ACTIVE DIRECTORY TEMEL KAVRAMLAR

Microsoft, Windows NT'nin ardından çıkardığı Windows 2000'le birlikte yeni bir directory sistemi olarak Active directory sistemini geliştirdi. Active directory, network üzerindeki nesneler hakkında bilgileri saklayan ve bu bilgileri kullanıcılar, network yönetimi ve güvenlik için kullanmamızı sağlayan bir servistir. Aktif dizin bünyesinde kullanıcılar, gruplar ve yapılandırma bilgileri gibi pek çok öğeyi barındır.

Aktif dizin üzerinde tutulan temel nesneler aşağıdaki gibidir:

- Kullanıcılar (kullanıcı hesapları)
- Gruplar (yöneticiler, operatörler, kullanıcı grupları vb.)
- Bilgisayarlar
- Yazıcılar
- Sunucular
- Etki alanları
- Site'lar

Active Directory Ne Sağlar?

Active directory'nin a yönetiminde kullanılan bir yönetim sistemi olduğunu ve network üzerindeki kaynakları yönettiğinden söz ettik. Örneğin şirket agı içinde; bir dosyaya erişecek (izinleri olan) kullanıcıların tanımlanması gibi. İzinlerin yanı sıra Active directory'de önemli şey kimlik denetimi (authentication) işlemidir. Kimlik denetimi sisteme giriş ve yapılan işlemleri kullanıcı bazında kısıtlanmasında diğer bir deyişle yalnızca yetkili kullanıcıların agı kullanmasını sağlar.

Active Directory'nin Sağladıklarını Şu Şekilde Sıralayalım:

- Network'ün domain olarak adlandırılan birimler (alanlar) halinde düzenlenmesini sağlar.
- Kullanıcı ve grupların listesini merkezi olarak tutar.
- Kimlik denetimi (authentication) sağlar: Kullanıcı ve grupların ancak gerekli izinlere sahip olması durumunda kaynaklara erişmesini sağlar.
- Domain içindeki nesnelere, birçok özelliklerinden aranarak bulunmasını sağlar.
- Domainin OU adı verilen alt parçalara bölünmesini sağlar. Daha küçük bu birimler, yönetimin delege edilmesini sağlar.
- Merkezi yönetim
- Ölçeklenebilirlik
- DNS ile entegrasyon
- Politika-tabanlı yönetim
- Multi-master replikasyon
- Esnek kimlik doğrulama ve yetkilendirme
- Diğer dizin servisleriyle birlikte çalışabilme
- İmzalanmış ve şifrelenmiş LDAP trafiği

Betikler ile Yönetim

Active directory bir database olarak gibide düşünülebilir. Active directory tek bir noktadan yönetim olanağı sağlar. Kullanıcıların tek bir oturumla dizin kaynaklarına erişebilmesine imkan verir.

Active Directory Özellikleri

Active Directory Belli Özelliklere Sahiptir:

- Merkezi veri depolama: Active directory'de sistemde yer alan tüm veriler tek bir veritabanında saklanır. (NTDS.DIT). Merkezi bir veritabanı sayesinde kullanıcılar istedikleri nesneye kolayca erişebilirler.

- Ölçeklenebilirlik: Active directory, farklı network gereksinimlerini karşılamak üzere ölçeklenebilme (scalability) yeteneğine sahiptir. Domain, OU ve tree yapıları sayesinde küçük, orta ve büyük ölçekli kurumsal aglara uygulanabilir.

- Genişletilebilirlik: Active directory veri tabanının yapısı genişletilebilme özelliğine sahiptir. Belli bir şemaya sahip olan veri tabanına ek özellikler eklenebilir.

- Hiyerarşik: Domain yapısı hiyerarşiktir. Bu aynı zamanda hiyerarşik bir adlandırma sistemini de destekler. DNS domainleri gibi internet modeliyle domainlerin adlandırılmasını sağlar. cy-holding.com, izmir.cy-holding.com gibi.

- Yönetilebilirlik: Active directory domainleri sistem yöneticisi tarafından birçok araçla yönetilebilir. Bu işlemler bir yerden ve bir logon ile (single sign on) yapılabilir.

- Domain Name System (DNS) ile entegrasyon: Active Directory, standart bir bir Internet (TCP/IP) servisi olan DNS ile entegre çalışır. Her ikisi de aynı hiyerarşik adlandırma yapısını kullanır. Özellikle adlandırma (adların çözülmesi) ve içerdiği server kayıtları aracılığıyla serverların bulunması işlemlerinde DNS önemli bir servistir. Politika-tabanlı yönetim: kullanıcı ve bilgisayarların bir site, domain ya da OU içerisindeki işlemlerini kısıtlayan merkezi politikalar düzenlenebilir. Böylece kullanıcıların yalnızca izin verilen işlemleri ve bilgisayar ayarların yapması sağlanır.

- Bilginin kopyalanması (replication): Active directory bilgilerinin sürekliliğini, hataya dayanıklılığını ve yük dengelemesini sağlamak için gelişmiş bir replikasyon teknolojisine sahiptir. Bu sayede domain controller bilgisayarlar arasında domain nesneleri (veriler) kopyalanır.

Active Directory sistemi belli teknolojilere dayanır:

- Esnek ve güvenli kimlik doğrulama (yetkilendirme): Active directory birçok kimlik doğrulama protokolünü kullanır. Kerberos v5, SSL v3 ve TLS v3 sertifikaları bunlardan bazılarıdır.

- Güvenlik entegrasyonu: Active directory, Windows Server 2012 güvenliği ile entegre çalışır. Dizinde yer alan her bir nesne için erişim kontrol edilebilir.

- Diğer dizin servisleriyle birlikte çalışabilme: Active directory LDAP v3 ve NSPI üzerine kuruludur. Bu protokolleri kullanan diğer dizin servisleriyle birlikte çalışabilir. İmzalanmış ve şifrelenmiş LDAP trafiği: Varsayım olarak tüm LDAP trafiği sayısal olarak imzalı (signed) ve şifrelidir (encrypted).

- Tek bir noktadan erişim: "Single Sing On". Tek bir logon ile bütün aga erişim. Administrator'ün bir yerden yapacağı logon işlemi ile bütün agı yönetmesi anlamına gelir.

- Delegasyon: OU'lar sayesinde yönetim işlemlerinin bazıları (password değiştirmek, kullanıcı oluşturmak günlük işlemler) yerel birimlerdeki (OU) yetkili bir kullanıcıya devredilebilir.

Active Directory Destekli Teknolojiler

Active directory'nin amacı standart bir sistem yönetimi (network yönetimi) sağlamaktır. Bu amaçla, Active directory tasarımında belli standartlar söz konusudur. Active Directory'nin desteklediği teknolojiler şunlardır:

DHCP

- DHCP (Dynamic Host Configuration Protocol) servisi IP adreslerinin merkezi olarak dağıtılmasını sağlar. DHCP servisi, DNS ile (Dinamik DNS) birlikte Active Directory sistemine destek olur.

