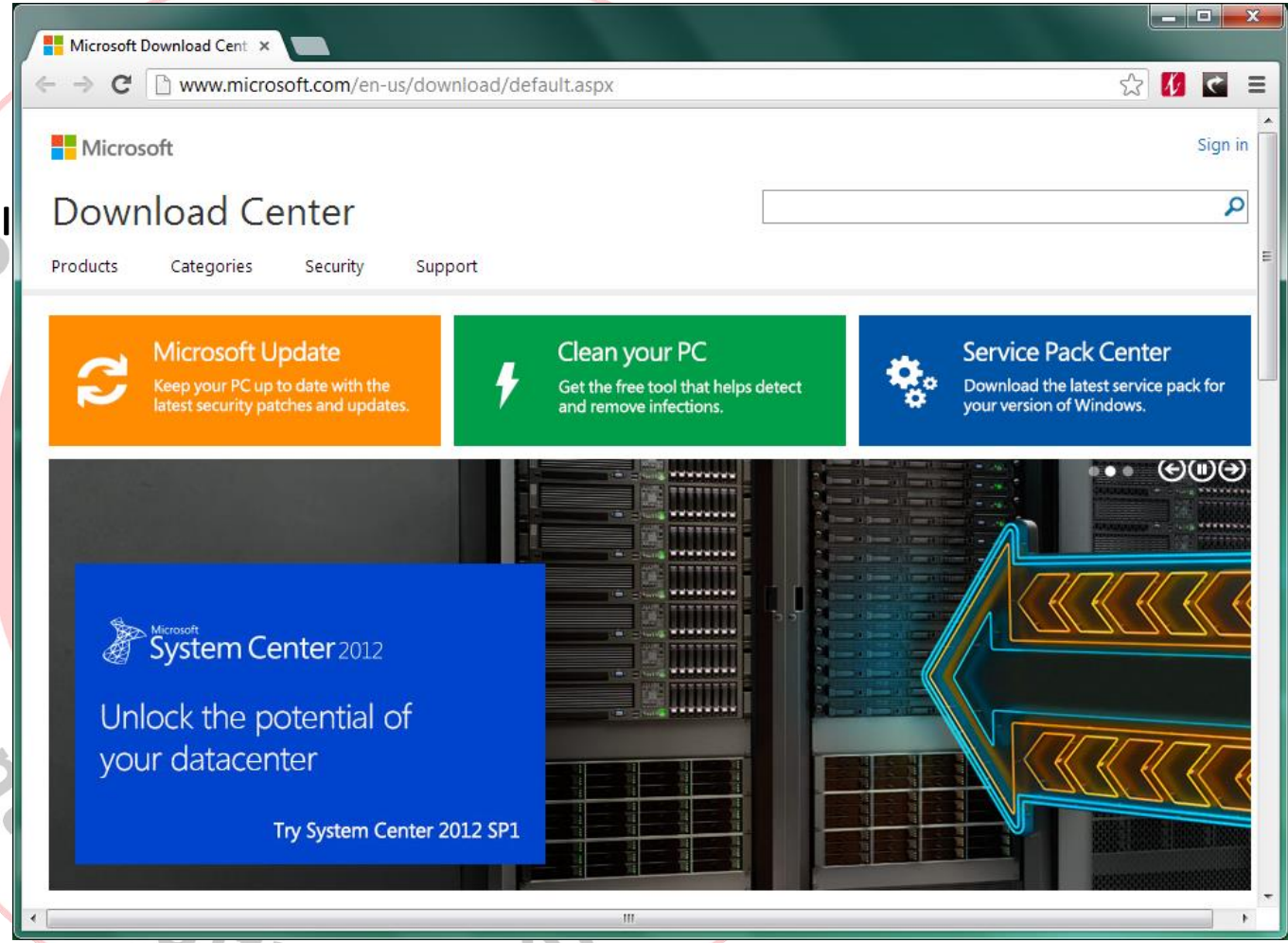
- Değerlendirme
- Tanımlama
- Karar & Plan
- Dağıtım

Terminoloji

- Bağlayıcı
- İsteğe Bağlı Kritik (COD)
- Kritik Güncelleştirme
- Toplu Güncelleştirme
- Geliştirme Seti
- Sürücü
- Özellik Paketi
- **Genel Dağıtım Sürümü (GDR)**
- Kılavuz
- Düzeltme
- İsteğe Bağlı (OD)
- Güvenlik Güncelleştirmesi
- Hizmet Paketi
- Yazılım Güncelleştirmesi
- Araç
- Güncelleştirme
- Güncelleştirme Toplaması
- Yükseltme