DNS

- DNS (Domain Name System) servisi ise domain adlarının temelini oluşturur. Ayrıca domain controller, üye bilgisayarlar ve client bilgisayarların kayıtları DNS üzerinde tutulur.

LDAP

- LDAP (Lightweight Directory Access Protocol), endüstri standardı olmuş bir directory erişim protokolüdür. Active Directory bilgilerine erişim sağlar. Active directory "LDAP" uyumlu bir veritabanıdır. Active Directory'nin veritabanı "ntds.dit" dosyasıdır. Active directory kullanılan bir sistemde "ntds.dit" dosyasının yedeğinin alınması gerekmektedir.

Kerberos v5

- Kerberos v5, domain içinde kimlik doğrulama (authentication) için kullanılan standart bir protokoldür. Kerberos v5 protokolü kullanıcıyı ve network servislerini tanımlar. Kerberos v5 kimlik doğrulama sistemi network servislerine erişim için ticket bilgisini kullanır. Bu bilgiler şifrelenmiş verilerdir. Kerberos v5 servisinin önemli bir kısmını Key Distribution Center (KDC) oluşturur. KDC, her Domain Controller üzerinde Active Directory servisinin bir parçası olarak çalışarak parolaları ve diğer hesap bilgilerini saklar.

Active Directory Bilinmesi Gereken Kavramlar

Organizational unit (Ou) nedir?

- Organizational unit (Ou) domain içerisinde kullanıcı, grup ve bilgisayarların yer aldığı konteynerlardır.

Organizational unit (Ou)'ların kullanım alanları:

- Yönetimi delege etmek
- Group policy sayesinde kısıtlamalar yapmak
- Nesneleri saklamak

Distinguished Name Nedir?

- Active directory içindeki her bir nesne kendisini ayırt edecek bir ada sahiptir. Bu ada "distinguished name" denir. Distinguished adlar nesnenin bulunduğu domain'i tanımlar.

Principal Name Nedir?

- User principal name kullanıcını logon adı ve domain adından oluşur. Örneğin nedir.com domaini içindeki Eray adlı kullanıcın'ın adı can@test.com olabilir. User principal name network'e dahil olmak için kullanılanılır.

Globally Unique Identifier Nedir?

- Windows 2000 yaratılan her bir nesneye 128-bitlik bir GUID (Globally Unique Identifier) atar. GUID, tek bir tane olduğu garanti edilen 128-bit'lik numaradır. Nesneler oluşturulduğunda atanmış bir GUlD'e sahip olurlar. Nesne yer değiştirmiş de olsa adı da değiştirilse GUID hiç¬bir zaman değiştirilemez. Uygulamalar nesnenin GUlD'ini saklayabilir ve o anki domain bilgisi ne olursa olsun nesneye erişim kesinleşir.

Kerberos Nedir?

- Kerberos domain içinde kimlik doğrulama (authentication) için kullanılan bir kimlik doğrulama protokolüdür.

ACTIVE DIRECTORY'NIN SIKILAŞTIRILMASI

Active Directory Kontrol Maddeleri:

BT yapılarında büyük oranda kabul görmüş olan Microsoft Active directory servislerine (Directory Services) yönelik gerçekleştirilen dış ve iç ataklar, büyüyen ve gelişen BT dünyasında popülerliğini korumaya devam ediyor. Şirketlerin kimlik yönetimi ve doğrulama süreçlerinde kritik görevler üstlenen Active directory servisleri, uzun süredir dış ve iç saldırılara karşı korunması gereken en önemli bileşenlerden biri durumunda.

Aktif Dizin üzerindeki nesnelerin güvenilir bir şekilde yönetilmesi için bir takım kontrol maddeleri bu başlık altında belirtilmiştir. Kontrol maddelerinde ne yapılması gerektiği üzerinde durulmuş olup, Kontrol maddelerinde belirtilen nesnelerin otomatik olarak nasıl tespit edileceği ile ilgili internet üzerinde - başta Powershell olmak üzere - bir çok betik bulunabilir. Ayrıca aşağıdaki maddeleri ve çok daha fazlasını gerçekleştirebilen otomatik denetim araçları da kullanılabilir.

Denetim sonucunda gerçekleştirilmesi gereken işlemler kurum politikasında belirtilmelidir. Örneğin, uzun süre oturum açmayan kullanıcı hesapları tespit edildikten sonra bu hesaplar belli bir süre boyunca devre dışı bırakılabilir ve bir süre sonra da tamamen silinebilir. Benzer olarak tespit edilen nesnelerin ne zaman, hangi kullanıcı tarafından oluşturulduğu da incelenebilir.

Not: PowerShell Windows ile birlikte kurulu halde gelmektedir. Komutlarını çalıştırabilmek için policy ayarlaması yapılması gerekmektedir.

Active Directory Kullanıcı Hesapları ile ilgili Kontrol Maddeleri:

Saldırı yüzeyi içeren kullanıcılar, bilgisayar hesapları, gruplar, OU'lar tespit edilerek ilgili aksiyon değerlendirilmeli ve önlemler uygulanmalıdır.

Ortak Hesap Kullanan Kullanıcı Hesaplarının Tespit Edilmesi:

- Ortak hesap kullanımı özellikle yardım masası veya teknik destek gibi vardiyalı çalışan bölümlerde sık karşılaşılabilen durumlardandır. Kurum içerisinde ortak kullanılan kullanıcı hesapları tespit edilmelidir. Aksi halde işlemi gerçekleştiren kullanıcının kimliğinin tespit edilmesi kayıdı tutulan başka faktörlerle (IP adresi, çalışılan saat dilimi, …) mümkün olabilmektedir.

Uzun Süredir Oturum Açmamış Kullanıcı Hesaplarının Tespit Edilmesi

- Kurum içerisinde uzun bir süre (3 hafta gibi) oturum açmayan kullanıcı hesapları tespit edilmelidir. Bu süre kurum politikasına göre değişiklik gösterebilir. Tatil izinleri, yurt dışı gezileri gibi durumlar göz önüne alınarak bu süre ve kapsam belirlenmelidir.

- **Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 | where {$_.ObjectClass -eq 'user'} | FT Name,ObjectClass –A**

Parolasını Hiç Değiştirmemiş Olan Kullanıcı Hesaplarının Tespit Edilmesi:
Birçok kurumda bir kullanıcı hesabı oluşturulurken standart bir parola ile oluşturulurlar. Bu parola o hesabın sahibi olan kullanıcı tarafından ilk oturumda değiştirilmesi gerekmektedir. Parolasını hiç değiştirmemiş olan kullanıcı hesapları tespit edilmelidir.

- **Search-ADAccount -PasswordNeverExpires | FT Name,ObjectClass -A**

Uzun Süredir Parolasını Değiştirmeyen Kullanıcı Hesaplarının Tespit Edilmesi:
Kurum politikasına uygun olacak şekilde kurum içerisinde bir parola politikası oluşturulmalı ve uygulanmalıdır. Parola politikasında parola değiştirme süresi için uygun bir değer verilmelidir. Belirlenen süre boyunca parolasını değiştirmeyen kullanıcı hesapları tespit edilmelidir. Uzun süredir parolasını değiştirmeyen ve parolası saldırganlar tarafından bir şekilde ele geçirilmiş olan bu kullanıcı hesapları etki alanına karşı gerçekleştirilebilecek sonraki saldırılarda kullanılabilmektedir.

- **Search-ADAccount –PasswordExpired**

Passwordu Expire Olmuş Kullanıcıları Listeler.

- **Get-ADUser -filter {Enabled -eq $True -and PasswordNeverExpires -eq $False} –Properties "DisplayName", "msDS-UserPasswordExpiryTimeComputed" | Select-Object -Property "Displayname",@{Name="ExpiryDate";Expression={[datetime]::FromFileTime($_."msDS-UserPasswordExpiryTimeComputed")}}**

Şifrelerin expire tarihlerini listeler.

Parolasını Değiştiremeyen Kullanıcı Hesapları:
Uygulama/servis kullanıcıları veya belirli sebeplerle bazı kullanıcı hesaplarının parolalarının değiştirilmemesi gerekebilmektedir. Parolasını değiştiremeyen kullanıcı hesapları tespit edilmelidir.

- **Get-ADUser -Filter * -Properties CannotChangePassword -SearchBase "DC=mydomain,DC=com"| where {$_.CannotChangePassword} | sort-object {$_.samAccountName} | Select samAccountName**

Parola Değiştirmesi Zorunlu Olmayan Kullanıcı Hesapları:
Başta uygulama ve servis kullanıcı hesapları olmak üzere, parola politikasına rağmen parola değiştirmesi zorunlu olmayan kullanıcı hesapları tespit edilmelidir.

- **Search-ADAccount -PasswordNeverExpires | FT Name,ObjectClass -A**

Parolası Sona Ermeyen Kullanıcı Hesapları
Parola politikasına rağmen parolası sona ermeyen kullanıcı hesapları tespit edilmelidir. Özellikle uygulama ve servis kullanıcı hesaplarında görülen bu durum saldırı yüzeyini arttırmaktadır.

- **Search-ADAccount -PasswordNeverExpires | FT Name,ObjectClass -A**

Süresi Geçmiş Kullanıcı Hesaplarının Tespit Edilmesi:
Kurum politikası gereği bazı kullanıcı hesapları (danışman, sistem destek, stajyer vs) süreli olarak oluşturulabilmektedir. Bu süre sonrasında bu hesaplar ile işlem yapılamamaktadır. Kurumda süresi geçmiş olan (expire) kullanıcı hesapları tespit edilmelidir.

- **Search-ADAccount –AccountExpired**

İşten Ayrılmış Kullanıcı Hesaplarının Tespit Edilmesi
Kurumların çoğunda merkezi kimlik yönetimi henüz tam anlamıyla aktif bir şekilde kullanılmamaktadır. İşten ayrılmış olan kullanıcı hesabı ile gerçekleştirilebilecek işlemler sonucunda kurum ve kurum çalışanları zor durumda kalabilmektedir. Bu sebeple, kurum ile ilişkisi kesilen kullanıcı hesapları tespit edilmelidir. Bunun yanında yetkilendirme işlemleri için kullanıcıdan bağımsız tasarımların kullanılması güvenliği arttırmaktadır.

- **Kurum Personeli Olmayan Kullanıcı Hesaplarının Tespit Edilmesi**

Danışmanlık, sistem destek, stajyerlik gibi sebeplerle etki alanında oluşturulan kullanıcı hesapları tespit edilmelidir. Bu hesaplar oluşturulurken süreli bir şekilde oluşturulması tavsiye edilmektedir. Ayrıca bu hesaplar için özel yapısal birimlerin (OU) oluşturulması ve bu OU altındaki nesnelere sıkılaştırılmış grup ilkelerinin uygulanması tavsiye edilmektedir.

Users" Konteynırında Bulunan Kullanıcı Hesaplarının Tespit Edilmesi
Bir kullanıcı oluşturulduğunda varsayılan olarak "Users" adlı verilen konteynır altında oluşmaktadır. Bir konteynır içerisindeki nesnelere varsayılan grup ilkeleri uygulandığı için "Users" altında kullanıcı hesabının bulunması kontrol eksiliğine sebep olmaktadır. Bu sebeple, "Users" konteynırında bulunan kullanıcı hesapları tespit edilmelidir. Etki alanına yeni eklenen kullanıcı hesapları üzerindeki denetimleri arttırmak için ve etki alanına eklenen ancak henüz faal olmayan nesneleri daha iyi takip edebilmek için; bu hesapların sıkılaştırılmış bir OU altında oluşturulması tavsiye edilmektedir. Kullanıcı hesabı ile işlem yapıldıktan ve grup ilkesi alındıktan sonra ilgili OU altına eklenmesi güvenliği arttırmaktadır.

- **Dial-in Bağlantı Hakkı Olan Kullanıcı Hesaplarının Tespit Edilmesi**

Dial-in bağlantı hakkı olan kullanıcılar tespit edilmelidir. Uzak erişimler için dial-in bağlantı yerine kurum ihtiyacına daha güvenilir bir şekilde vap verecek yöntemler (SSL VPN gibi) tercih edilmelidir.

- **Get-ADUser -IncludeAllProperties | ?{$_.msNPAllowDialin -eq $true} |Select Displayname,mailnickname**

İsimlendirme Standardına Uymayan Kullanıcı Hesaplarının Tespit Edilmesi:
Kurum politikası gereği kullanıcı hesaplarının nasıl oluşturulacağı belirlenmelidir. Personelin ad ve soyadının farklı şekillerde kullanılması (can.yoleri, cyoleri, c.yoleri, yoleri.can…) bir standart olarak belirlenmelidir. Bunun yanında aynı isim ve soy isme, iki ve daha fazla isme veya soy isme sahip personel için de standartın oluşturulması tavsiye edilmektedir. Belirlenen isimlendirme standardına uymayan kullanıcı hesapları tespit edilmelidir.