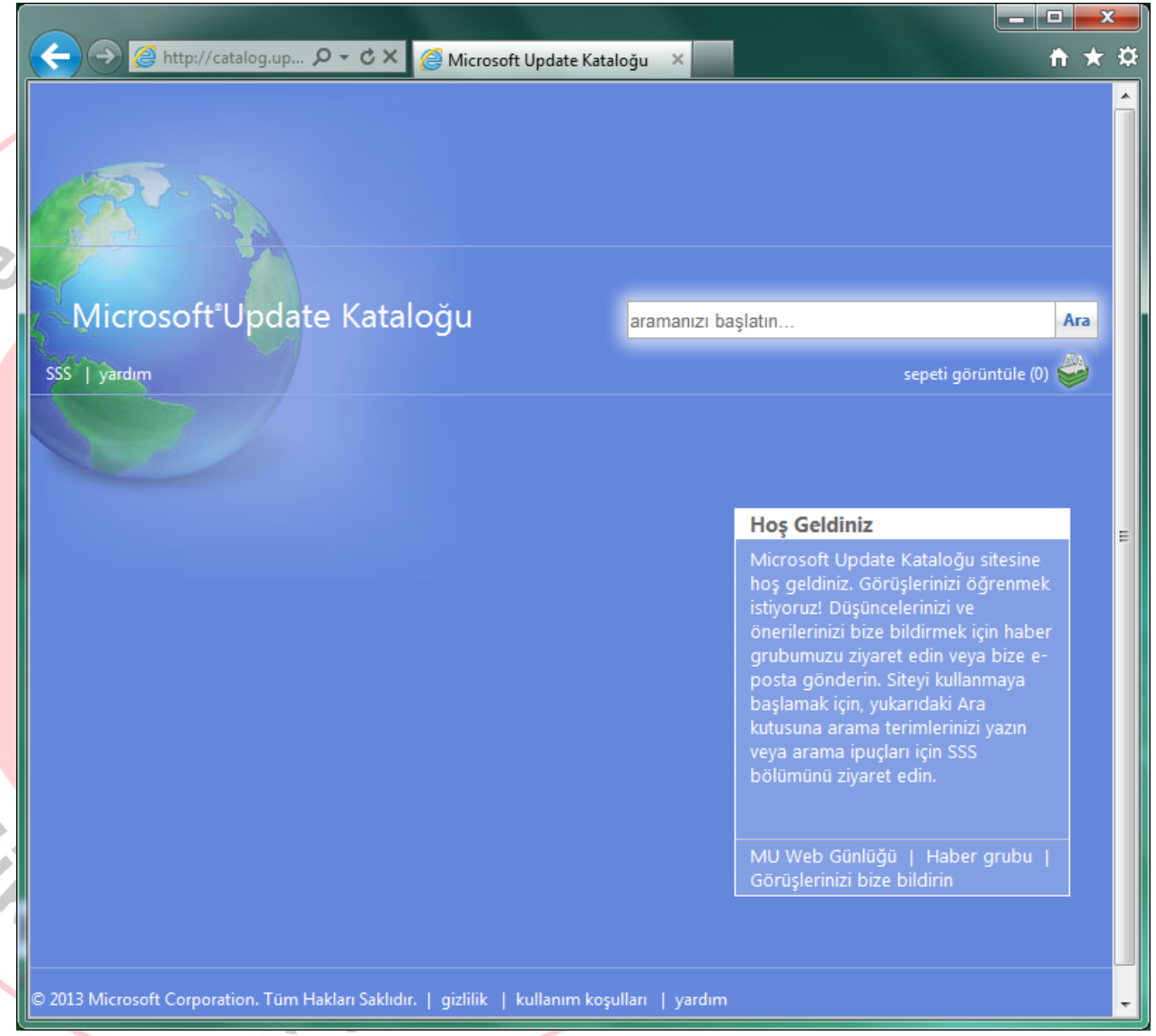
Microsoft Download Center

- Güncelleştirmeler
- Araçlar
- Deneme yazılımları
- Dokümanlar



Microsoft Upload Catalog

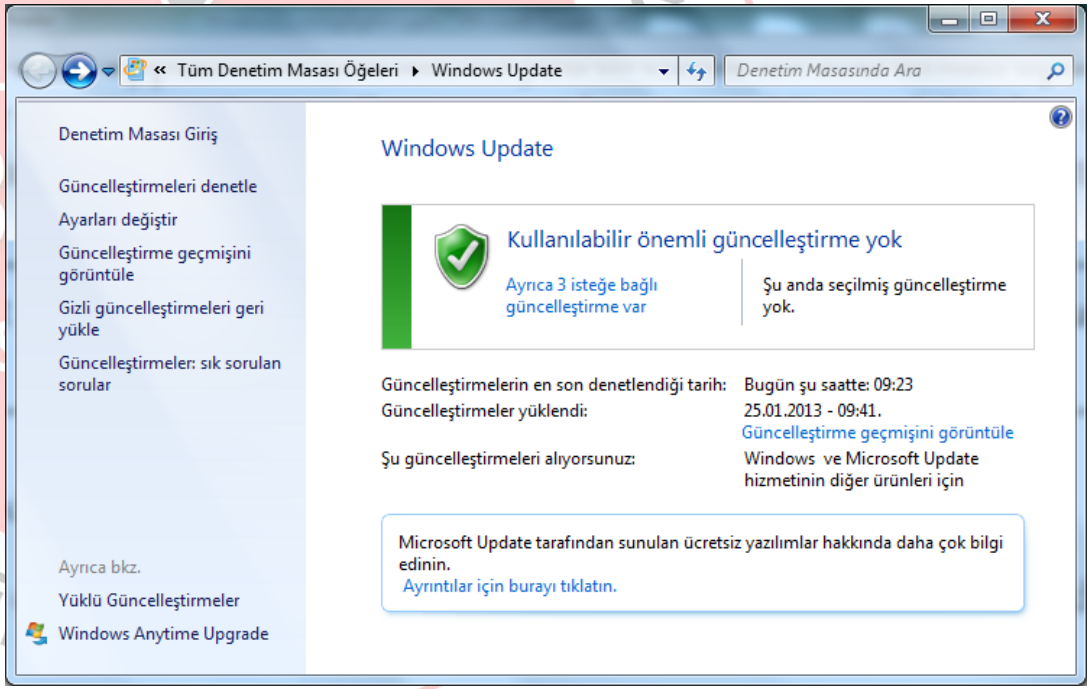
- Alışveriş Sepeti
- Tam-metin arama
- RSS beslemeleri
- BITS desteği



Windows Update & Microsoft Update

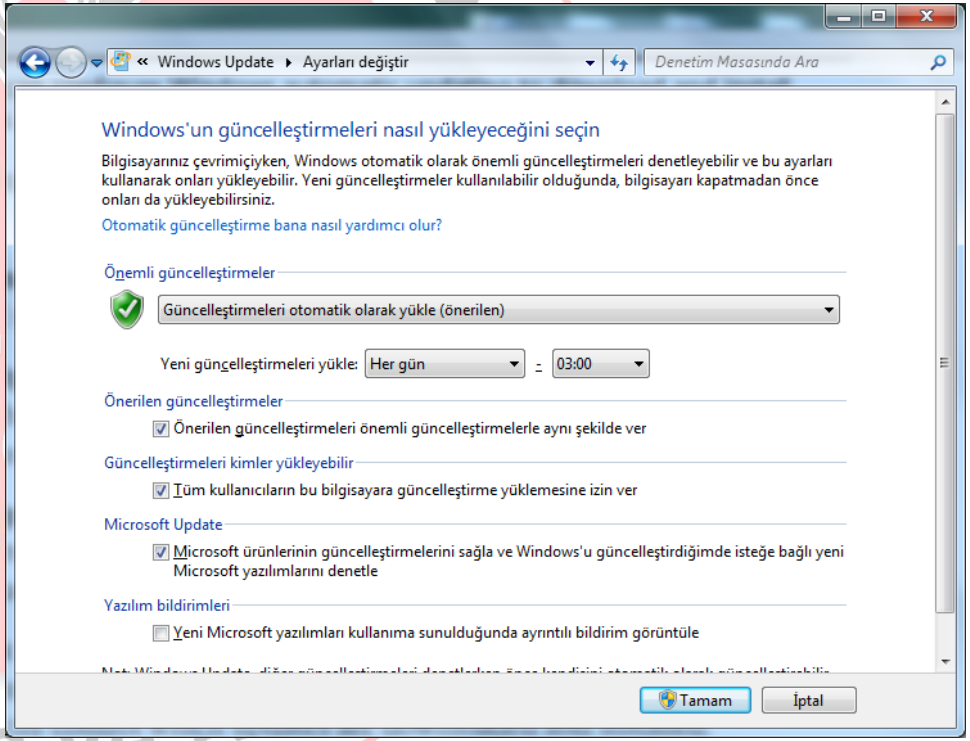
- Güncelleştirmeleri denetle
- Ayarları değiştir
- Güncelleştirme geçmişini görüntüle
- Gizli güncellleştirmeleri geri yükle
- Güncelleştirmeler: sık sorulan sorular

Windows Otomatik Güncelleştirme



Windows Automatic Updating

- Güncelleştirmeleri otomatik olarak yükle (önerilen)
- Güncelleştirmeleri karşıdan yükle, ancak kurma konusundaki kararı bana bırak
- Güncelleştirmeleri denetle, ancak karşıdan yükleme ve kurma konusundaki kararı bana bırak
- Güncelleştirmeleri hiçbir zaman denetleme



Windows Server Update Services

- Merkezi yama yönetimi
- Bant genişliği optimizasyonu (BITS)
- Yönetici onayı
- Raporlama
- Otomatik olarak indirme ve dağıtım
- GPO ile yönetilebilme
- Yük dengemeli kurulum
- Hepsi ücretsiz...

Ticari Güncelleme Yazılımları

- GFI LANGuard
- Lumension
- Microsoft SCCM
- BigFix
- Shavlik
- Solarwinds

Ve çok daha fazlası...

Yedekleme ve Geri Getirme

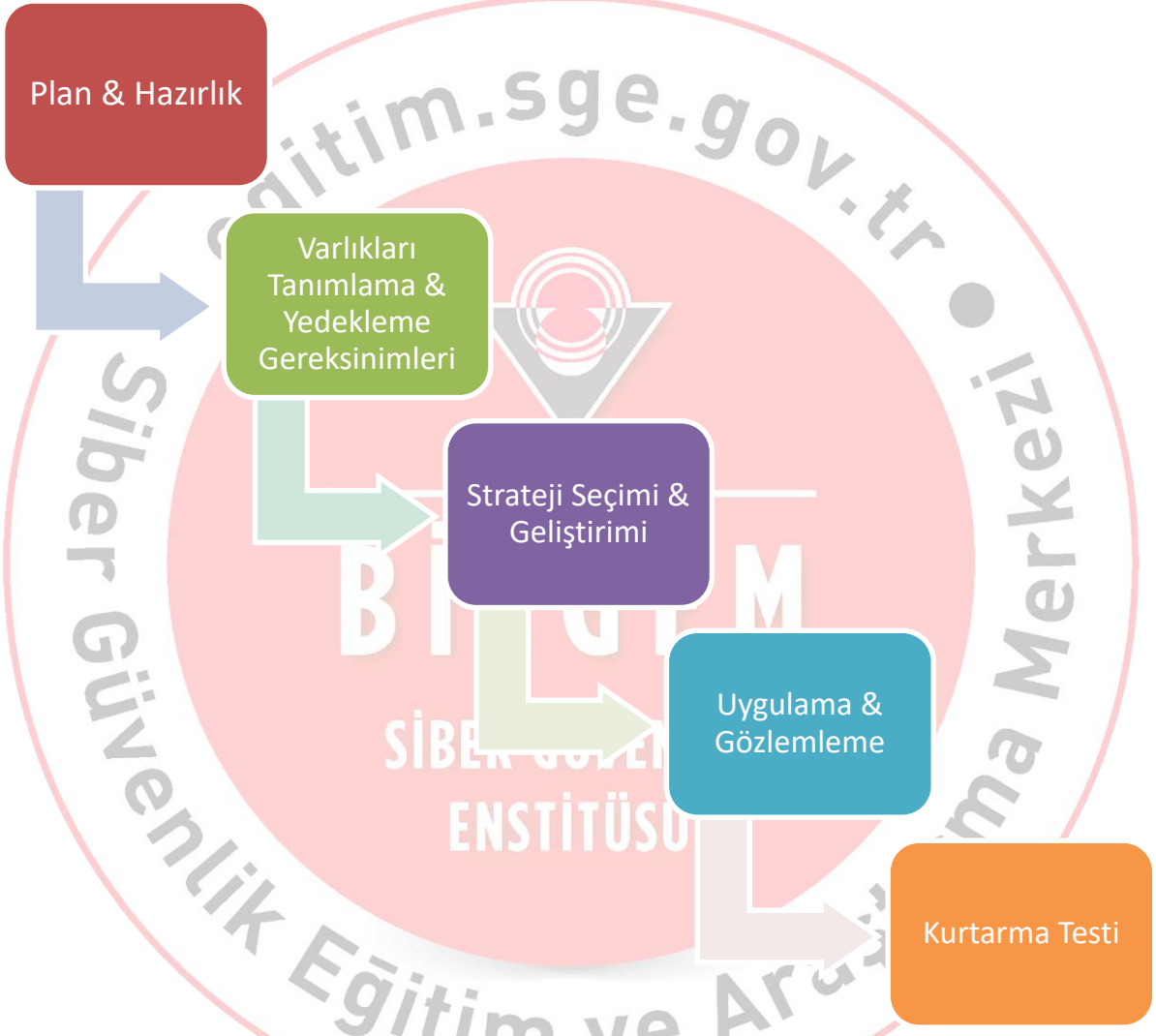
Yedekleme

- Gizli bilginin yedeği de gizlidir.
- Yedekler asıl bilgiden uzakta saklanmalıdır.
- *İnsan kaynağının yedeklenmesi?*

Yedekleme'nin Önemi

- **Adli Analiz**
- **Veri kaybına karşı alınan son önlem**
  - Donanım hatası
  - Yanlışlıkla silme
  - Doğal felaketler
  - Saldırgan tarafından veri tahrifi
  - Virüsler
  - İnsan hatası
  - Ve diğer nedenler...

Yedekleme Süreci



Yedekleme Türleri

- **Üç ana tür:**
  - Normal
  - Incremental
  - Differantial
- **Avantajları & Dezavantajları**

Windows Yedekleme Teknolojileri

NTBackup

- Dahili
- 2000, XP, 2003
- BKF formatı
- Desteklenen medyalar:
  - Type
  - Zip sürücüleri
  - Floppy diskler
  - Hard diskler
- Zamanlanmış görevler desteği
- Komut satırı desteği

Backup & Restore

- Dahili
- Vista, 7, 8, 10,2008, 2012,2016
- VHD formatı
- Desteklenen Medyalar:
  - DVD
  - Imaj temelli full sistem yedeği
- BKF formatı desteği

NTBackup.exe

NTBackup

- Dahili, Windows 2000, XP, 2003
- BKF formatı
- Desteklenen medyalar:
  - Type
  - Zip sürücüleri
  - Floppy diskler
  - Hard diskler
- Zamanlanmış görevler desteği
- Komut satırı desteği

Backup & Restore

- Dahili
- Vista, 7, 8, 10,2008, 2012, 2016
- VHD formatı
- Desteklenen Medyalar:
  - CD/DVD – Blu-ray
  - Imaj temelli full sistem yedeği
- Tape sürücüleri desteklenmez
- BKF formatı desteği
- Dosya türü seçebilme

Windows Server Backup

Windows Server 2008 R2

- Performans iyileştirmeleri
- İncremental yedekleme
- Gelişmiş sistem durumu yedekleme ve yedekten geri dönme seçenekleri
- Genişletilmiş komut satırı desteği
- Powershell desteği
- Genişletilmiş yedekleme medyası desteği
- Yerel ve uzak sistemlerin yedeğinin alınması

Ticari Yedekleme Yazılımları

Diğerleri

- Acronis True Image
- Backup Exec
- Comodo Backup
- HP Data Protector
- IBM Tivoli Storage Manager
- NetBackup
- Norton Ghost
- EMC RecoverPoint
- UltraBac
- Ve çok daha fazlası...

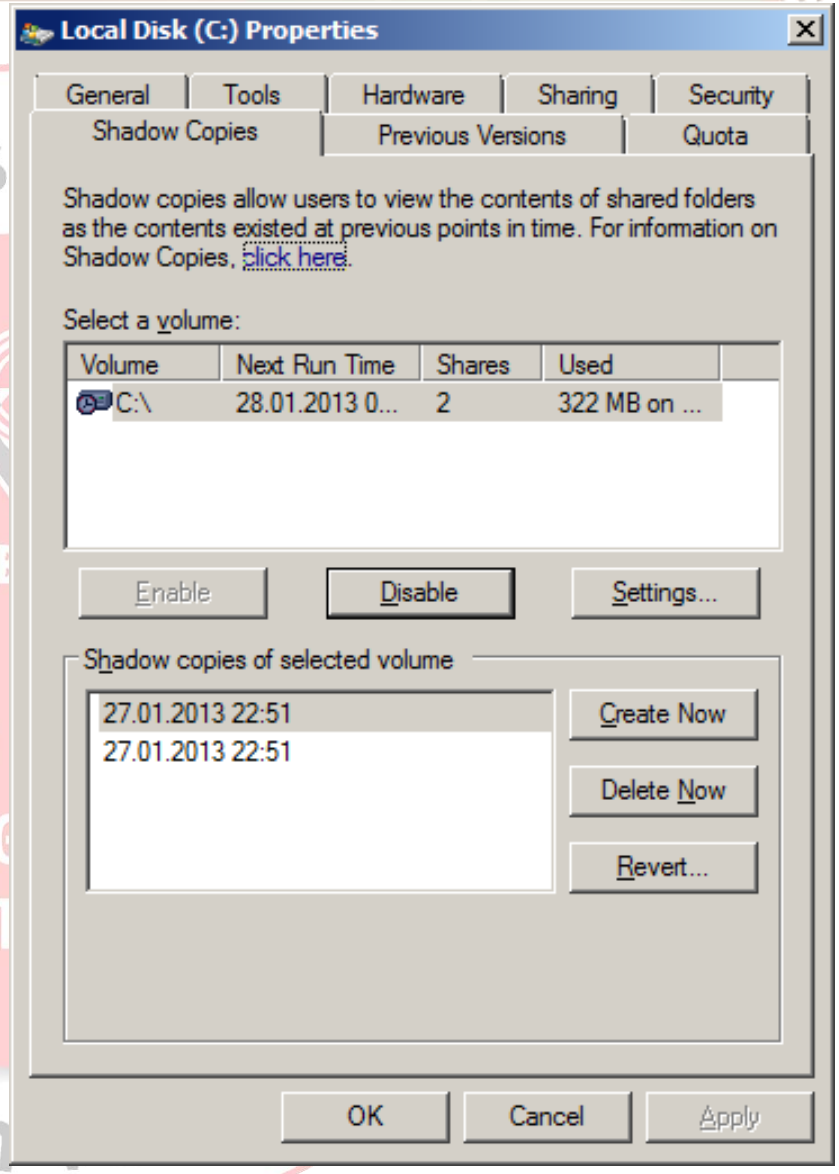
Sistem Geri Yükleme

- **Windows ME, XP, Vista, 7, 8, 10**
- **Sunucu sistemlerde bulunmaz**
- **Zaman Makinası**
  - Sistem dosyaları
  - Registry anahtarları
  - Yüklü programlar

Gölge Kopyalama

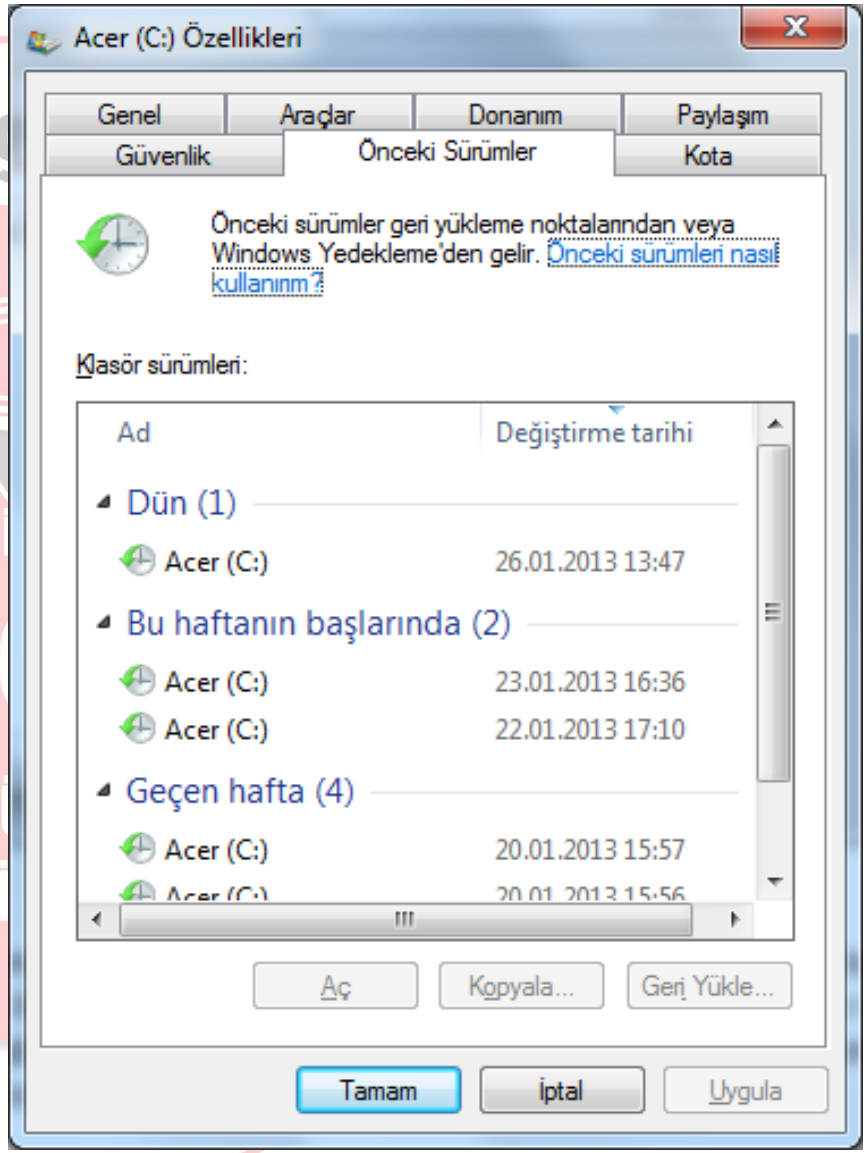
- Yanlışlıkla silinen
- Üzerine yazılan
- Eski hali ile karşılaştırma