Kritik Gruplara Üye Olan Ortak Kullanılan Kullanıcı Hesaplarının Tespit Edilmesi:
Etki alanında bazı grupların yetkileri diğerlerinden daha fazla öneme sahip olmaktadır. Bu gruplardan bazıları yerleşik (built-in) gruplar (Domain Admins, Enterprise Admins, …) olablildiği gibi, bazı gruplar (Oracle Admins, Microsoft Sistem Yöneticileri, Aktif Cihaz Yönetim Grubu,…) ise daha sonradan oluşturulmuş olabilir. Etki alanında kritik yetkilere sahip olan gruplar belirlenmeli ve bu gruplara üye olan kullanıcı hesapları tespit edilmelidir.

- **Get-ADGroupMember "Domain Admins" | select name,distinguishedName**

Hiçbir Gruba Üye Olmayan Kullanıcı Hesaplarının Tespit Edilmesi:

- **$DomainsAdminsDn = (Get-ADGroup 'Domain Admins').DistinguishedName Get-ADUser -Filter { -not (memberof -eq $DomainsAdminsDn) } # OR Get-ADUser -LDAPFilter "(!(memberof=$DomainsAdminsDn))"**

Üyesi Olmayan Grupların Tespit Edilmesi
İçerisinde hiçbir üyesi olmayan, boş gruplar tespit edilmelidir.

- **Get-ADGroup -Filter {GroupCategory -eq 'Security'} | ?{@(Get-ADGroupMember $_).Length -eq 0}**

Uzun Süredir Kullanılmayan Bilgisayar Hesaplarının Tespit Edilmesi:
Kullanıcı hesaplarında olduğu gibi, uzun süredir kullanılmayan bilgisayar hesapları tespit edilmelidir.

1. $then = (Get-Date).AddDays(-60)

2. Get-ADComputer -Property Name,lastLogonDate -Filter {lastLogonDate -lt $then} | FT Name,lastLogonDate

Devre Dışı Bırakılmış Bilgisayar Hesaplarının Tespit Edilmesi
Kullanıcı hesaplarında olduğu gibi, devre dışı (disabled) bırakılmış olan bilgisayar hesapları tespit edilmelidir.

- **Get-ADComputer -ldapFilter '(userAccountControl:1.2.840.113556.1.4.803:=2)'**

"Computers" Konteynırında Bulunan Bilgisayar Hesaplarının Tespit Edilmesi

- **Get-ADComputer -Filter * -Properties MemberOf | Where-Object { $_.MemberOf -NotIn "{CN=GROUP NAME,OU=Computer Groups,OU=Groups,DC=DOMAIN,DC=local}" }**

İçerisinde Nesne Bulunmayan Yapısal Birimlerin Tespit Edilmesi
Gruplarda olduğu gibi, içerisinde hiçbir üyesi olmayan, boş yapısal birimler (OU) tespit edilmelidir.

- **Get-ADOrganizationalUnit -Filter * | Where-Object {-not (Get-ADObject -Filter * -SearchBase $_.Distinguishedname -SearchScope OneLevel -ResultSetSize 1)}**

Site İçerisinde Belirtilmemiş Olan Yerel Ağların Tespit Edilmesi:
Site, birbiri ile ağ iletişimi kuvvetli olan fiziksel yapılardır. Site, ağın hızına ve trafik kapasitesine göre tasarlanır. Özellikle oturum açma ve replikasyon işlemlerinin daha hızlı gerçekleşebilmesi için Site yapısının iyi tasarlanması gerekmektedir. Bir Site içerisinde bir veya daha fazla alt ağ (subnet) bulunabilmektedir. Böylece bir kullanıcı aynı site içerisinde bulunduğu etki alanı denetleyicisini (DC) kullanarak kimlik doğrulatır. Benzer olarak bir etki alanı denetleyicisi aynı site içerisindeki bir etki alanı denetleyicisi ile replikasyon işlemini gerçekleştirmek için oluşturulan Site ve Subnet bilgilerini kullanılır. Aynı site içerisinde etki alanı denetleyicisi bulunamazsa, farklı site üzerindeki etki alanı denetleyicisi arayışında bulunulur.Kurum içerisindeki her bir yerel ağ (LAN), içerisinde etki alanı denetleyicisi bulundurmasa dahi, Aktif Dizin üzerinde tanımlanması tavsiye edilmektedir. Bu sebeple, Site içerisinde belirtilmemiş yerel ağlar tespit edilmelidir.

DNS Üzerinde Kaydedilmemiş Yerel Ağların Tespit Edilmesi:
Alan Adı Sistemi (Domain Name System - DNS); ağdaki bilgisayarları ve ağ hizmetlerini adlandırmak için kullanılan bir sistemdir. DNS, Aktif Dizin yapısı için zorunlu bir roldür. Microsoft ortamlarında, istemciler ağdaki etki alanı denetleyicilerinin ve diğer servis sunucularının yerlerini DNS kullanarak tespit ederler. Eğer DNS üzerinde bir problem oluşursa, erişimlerde problem yaşanacaktır. Aktif Dizin ile entegre olarak oluşturulan Microsoft DNS üzerinde tüm yerel ağlara ait kayıtların bulunması tavsiye edilmektedir. Bu sebeple, DNS üzerinde kayıtlı olmayan kuruma ait yerel ağlar tespit edilmelidir.

BIOS Yapılandırma Kontrol Maddeleri
Fiziksel saldırının gerçekleştirilememesi için, yerel kullanıcı bilgilerinin SAM dosyasından alınamaması sağlanmalıdır. Yerel kullanıcıların bilgileri, çevrimiçi olarak yerel yönetici haklarıyla elde edilebileceği gibi çevrimdışı yollarla da bir işletim sistemi kullanılarak gerçekleştirilebilir. Bu amaçla, kullanıcılar yerel yönetici haklarına sahip olmamalı ve BIOS ayarları uygun şekilde yapılandırılmalıdır. BIOS ayarlarının yapılandırılması için, en az aşağıdaki ayarların uygulanması gerekmektedir.

Bilgisayarın BIOS ayarı yapılandırılmasında parola koruması eklenmelidir. Bu parolalar oldukça karmaşık ve her bilgisayar için farklı olması tavsiye edilmektedir. Bilgisayarın pili çıkarıldığında BIOS şifresinin sıfırlanmaması için özel donanımlar tercih edilmelidir. Bilgisayarın BIOS ayarı kontrol edilmeli ve öncelikle hard diskten başlatıldığından emin olunmalıdır. Bilgisayarlar çevrim dışı olarak açıldığında içerisindeki verilere erişilememesi için, BitLocker gibi çözümler kullanılarak tam disk şifreleme gerçekleştirilmelidir. Böylece disk içerisindeki veriler okunamayacaktır.