Yerel veya ağ üzerinde



Önceki Sürümler

- Vista ve sonrası
- Kullanıcı dosyaları da yedeklenir
- Sistem > Sistem Koruması



File History

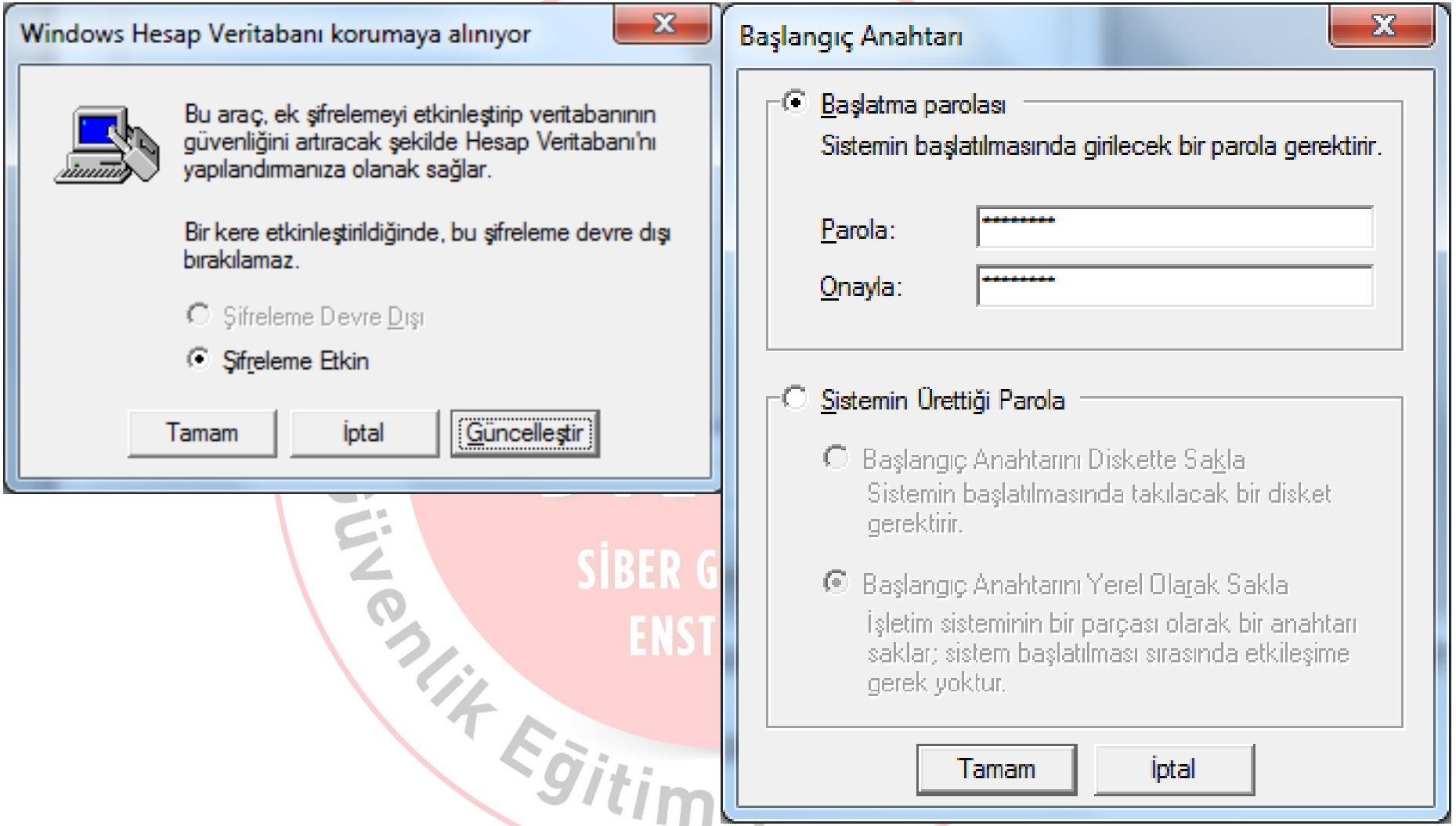
- **Windows 8**
- **Backup & Restore'un yerini almıştır**
- **Değişen dosyaların kopyasını tutar**
  - Tarama, Arama, Önizleme, Geri getirme
- **Yedeklenen alanlar**
  - Kütüphane
  - Kişiler
  - Masaüstü
  - Favoriler

Korunma Teknolojileri

Encrypting File System - EFS

- **Fiziksel saldırılara koruma**
- **Dosya Sistemi Seviyesi Şifreleme**
  - Dosya
  - Klasör
  - Sürücü
  - NTFS 3.0 ve sonrası
- **Saydam şifreleme**
- **Windows 2000 ve sonrası**
- **Grup İlkeleri ile Yönetim,** secpol.msc, gpedit.msc

SYSKEY.EXE



BitLocker

- **Tüm disk şifrelemesi**
  - Kayıp, çalıntı
- **Windows Vista & 7**
  - Ultimate & Enterprise
- **Windows 8**
  - Pro & Enterprise
- **Windows 10**
  - Pro & Enterprise & Education
- **Server 2008, 2008R2, 2012, 2012R2, 2016**
- **AES Şifreleme**
  - 128 || 256 bit

BitLocker

Trusted Platform Module (TPM)

- Açılış dosyaları bütünlük kontrolü
- Tüm disk şifrelemesi

Çok aşamalı kimlik doğrulama

- TPM + Açılış Anahtarı + PIN
- TPM + Açılış Anahtarı
- TPM + PIN
- TPM
- Açılış Anahtarı

Açılış dosyalarının bütünlük kontrolü ***gerçekleştirilmez...***

Kurtarma Anahtarı

- 48 karakterli bir parola
- Tüm diskin şifresi çözülebilir
  - PIN unutulduğunda
  - TPM zarar gördüğünde
  - Açılış Anahtarı kaybedildiğinde
- Aktif Dizin'de depolama

Software Restriction Policies

- Virüslerle mücadele
- Kontrollü ActiveX yükleme
- Yalnızca imzalı betiklerin çalıştırılması
- Yalnızca imzalı yazılımların kurulması
- Dört farklı şekilde yazılım tanımlama
  - Hash
  - Sertifika
  - Yol
  - Alan (Zone)

AppLocker

- **Zararlı yazılım ile mücadele**
- **Yetkisiz yazılım kurulumu ve çalıştırılması**
- **Yazılım kontrol politikasına uyumluluk**
- **Kernel-Mode**
  - Executables (.exe, .com)
  - Dlls (.ocx, .dll)
  - Scripts (.vbs, .js, .ps1, .cmd, .bat)
  - Windows Installers (.msi, .mst, .msp)
  - Packaged app installers (.appx)

Windows Güvenlik Duvarı

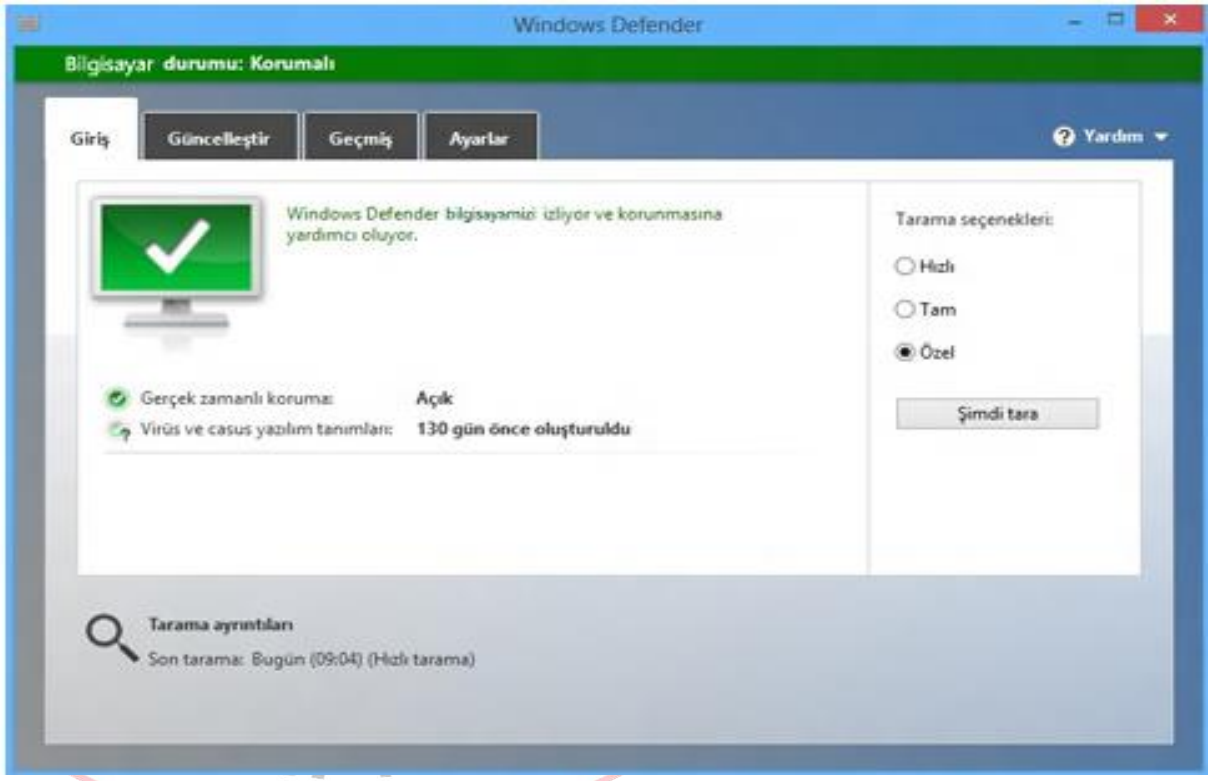
- **Windows XP**
  - Internet Connection Firewall
    - Varsayılan olarak devre dışı
- **Windows XP SP2**
  - Windows Firewall
    - Varsayılan olarak etkin
  - Dahili (Host-based, Stateful)
  - Yalnızca Gelen trafik

Windows Firewall with Advanced Security

- **Windows Vista & 7 & 8 & 10**
  - Gelen ve Giden trafik
  - Network Location Awareness (NLA) ayarları
    - 7 ile birlikte her arayüzde farklı NLA ayarı
      - Ev, İş, Genel
    - İşletim Sistemi parmak izi engelleme
  - IPSec desteği
  - Grup İlkeleri ile yönetim
  - **Netsh** ile komut satırı desteği

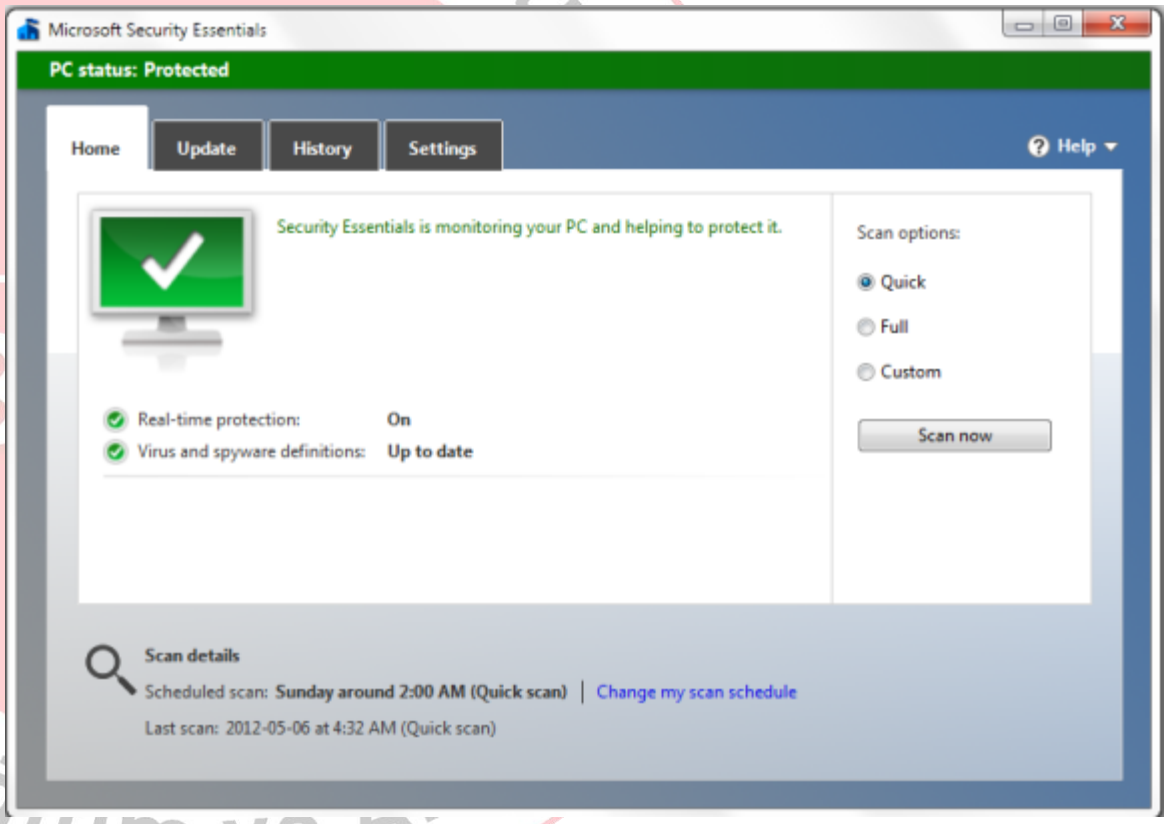
Windows Defender

- Microsoft AntiSpyware ➔ Windows Defender
- Windows Vista & 7 - AntiSpyware
- Windows 8 - Antivirüs
- Windows 10



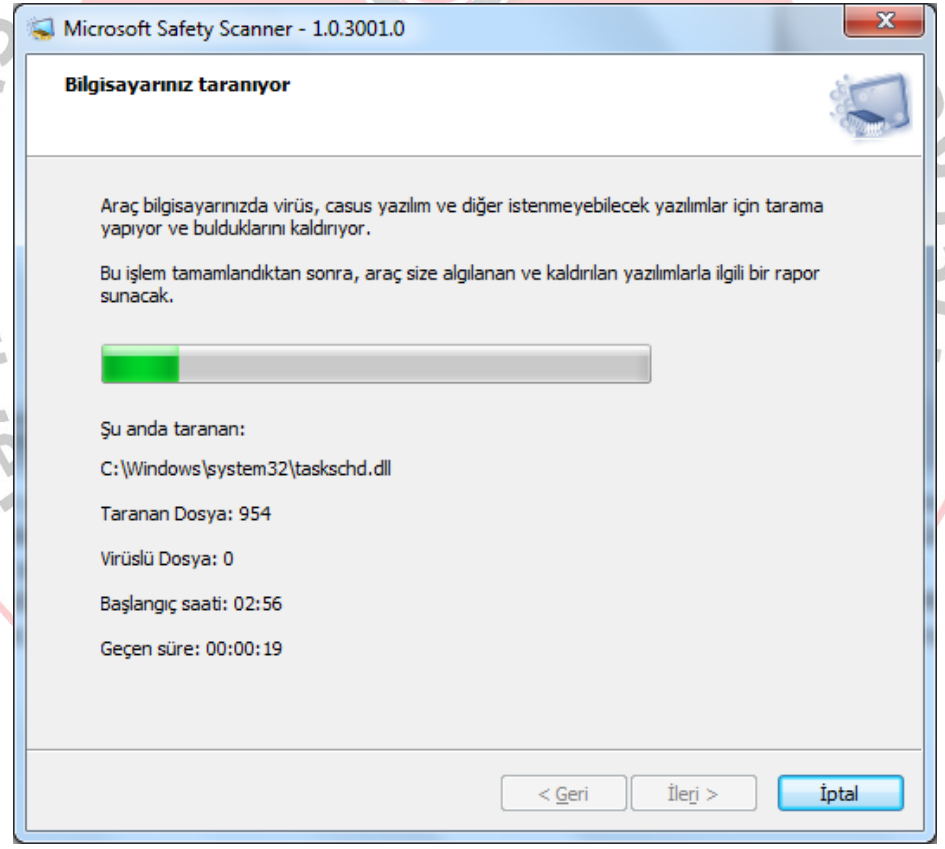
Microsoft Security Essentials

- **Zararlı yazılımlara karşı koruma**
  - Virüsler
  - Casus yazılımlar
  - Rootkit
  - Truva Atları
- **XP, Vista, 7**