Yerel kullanıcıların bilgilerine erişilebilse bile, parolanın açık halinin elde edilememesi için hem LM özetlerinin kaydedilmemesi hem de parola oldukça karmaşık olarak belirlenmesi gerekmektedir. Ancak Windows işletim sistemindeki kimlik doğrulama mekanizmalarındaki zayıflıktan dolayı parolaların açık hali elde edilmeden de, parola özetleri kullanılarak diğer bilgisayarlara yayılma gerçekleşebilir. Bu sebeple, üst taraftaki operasyonlar gerçekleştirilerek SAM dosyasına erişilememesi sağlanmalıdır.

Ağ Yapılandırma Kontrol Maddeleri
Ağ taraması sonucunda olabildiğince az bilginin açığa çıkarılması sağlanmalıdır. Bu amaçla ağ ayarları sıkılaştırılmalı ve yapılandırılmalıdır. Ağ ayarlarının yapılandırılması için, en az aşağıdaki ayarların uygulanması gerekmektedir.

Etki alanındaki bilgisayarlara erişimler ortamdaki aktif cihazlarla kontrol edilmelidir. Sadece gerekli olan IP veya IP bloklarından erişimler sağlanabilmelidir. Ayrıca port kontrolü de gerçekleştirilmelidir. Özellikle kritik konumdaki sunuculara olan ağ bağlantıları için erişimler kontrollü olarak verilmelidir. Ayrıca ortamda gerçekleştirilen tarama işlemlerinden haberdar olunabilmesi için anormal ağ trafiğinin tespiti ve önlenmesine yönelik gerekli çözümler kullanılmalıdır.

Bilgisayarlarda gereksiz olan tüm servisler kapatılmalıdır. Böylece saldırı yüzeyi azaltılır. Servis güvenliği için servisi çalıştıran kullanıcılar kontrol edilmelidir, varsayılan dışında oluşturulan servis hesaplarının parolalarının karmaşık ve uzun olması sağlanmalı, kilitlenmeyecek şekilde ayarlanmalı, periyodik olarak değiştirilmelidir.

Bilgisayarlar üzerinde yayılma işlemi gerçekleştirilirken, yönetimsel paylaşımlar kullanılmaktadır. Bu sebeple yönetimsel paylaşımların kapatılması gerekmektedir. Eğer etki alanındaki yönetimsel operasyonlar için yönetimsel paylaşımlar gerekli ise, sadece bu operasyonları gerçekleştirecek olan özel kullanıcılar için yönetimsel paylaşımlarda işlem gerçekleştirme hakkı verilmesi gerekmektedir. Bu amaçla aşağıda belirtilen anahtar değerleri 0 olarak ayarlanmalıdır.

- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\AutoShareServer**
- **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\AutoShareWks**

Bilgisayarlardaki TCP/IP güvenliğine önem verilmelidir. Bu amaçla internet seçeneklerinden ayarlar yapılabileceği gibi, kayıt defterinde de gerekli ayarlar gerçekleştirilmelidir.

Güncelleştirmelerin Gerçekleştirilmesi

Etki alanı sızma testi adımlarındaki zafiyet taramalarının etkin olarak gerçekleştirilememesi için, zafiyet taraması sonucunda olabildiğince az bilginin açığa çıkarılması sağlanmalıdır. Bu amaçla ağ ayarları uygun olarak yapılandırılmalı ve etki alanındaki bilgisayarlarda veya etki alanına erişebilen sistemlerde güncelleştirmeler gerçekleştirilmelidir. Yama yönetimi için, en az aşağıdaki ayarların uygulanması gerekmektedir.

Güncellemeler konusundaki en önemli unsur kurum tarafında uygulanmak üzere bir yama yönetimi politikasının oluşturulması, adımlarının belirlenmesi, uygulanması ve sürekli olarak geliştirilmesidir.

Etki alanında ve etki alanına erişimin sağlandığı sistemlerde periyodik olarak zafiyet taraması gerçekleştirilmelidir. Zafiyet taramasında mümkünse farklı araçların kullanılması tavsiye edilmektedir. Böylece bir araç tarafından tespit edilemeyen bazı zafiyetler diğer araçlarla tespit edilebilmektedir. Ayrıca kullanılan araçların da en güncel zafiyetleri barındırdığından emin olunmalı, güncelliği kontrol altında tutulmalıdır.

Anti virüs, saldırı tespit ve önleme sistemleri, anormallik tespit sistemleri gibi etki alanı ortamında güvenliği sağlamakla görevleri sistemlerin güncel olması ve son imzalara sahip olması gerekmektedir.

Tespit edilen zafiyetler kurumda uygulanan güncelleme yönetimi politikası kapsamında değerlendirilmelidir. Kritik zafiyetler, politika kapsamında belirlenen adımlardan geçtikten sonra, en kısa süre içerisinde merkezi olarak etki alanındaki bilgisayarlara dağıtılmalı ve yüklenmelidir. Güncelleştirmeleri almayan ve yüklenmeyen bilgisayarlar tespit edilmeli ve son güncelleştirmeleri alması sağlanmalıdır.

Saldırı yüzeyini azaltmak için bilgisayarlarda sadece gerekli programların bulunması ve bu programların sürüm kontrollerinin belli aralıklarla gerçekleştirilmesi gerekmektedir.

En son güncelleştirmelerden ve zafiyetlerden haberdar olmak için kurumda kullanılan sistemlere ait güvenlik bültenlerine, bloglara, posta gruplarına üye olunması gerekmektedir.

İmaj Yapılandırması

Etki alanı sızma testlerinde gerçekleştirilen yayılma adımında, etki alanındaki bir bilgisayarda bir şekilde elde edilen yerel yönetici kullanıcı parola bilgileri kullanılarak (özet veya açık halinin) diğer bilgisayarlara erişim sağlanamamalıdır. Bu amaçla, kurum içinde kullanılan imajlar uygun şekilde oluşturulmalı ve özelleştirilerek kullanılmalıdır. İmaj yapılandırılması için, en az aşağıdaki ayarların uygulanması gerekmektedir.

İmajlar güncellenmeli ve en güncel hali ile kullanılması sağlanmalıdır. Sıkılaştırma işlemleri için güvenlik şablonları kullanılabilmektedir. Güvenlik şablonları için aşağıda belirtilen kaynak tercih edilebilir:

http://web.nvd.nist.gov/view/ncp/repository

Etki alanına eklenen bir bilgisayar özel bir OU altına yönlendirilmesi sağlanarak (redircmp aracıyla veya hazırlanabilecek betiklerle) bu bilgisayarlar için özel grup ilkeleri kullanılmalıdır. Böylece etki alanına eklenen bir bilgisayarın otomatik olarak sıkılaştırılması da gerçekleştirilebilir.

İmajlar kullanılarak işletim sistemi kurulurken, sadece gerektiği kadar kullanıcı oluşturulması saldırı yüzeyini azaltacaktır. Yerel yönetici haklarına sahip kullanıcılar oluşturulmamalı veya kontrollü bir şekilde oluşturulmalıdır.