Microsoft Safety Scanner

- Ücretsiz güvenlik taraması
- 10 gün sonra sona erer
- Şüphelenilen durumlarda kullanılabilir



Windows SmartScreen

- **Fonksiyonları**
  - Otlama saldırılarına ve zararlılara karşı
  - Zararlılara karşı kullanıcıyı uyarma: Sil – Çalıştır – Kaydet
  - Sahte web sitelerine yönlenen bağlantılar
  - Kara liste kontrolü
- **İlk kez: IE 8**
- 2010'da 1 milyar+ engelleme başarısı
- Windows 8 ile işletim sistemi seviyesinde kontrol
- **Aktivasyon ve Denetim**

Araçlar -> SmartScreen Filtresi

Bütünlük Kontrolü

- **Windows File Protection**
  - Server 2003 & XP
- **Windows Resource Protection**
  - Server 2008 & Vista
- **System File Checker**
  - sfc.exe /SCANNOW
  - sfc.exe /VERIFYFILE
  - sfc.exe /VERIFYONLY

Tarayıcı Güvenliği

- **Muhtemel saldırılara karşı kullanıcıyı uyarma**
  - Smart Screen
  - Protected Mode

IP Security

- **IPSEC**
  - IPv4 & IPv6 desteği
  - Kimlik doğrulama + Bütünlük + Gizlilik
  - Ağ ve taşıma katmanları arasında çalışır
  - IPSec destekli ağ cihazları ve istemcide VPN yazılımı gerekir
- **Protokol bileşenleri:**
  - AH: Bütünlük + Kimlik doğrulama
  - ESP: Kimlik doğrulama(Paketin tamamı) + Bütünlük + Gizlilik
  - IKE: Anahtar değişimi,
  - Anahtar: Manuel veya Sayısal Anahtar

Güvenlik Denetimi ve Sıkılaştırma

Güvenlik Denetimleri

- **Genel tanım:**
  - Önceden tanımlanmış güvenlik kriterleri ile kurulu sistem ya da ağların güvenlik seviyelerinin karşılaştırılması.
- **Amaç:**
  - Kuruluşun, devletin, yerel yönetimin güvenlik politikaları ışığında varlıkların korunmasını sağlamak.
  - Bu varlıkların korunması adına gerekli ihtiyaçların belirlenmesi.
  - Sistem yöneticilerinin hayatını zorlaştırmak.

Güvenlik Denetimleri

- **Ne?**
  - Varolan sistem konfigürasyonlarının güvenliğinin sağlaması
  - Yeni sistemlerin güvenli konfigürasyon ile kurulması
- **Nasıl?**
  - Manuel
  - Otomatik

Grup İlkeleri

- Birden çok bilgisayar
- Yönetimsel kolaylık
- Merkezi yapı
- Hızlı aksiyon alabilme

*** Yapılabilecekler:**

- Parola politikaları
- Masaüstü ayarları
- Oturum açma/ kapama sırasında betik çalıştırabilme
- Uygulama çalıştırma kontrolü
- Ağ trafiğini ve diğer bileşenleri sıkılaştırma

Sunucu Yönetimi (Server Manager)

- **Sunuculardaki sistemlerin durum kontrolü**
- **Merkezi denetim ve yönetim**
  - Rol / Özellik ekleme
  - Kullanıcı / grup denetimi
  - Olay günlüğü yönetimi
  - Performans izleme
  - Zamanlanmış görevleri yönetme
  - Servis izleme

Kontrol Listeleri

Bilgi Güvenliği Kapısı

Tübitak bünyesindeki kontrol denetimleri

Sunucu ve istemcilere yönelik

Güncel zafiyetler, açıklıklar, kavramlar

http://www.bilgiguvenligi.gov.tr/

CIS Security

Dünyaca ünlü kontrol denetimleri

Microsoft Baseline Security Analyzer

- 3 milyon+ / hafta
- IP, IP bloğu, etki alanı bazlı analizler
- Detaylı ve grafiksel HTML raporlama
- **Analizler**
  - Yamalar
  - Yönetimsel Zafiyetler
  - Roller
  - Uygulamalar

CIS-CAT

Center for Internet Security

http://www.cisecurity.org/

- Sunucu ve istemciler için denetim
- Ücretsiz
- Güvenlik şablonları seçimi: EC, SSLF vs..

http://benchmarks.cisecurity.org/downloads/browse

Uygulama – CISCAT

- Uygulama 5 dosyasını indiriniz.

Lütfen uygulamayı tamamlayınız!

Açıklık Taramaları

- Nessus, Nexpose vs..
- Eklenti imkanı
- Taramalar ve Denetim şablonları
- Sonuçları raporlama

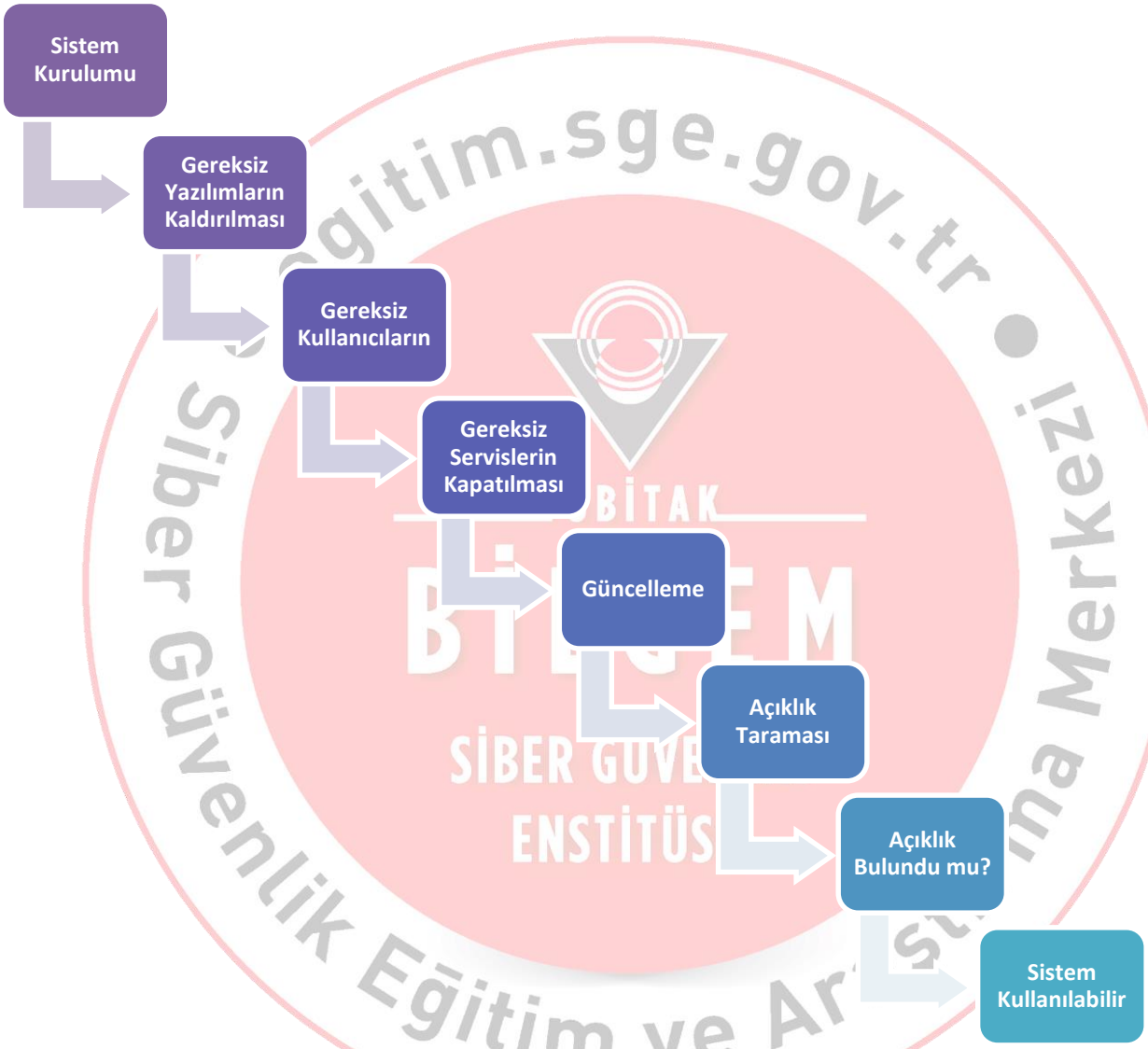
Sistem Görüntüsü Oluşturma

- **Belirli bir zamanda sistemin çalışma anındaki görüntüsü çıkartılır:**
  - İleride alınacak görüntülerle karşılaştırılabilmesi için temel oluşturur.
  - Önce ve sonra karşılaştırılmasına imkan tanır.
  - Sistemin ele geçirildiği tespit edilebilir.
  - Değişiklikleri gösterir.
  - Sorun gidermeye yardımcı olur
  - Yasal delil sunar.