Etki alanı saldırılarından korunma için kullanılan en temel yöntemlerden biri de tuzak kullanıcı oluşturmaktır. Bu amaçla, etki alanında kullanılan yerel ilkede üç adım gerçekleştirilebilir.

*Bilgisayardaki gömülü (built-in) yerel yönetici kullanıcısı (Administrator) devre dışı bırakılarak, adı "Test" veya "Deneme" gibi şüphe çekmeyecek şekilde güncellenir. Parolası uzun ve karmaşık verilebilir. Bu işlem grup ilkelerindeki Preferences özelliği kullanılarak aşağıdaki gibi gerçekleştirilebilir.

Gerçek yerel yönetici kullanıcısının kimliği güncellendikten sonra, yerel yönetici olarak kullanıcı adı Administrator, tanımı gömülü yerel yönetici tanımı ile aynı olan ("Built-in account for administering the computer/domain") tuzak bir kullanıcı oluşturulur. Tuzak kullanıcı parolası çok uzun ve karmaşık seçilerek parolanın açık halinin elde edilmesi zorlaştırılabilir. Ayrıca bu kullanıcı devre dışı bırakılarak, saldırganın zaman kaybetmesi sağlanabilir. Bu işlem grup ilkelerindeki Preferences özelliği kullanılarak aşağıdaki gibi gerçekleştirilebilir.

Not: Tuzak kullanıcı yukarıdaki gibi önleyici amaçla kullanılabildiği gibi, tespit amaçlı da kullanılabilir. Bu amaçla, tuzak kullanıcı parolası kolay elde edilebilecek şekilde kısa olarak ayarlanır. Daha sonra bu hesap ile bir kez oturum açılarak hesap etkin olarak bırakılır. Bu hesap ile yapılan işlemlerin denetim kayıtları tutularak bu hesaplar ile yapılan işlemlerden anlık olarak haberdar olunması sağlanabilir. Bu yöntem kullanılırken anlık haberleşme sisteminin etkin şekilde çalıştığından emin olunmalıdır.

Son adım olarak da, oluşturulan tuzak kullanıcı Users veya Guests gibi bir gruba üye yapılabilir ve bilgisayar üzerindeki tüm hakları alınır.

Not: Tuzak kullanıcı oluşturma oldukça yaygın kullanılan bir yöntemdir. Bu sebeple sızma testi sırasında deneyimli kişilerce veya saldırı anında deneyimli saldırganlarca kullanıcıların SID değerleri kontrol edilerek tespit edilebilir. Ayrıca tuzak kullanıcı oluşturulurken Preferences üzerinden parola atanması işlemi çok güvenilir bir yöntem değildir. Konu ile ilgili bir sunum şu şekildedir:

http://www.carnal0wnage.com/papers/LARES-GPP.pdf

Bu sebeple, yerel yönetici parolalarının yönetimi için özelleşmiş uygulamaların veya betiklerin kullanılması tavsiye edilmektedir.

Kritik Hesapların Kullanımı

Etki alanı sızma testlerinde gerçekleştirilen araştırma adımında, oturum açılan bilgisayarlarda kritik kullanıcılara ait bilgilerin elde edilememesi sağlanmalıdır. Bu amaçla, etki alanındaki kritik hesaplar uygun şekilde kullanılmalıdır.

Kritik hesaba sahip kullanıcıların iki ayrı hesabı bulunmalıdır: Etki alanında yönetimsel operasyonlar için kullanılan yetkili kullanıcı hesabı ve bu kritik hesaba sahip yöneticinin günlük işlemlerini gerçekleştirdiği yetkisiz kullanıcı hesabı. Kritik hesapların kullanımı için, en az aşağıdaki önlemlerin uygulanması gerekmektedir.

Yetkili hesap ile DC hariç hiçbir bilgisayarda oturum açılmamalıdır. Açılmış oturum varsa, bu oturumlar kapatılmalıdır. Gerekiyorsa etki alanındaki kritik kullanıcıların istemci makinelerde ve DMZ ağındaki bazı sunucular olmak üzere bu hesapların oturum açması gerekmeyen sunucularda oturum açamayacakları şekilde grup ilkeleri düzenlenmelidir. Etki alanında kritik olan gruplar yerine, yardım masası veya destek grupları gibi grupların bu sistemlerde oturum açıp, bakım yapabilmesine izin verilmelidir. İzin verilen bu kullanıcıların da yetkilerinin iyi sınırlandırılmış olması, sadece gerekli izinlerin verildiğinden emin olunması gerekir. Günümüzde sızma testlerinde açık bırakılmış oturumdaki parola bilgilerini bellekten elde edebilen ve parolaları açık olarak sunan uygulamalar kullanılmaktadır. Bu uygulamalara karşı üç temel önlem alınabilmektedir:

- Bellek üzerinde herhangi bir bilginin bulunmaması sağlanmalıdır. Bu amaçla oturum kapatılırken bilgisayarın yeniden başlatılması gerekmektedir.

- Bu uygulamalar güvenlik paketlerini (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages) kullanmaktadır. Bu paketlerden gereksiz olanların kaldırılması saldırı yüzeyini azaltacaktır. Ancak etki alanında gerekli olan TsPkg veya Kerberos gibi paketlerin kaldırılması, kimlik doğrulaması işlemlerinde sıkıntı oluşturabileceği için tavsiye edilmemektedir.

- Etki alanında kritik olan hesaplar ile DC haricinde hiçbir bilgisayarda process başlatılmamalıdır. Başlatılmış process varsa, bu process sonlandırılmalıdır. Processlerin sonlandırılmasının yanında, bilgisayarın yeniden başlatılması tavsiye edilmektedir.

Yetkili hesaplar ile etki alanı denetleyicisi (DC) üzerinde açılan oturumda sadece etki alanı yönetimi ile ilgili işlemler gerçekleştirilmelidir. Özel işlemler için yetkisiz olan hesap ve kritik olmayan bir bilgisayar kullanılmalıdır.

Yetkili hesaplarla gerçekleştirilen kritik işlemler sırasında anlık olarak bilgilendirme sağlanabilmesi için alarmlar oluşturulmalıdır. Alarm oluşturulabilecek bazı durumlar aşağıdaki gibidir:

- Etki alanındaki kritik gruplara kullanıcı ekleme veya kritik gruplardan kullanıcı çıkarma işlemleri
- Etki alanındaki kritik gruplar veya kullanıcılar üzerinde gerçekleştirilen yetki değiştirme işlemleri
- Grup politikaları üzerinde gerçekleştirilen güncelleme, yetki devri, yetki değiştirme işlemleri
- Kritik grupların kapsam (scope) veya tipi üzerindeki değişiklik işlemleri

Yetkili ve yetkisiz kullanıcı hesaplarının adlarının (account name) birbiri ile benzer olmaması gerekmektedir. Böylece etki alanında yönetici konumda olan kişinin bilgisayarının tespiti kısmen de olsa zorlaşır, etki alanı yöneticisine ait bilgisayardan elde edilebilecek kritik bir takım bilgilerin elde edilmesi daha fazla zaman alır.

Bir kullanıcı herhangi bir bilgisayarda ilk kez oturum açtığında bilgisayar üzerinde bazı bilgiler oluşturulmaktadır. Örneğin kayıt defteri (Registery Editor) değerlerinde bazı güncelleştirmeler gerçekleştirilmekte, Windows 7 işletim sisteminde C:\Users altında otomatik olarak bazı dosyalar oluşturulmaktadır. Sızma testleri ve etki alanı saldırılarındaki adımlardan biri olan "Araştırma" adımında otomatik olarak oluşturulan bu bilgiler aranmaktadır. Bu sebeple, kritik kullanıcıların (Domain Admins grubu kullanılmıyorsa Yardım Masası gibi grupların üyeleri kritik grup olarak görülebilir) kendi bilgisayarları haricinde oturum açtığı oturumlar kapatıldığında bu bilgilerin otomatik olarak silinmesi için grup ilkeleri ile betikler kullanılabilir.

Diğer Güvenlik Önlemleri

Etki alanı sızma testlerinden ve etki alanında gerçekleştirilebilecek saldırılardan korunmak için yukarıda bahsi geçen önlemler dışında gerçekleştirilebilecek birçok önlem bulunmaktadır. Diğer temel önlemler şu şekildedir:

Kaba kuvvet saldırılarından korunmak için parola ilkesi uygun şekilde ayarlanmalıdır. Bu amaçla karmaşık, uzun, sık sık güncellenen, birbirini tekrar etmeyen parolaların kullanılması sağlanmalıdır. Kritik kullanıcılar için özel parola politikaları belirlenmelidir. Bu amaçla gölge (shadow) gruplar oluşturularak bu gruplara Fine-Grained Parola Politikaları uygulanabilir.

Kullanıcıların bilgisayarlarında yönetici olarak oturum açmaması sağlanmalıdır. Yönetici hakkı ile gerçekleştirilmesi gereken işlemler özel bir grup (yardım masası gibi) tarafından gerçekleştirilmeli ve gerekli işlemler gerçekleştirildikten sonra bilgisayar yeniden başlatılmalıdır.

En az yetki prensibi doğrultusunda, yerel bilgisayarlardaki ve etki alanındaki kullanıcılara sadece görevleri doğrultusunda haklar verilmelidir. Kısa süreli olarak gerekli olan haklar ise, takip edilmeli ve denetlenmelidir; işlem bittikten sonra bu haklar geri alınmalıdır. Özellikle antivirüs, DLP gibi ajanlarla çalışan sistemler etki alanındaki kritik kullanıcıların hakları ile çalıştırılmamalı, özel olarak oluşturulmuş ve yetkilendirme yapılmış servis hesapları ile çalıştırılmalıdır. Kritik hesap yetkileri ile çalıştırılması durumunda, ilgili makinede yönetici yetkisi olan bir kullanıcı saldırı araçları ile o hesabın jetonu (token) alarak veya processine sıçrayarak etki alanında yönetici durumuna geçebilir ve kendisine Domain Admins veya Enterprise Admins gruplarına üye olan bir kullanıcı oluşturabilir (alarm oluşturulmamışsa bu durumdan haberdar olunmaz). En az yetki prensibinin bir tarafı da yetkinin uygulandığı alan olarak düşünülebilir. Özellikle kritik işlemler için, işlemi yapan kullanıcının yetkisinin sınırlı olması yetmez, yetkinin kullanıldığı sistemin (bilgisayarın) da sınırlı yetkilendirmeye sahip bir bilgisayar olması tavsiye edilmektedir. Şöyle ki, yardım masası gibi belli yetkileri olan kullanıcıların, RDP veya bazı sistemler kullanarak kurum personelinin bilgisayarına eriştiği makinenin (kurumsal görevi için kullandığı makinenin), günlük işlemler için kullandığı makine haricinde olması, mümkinse de bir sanal makine veya uzak makine olması güvenliği bir kat daha arttıracaktır.

Linkedin, Hotmail, Facebook gibi sitelerdeki üyelerin parolaları veya parolaların özetlerinin saldırganlar tarafından ele geçirildiği sık sık gündeme gelmektedir. Bu sebeple etki alanındaki (özellikle kritik sistemlere erişen) personelin oturum açmak için ve kurum içindeki sistemlere bağlantı için kullandıkları parolalarını, kurum dışındaki sistemlerde (bloglar, sosyal paylaşım siteleri, haber siteleri vs) kullanmamaları önerilmelidir. Ayrıca parolalarının da bu sitelerdeki parolalarıyla benzer olmaması - tahmin edilebilir olmaması - da tavsiye edilmektedir.

Bilgisayarlardaki güvenlik duvarları, UAC gibi güvenlik sistemleri etkin olmalıdır. Hak yükseltme işlemleri sırasında işletim sistemi tarafından yönetici onay modunun etkinleştirilmesi tavsiye edilmektedir.

Bilgisayarlar veya paylaşımlar üzerinde kritik bilgiler bulunmamalıdır. Bu kritik bilgilerden bazıları aşağıdaki gibidir:

- Şifresiz olarak saklanan kritik bilgiler (özellikle kritik kullanıcılara ait parola ve kritik sunuculara ait IP veya oturum bilgileri)

- Zamanlanmış görevler veya özel operasyonlar için kullanılan betikler içerisinde kullanıcı hesabı ve sistem bilgileri

- Kritik sistemlere bağlantı için kullanılan ve oturum bilgileri içerisinde kayıtlı olan RDP, SSH veya FTP bağlantı dosyaları

- Etki alanı denetleyicisi (DC) gibi kritik sunuculara uzaktan erişimler (RDP,SSH, FTP,... vs.) engellenmelidir. Kritik sunuculara fiziksel güvenlik önlemlerinin alındığı ortamlardan erişilebilmelidir. Bu önlemin mümkün olmadığı durumlarda sadece belli adreslerden uzak bağlantı yapılmasına izin verilmelidir. Bunun yanı sıra güvenliğin yeteri kadar sağlanamadığı ortamlara etki alanı denetleyicisi kurulması gerekiyorsa RODC sunucularının kullanılması tavsiye edilmektedir.

- Gerçekleştirilecek her güvenlik önlemi iyi planlanmalı, test edilmeli, daha sonra uygulanmalıdır. Gerçekleştirilen önlemler öncesinde ve sonrasında denetlenmelidir.