Sistem Görüntüsü Oluşturma

- Kullanıcı Hesapları
- Grup Üyelikleri
- Paylaşılan Klasörler
- Hesap Politikaları
- Kullanıcı Hakları
- Prosesler
- Cihaz Sürücüleri
- Servis Ayarları
- Ağ Yapılandırması
- Açık Portlar
- Çevresel Değişkenler
- Tüm Registry Değerleri
- Tüm NTFS DACLs
- Her Klasörün Boyutu
- IIS Yapılandırma Dosyaları
- Yararlı olabilecek herşey!

Sıkılaştırma



Administrator

- **Yönetici hesabı isimleri değiştirilmiş mi?**
  - Lokal yönetici hesabı ismi “Administrator” değiştirilmiş olmalıdır.
  - Etki alanında(Domain) görev tanımına uygun ve sadece görev tanımı için yeterli haklarla donatılmış yönetici hesapları oluşturulmuş olmalıdır.
  - Kullanıcı SID numaralarını takip eden saldırganlar isim değiştirilmesinden etkilenmezler fakat bu sayede saldırganların büyük çoğunluğunu oluşturan “script kiddie” ve otomatize programlara karşı etkin koruma sağlanmış olunur.

Tuzak Yönetici Hesabı

- **Tuzak Yönetici Hesabı oluşturulmuş mu?**
  - Yerel kullanıcılar arasında Administrator vb. isimli bir kullanıcı oluşturulur.
  - Guests grubuna dahil edilebilir veya hiçbir grup üyesi olmayabilir. (Varsayılan olarak Users grubu)
  - Bu kullanıcının parolası uzun ve karmaşık olarak belirlenir.
  - Bu kullanıcı üzerindeki aktiviteler sisteme sızma denemesi yapanları izlemek için çok kullanışlıdır.

Yönetici Hesapları

- **Yönetici hesapları(Admin) farklılaştırılmış mı?**
  - Sistem üzerinde farklı görev tanımları için farklı yönetici hesapları oluşturulmuş olmalıdır.
  - Sistem yöneticisi ofis işleri için de aynı sunucuyu kullanıyorsa normal kullanıcı ile yönetici hesabı ayrılmalı ve e-mail, doküman okuma/yazma gibi görevler normal kullanıcı ile yapılmalı, yönetimsel işler için "Run As" işlevi kullanılıyor olmalıdır.
- **Güvenlik gruplarının üyeleri uygun mu?**

Misafir (Guest)

- **Misafir (Guest) kullanıcı hesabı devre dışı bırakılmış (disabled) mı?**
- **Gereksiz kullanıcı var mı?**
  - İkili(Duplicate) kullanıcı hesapları
  - Test kullanıcı hesapları
  - Paylaşılan kullanıcı hesapları
  - Genel kullanıcı hesapları
  - İşten ayrılan personelin kullanıcı hesapları

Everyone Grubu

“Everyone” grubuna kesinlikle herhangi bir erişim hakkı verilmemiş olmalıdır

- “Authenticated Users” grubu kullanılmalıdır

Erişim Kontrol Listesi (ACL) ‘nde belirtilen kullanıcı hesaplarının ve grupların erişim hakları görev tanımına uygun ve minimum olmalıdır.

Paylaşımlar

- **Bilgisayarda oluşturulmuş klasör paylaşımları gerekli mi?**
- **Çoğu zaman geçici olarak oluşturulan paylaşımlar unutulur ve yetkisiz erişim için müsait durumda kalır.**
  - Çünkü çoğu zaman erişim kontrol listesi “Everyone” – “Full Control” olarak düzenlenir
- **Mevcut klasör paylaşımlarının erişim kontrol listeleri düzenlenmiş mi?**

Güvenli Ekran Koruyucu

- **Kullanıcılar tarafından atlatılmak istenen özelliklerden bir tanesidir.**

- **Tüm kullanıcı ve sunucu bilgisayarlarında "şifre korumalı" ekran koruyucu bulunmalıdır.**

Şifre Politikası

Kurumun Ağ Güvenliği açısından en kritik bileşenlerinden bir tanesi etkin Şifre Politikalarının uygulanıyor olmasıdır.

- Yazılı Şifre Politikanız var mı?
- Uygulanıyor mu?
- Nasıl zorunlu kılıyorsunuz?
- Şifre politikası, sistemde şifre yönetimi yapılan tüm bileşenleri kapsıyor mu?

Şifre Politikası

İyi bir şifre politikası nasıl olur?

- Kurumun ihtiyaç duyduğu "Güvenlik Seviyesi" göz önünde bulundurulmalıdır.
- Şifrelerin karmaşıklık ihtiyacı belirtilmelidir.
- Şifrelerin minimum uzunluğu belirtilmelidir.
- Şifrenin maksimum geçerlilik süresi belirtilmelidir.
- Şifrenin minimum geçerlilik süresi belirtilmelidir.
- Üst üste kaç yanlış şifre girildiğinde kullanıcı hesabının kilitleneceği belirtilmelidir.
- Kilitli kullanıcı hesabının hangi şekilde açılacağı belirtilmelidir.
- Kullanıcıların ilk şifrelerinin nasıl bildirileceği belirtilmelidir.
- YAZILI OLMALIDIR !
- UYGULANMALIDIR !!
- DENETLENMELİDİR !!!

Şifre Politikası

Öneriler

- Aşağıdaki 4 özellikten “en az” üç tanesini içermelidir.
  - Büyük Harf
  - Küçük Harf
  - Rakam
  - Noktalama İşareti
- En az 1 gün, En fazla 90 gün geçerli olmalıdır.
- En az 8 karakter uzunluğunda olmalıdır.
- Şifrelerinizde Türkçe karakter de “KULLANIN”
- Üst üste 5 yanlış şifre girilmesi durumunda kullanıcı hesabı kilitlenmelidir.
- Sistemin Güvenlik ihtiyacı ve Sistem yöneticisinin iş yoğunluğuna göre kilitli hesabın nasıl açılacağına karar verilmelidir.

Şifre Politikası

- **Grup İlkesi olarak**
  - Computer Configuration
    - Windows Settings
      - Security Settings
        - » Account Policies
          - Password Policy
- **Enforce password history**
- **Maximum password age**
- **Minimum password age**
- **Minimum password length**
- **Password must meet complexity requirements**
- **Store passwords using revirseble encryption**

Denetim Ayarları

- **Sistem genelinde denetleme ayarları etkin değilse, güvenlik ihlallerinde olay takibi zorlaşacaktır.**

- **Kullanıcıların aktivitelerinin yeterli seviyede takip edilebilmesi ve yetkisiz aktivitelerin iz takibinin yapılabilmesi amacıyla yeterli seviyede denetleme ayarları etkin hale getirilmelidir.**

Denetim Ayarları

Sistemde Denetim Kayıtları tutuluyor mu?

Denetim kayıtları, Yerel Güvenlik İlkesi (Local Security Policy) veya Etki Alanı Grup İlkeleri (Domain Group Policy) kullanılarak etkin hale getirilebilir.

- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

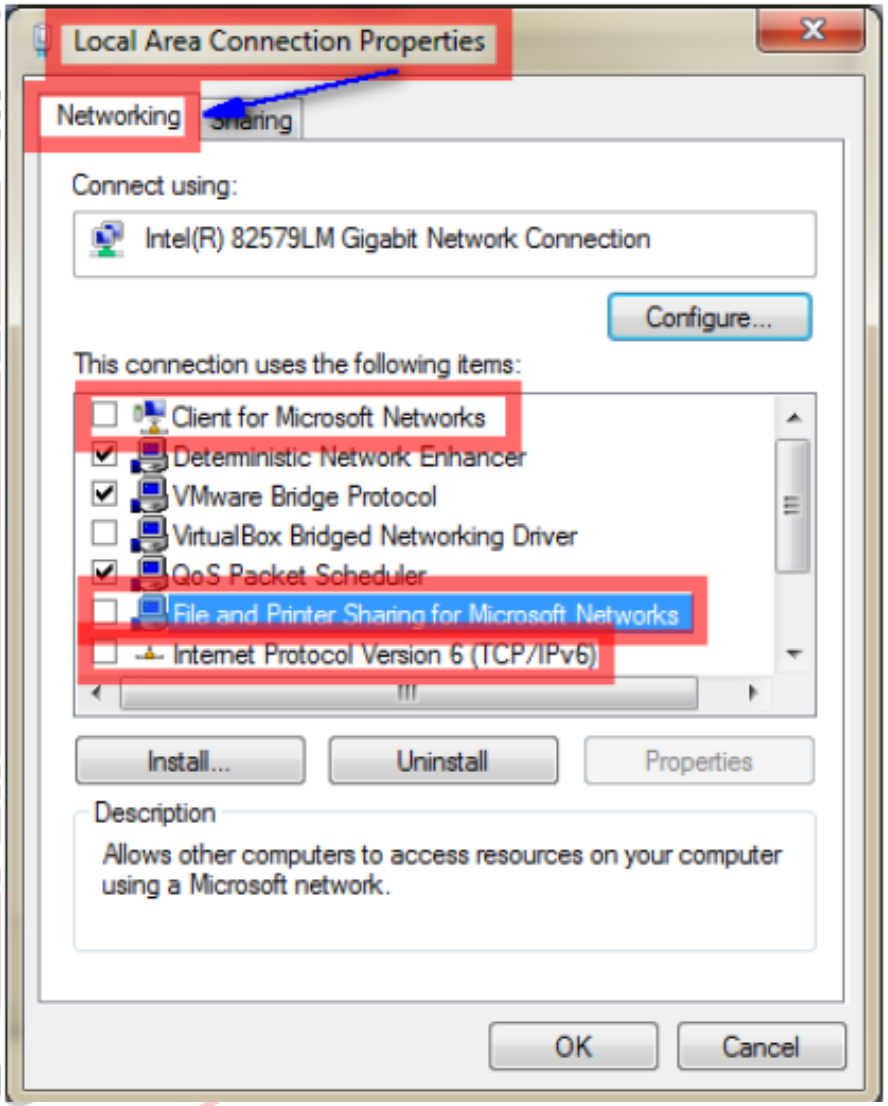
Servisler

Gereksiz servislerin kapatılması

- Remote Registry
- Fax
- Tablet PC Input Service
- IP Helper
- HomeGroup Listener
- HomeGroup Provider
- Vb...

Binding'ler

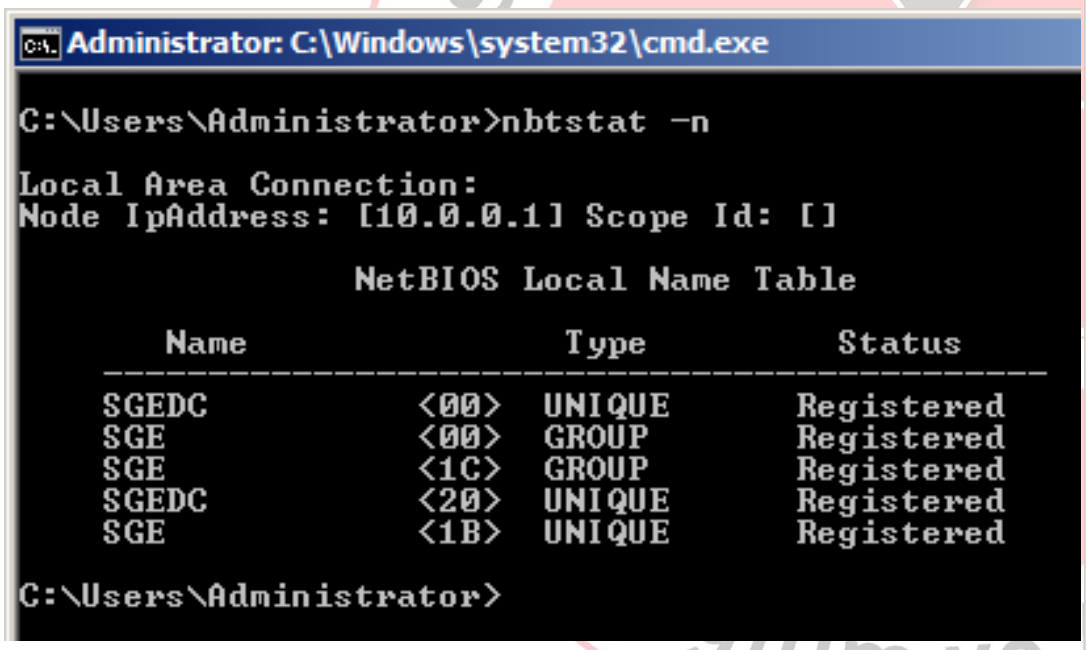
- Client for Microsoft Networks
- File and Printer Sharing
- IPv6

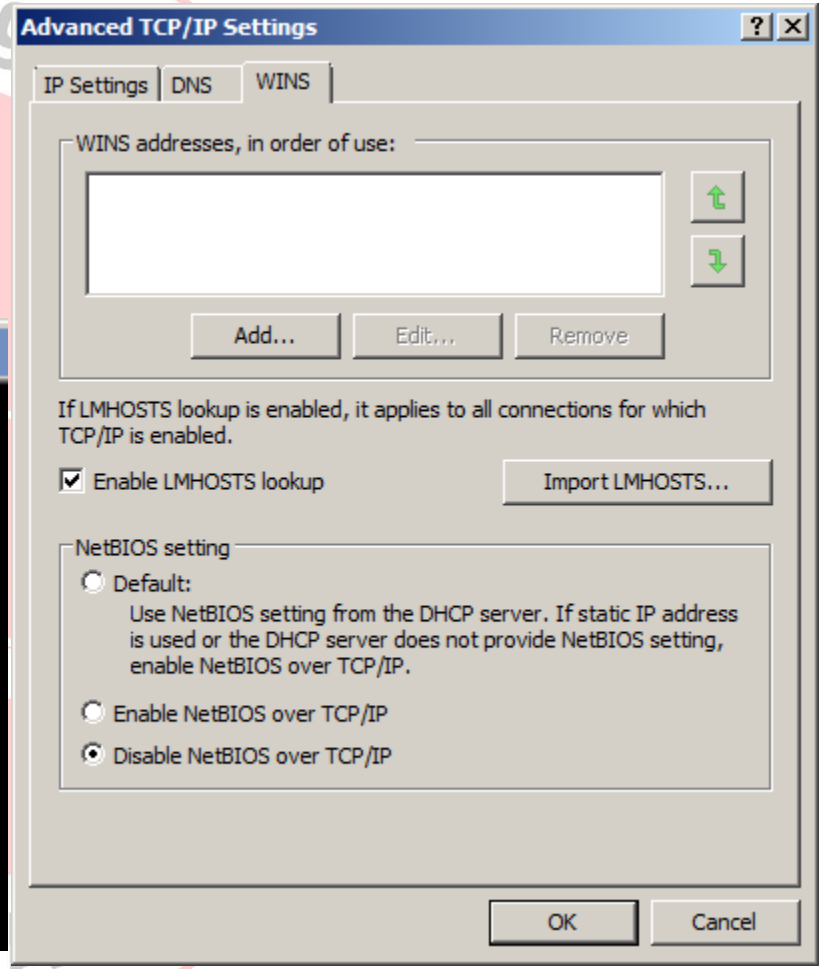


NetBios

- Bilgi toplamada kullanılabilir.
- Devre dışı bırakılması önerilir.

- nbtstat –A xxx.xxx.xxx.xxx





Olay Kayıtları (Event Logs)

- **Türleri**
  - Security
  - Application
  - System
  - Setup
- **Olay Kayıt dosyaları, işletim sisteminden farklı bir sabit disk bölümü üzerinde tutulmalıdır.**
- **Olay Kayıt dosyalarının saklama metoduna uygun olan bir yedekleme planı bulunmalı ve dosyaların yedeği alınmalıdır.**
- **Olay kayıtları düzenli olarak izlenmelidir.**

Faydalı Araçlar

Otomatikleştirme

Arayüz aracılığıyla yapılan işlerin neredeyse %95'i betiklerle de yapılabilir:

- Betikler
  - Batch
  - VBScript
  - Powershell
- Zamanlanmış Görevler

Taramalar

Analizler

Denetlemeler

Batch

- **Kelime Anlamı:** Grup, harman, sürü, toplu iş, yığın.
- **.bat, .cmd veya .btm dosyaları cmd.exe** tarafından satır satır yorumlanır.

Komut Satırı Komutları

- WMIC.EXE
- GPRESULT.EXE
- IPCONFIG .EXE
- NSLOOKUP.EXE
- NETSH.EXE
- NET.EXE
- NETSTAT.EXE
- /?
- http://ss64.com/nt/

VBScript

- **Batch'den daha güçlü**
- **.vbs, .vbe, .wsf, .wsc**
  - Wscript.exe
  - Cscript.exe

Powershell

- **COM ve WMI nesnelerine tam erişim**
- **.NET Framework ile entegre çalişabilir**
- **cmdlets**
  - SET-
  - GET-

Zamanlanmış Görevler

- Özel bir durum olduğunda
- Event Log düştüğünde
- Belirli bir zamanda
- Bilgisayar boştayken
- Sistem baştan başlatıldığında
- Kullanıcı oturum açtığında

schtasks.exe

Teşekkürler