- Farklı etki alanlarına sahip kurumlarda, sızılan bir etki alanından diğer etki alanlarına erişilememesi için, her etki alanı diğer etki alanları ile olabildiğince soyutlanmalıdır. Bu amaca boş kök etki alanı (empty root domain) kullanılabilir. Ayrıca, kök etki alanında bulunan kritik gruplardaki (Enterprise Admins) kullanıcılar, alt etki alanlarında oturum açmamalıdır. Bunun yanında etki alanları arasında kurulan güven ilişkilerinde (trust relationship); ilişkinin geçişliliği, yönü ve türü konularına dikkat edilmeli, seçmeli kimlimlik doğrulama (selective authentication) kullanılmalıdır. Böylece saldırı yüzeyi daraltılmaktadır.

- DMZ içerisindeki sunucular tekil (stand-alone) olarak çalışmalı veya kuruma ait etki alanı dışında ayrı bir etki alanı ile yönetilmelidir. Ayrı olarak oluşturulacak yeni etki alanının, kurum etki alanıyla ilişkisi bulunmamalıdır. İki farklı etki alanının yöneten sistem yöneticileri farklı olmalı veya farklı/benzer olmayan hesap bilgileri kullanmalıdırlar.

- Sızma testleri ve etki alanı saldırıları sırasında etki alanındaki hesapların ve kurumda bulunan bilgisayarlardaki yerel hesapların parolaları açık olarak ve özet halinde elde edilebilmektedir. Bu sebeple bir saldırı durumunda veya etki alanı sızma testinden sonra, bilgisayarlardaki yerel kullanıcıların (local users) ve etki alanındaki kullanıcıların (domain users) parolaları değiştirilmelidir. Etki alanındaki kullanıcıların parolalarını değiştimeleri için grup ilkeleri ile değişikliğin gerçekleştirilmesi beklenebilir, ancak kritik sistemlere (veritabanı, aktif cihaz gibi) erişimi olan veya kurum için kritik varlıklara (müşteri bilgileri gibi) erişimi olan personelin parolalarını derhal değiştirmeleri tavsiye edilmektedir. Benzer şekilde kritik makinelerdeki yerel kullanıcıların parolaları değiştirilmeli, yerel yönetici parolaları birbirinden farklı olarak ayarlanmalıdır.

Not: Etki alanı sızma testlerinden önce (ve saldırının her an olabileceği düşüncesi ile belli periyotlarla) kritik sistemlere ait yedeklerin alınması ve güvenilir şekilde korunması tavsiye edilmektedir. Bir problem durumunda gerçekleştirilecek işlemler için de acil eylem planlarının hazır olması tavsiye edilmektedir.

Kimlik doğrulamasını etki alanı denetleyicilerine sorgulatan ara sistemlerden (örneğin, Exchange Server 2010 için CAS rolüne sahip sunuculardan) personelin parolaları, bazı processlerden açık olarak alınabilmektedir. Bu durum kurumda bir takım iyileştirmeler için de kullanılabilir. Örneğin;

İç eğitimlerde kullanılabilir. Personele, özel hayatında kullandığı parolalara benzer parolalar kullanmaması gerektiği belirtilebilir. Özellikle kritik sistemlere ve verilere erişimi olan personelin parolalarını farklı oluşturmaları sağlanmalıdır.

Denetimlerde kullanılabilir. Bu sunuculardaki processlerinin dump'ının alınması da dahil olmak üzere, belirli nesnelere erişimlere erişimleri kayıtları alınmalı ve bu kayıtlar güçler ayrılığı prensibine uygun olacak şekilde (Güvenlik Birimi gibi sistemin yöneticileri haricinde bir grup tarafından) denetlenmelidir.

Sıkılaştırmalarda kullanılabilir. Elde edilen parolalar kullanılarak, personelin kullandığı parolaların güçlü olup olmadığı incelenebilir. Kolay parola kullanan, kaba kuvvet saldırıları ile parolası tespit edilebilecek personel uyarılmalıdır.

Microsoft, sistemin sürekliliğinin sağlanması için önbelleğe alınmış kimlik bilgileri (cached credentials)kullanmaktadır. Bu bilgiler sayesinde etki alanı denetleyicisine erişim sağlanamadan etki alanı hesabı ile oturum açılabilmekte ve bazı sistemlere erişim sağlanabilmektedir. Ancak bu durum saldırganlar tarafından kötüye kullanılabilmektedir. Bilgisayarı ele geçiren ve kaba kuvvet saldırısı gerçekleştiren saldırgan - hesap kilitleme, loglanma, parola kırma gibi dertleri olmadan - kullanıcıya ait kimlik bilgilerini ele geçirebilir. Bu sebeple özellikle kritik kullanıcıların son oturumlarına ait bilgilerinin bilgisayar üzerinde saklanmaması tavsiye edilmektedir.

Sızma testleri sırasında, sızma testlerini gerçekleştiren kullanıcılara ve bu kullanıcıların bilgisayarlarına verilen tüm yetkilerin geri alınması unutulmamalıdır. Ayrıca sızma testlerini gerçekleştiren personelin, test sırasında oluşturduğu tüm kullanıcılar ve gerçekleştirdikleri tüm değişiklikler geri alınmalıdır.

Gerçekleştirilecek teknik önlemler haricinde iki temel noktaya daha dikkat çekilmesinde fayda bulunmaktadır.

Kurumda çalışan personel belki de kurum için en zayıf halka niteliğindedir. Nasıl ki bir zincir en zayıf halkası kadar güçlü ise, bir kurumun güvenliği de en zayıf bileşeni kadar güvenilir sayılır. Bu sebeple kurum personeline gerekli güvenlik eğitimlerinin verildiğine ve bilinçlenmenin sağlandığına emin olunmalıdır. Yeni işe başlayan veya teknik işlerde çalışmayan personel de dahil olmak üzere uygun seviyede bilinçlendirme eğitimleri düzenlenmeli, bu eğitimler ölçülmeli, iyileştirilmeli ve sürekliliği sağlanmalıdır. Özellikle sosyal mühendislik saldırılarına karşı bilinçlendirme sağlanmalıdır.

Belki de en önemli önlem: Üst Yönetim Desteği. Etki alanı saldırılarına karşı teknik operasyonların uygulanması ve sürekliliğin sağlanması oldukça önemli konulardır. Ancak gerçekleştirilen bu önlemler kurum personelinin tepkisine yol açabilecektir. Örneğin; personelin parolasını en az 8 karakter olarak oluşturmak zorunda olması, bilgisayarlarında yerel yönetici haklarına sahip olan personelden bu hakların alınması gibi durumlarda karşılaşılabilecek tepkilere karşı üst yönetim maddi ve manevi destekten kaçınmamalıdır. Böylece kurum bilgisi ve imajı korunacaktır.