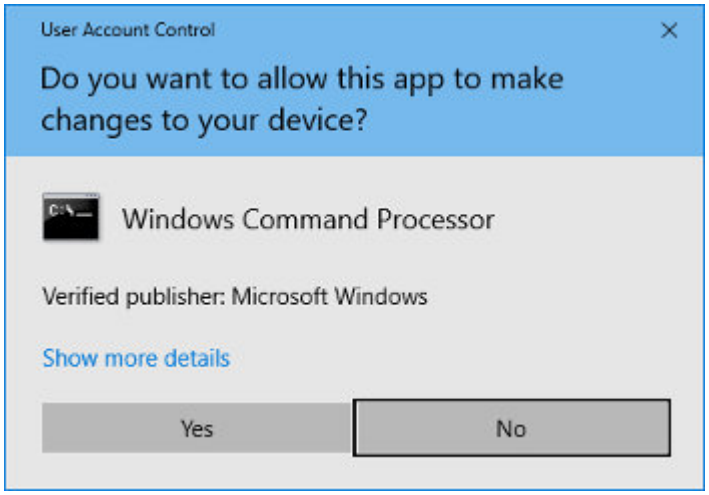
Yönetici İznine (UAC) Takılan Program Sorunu



Çalışırken bazı programlar görünürde yönetici iznini gerektirecek her hangi bir işlem yapmamalarına rağmen yönetici izni istemektedirler. Özellikle bilgi güvenliği noktasında prosedürler yürüten firmalarda da kullanıcı bilgisayarı üzerinde yönetici olmadığından uygulamayı çalıştırmakta başarısız olmaktadır.

Programın yönetici izni istemesinin temelinde yatan neden, çalışırken ya sistem ayarlarına müdahale ediyor olması yada sistem dosyalarında işlem yapmaya çalışmasıdır. Burada sistem dosyaları sözü aklı karıştırmasın. Program “Program Files” varsayılan klasörüne yüklendiğinde kendi dosyaları da “Program Files” klasörünün özelliği gereği Windows tarafından sistem dosyası olarak işaretlenmektedir ve bu dosyalar üzerinde işlem yapabilmek için yönetici izni gerekmektedir.

Çözüm olarak karşımıza iki seçenek çıkmaktadır;

- Kullanıcıya yerel yönetici haklarını vermek ki bu özellikle bilgisayar noktasında tecrübesi olmayan kullanıcılar tarafında ayrı bir güvenlik açığına sebep olmaktadır.
- Diğer bir seçeneğimiz de programın kurulum yolunu değiştirmektir. Örneğin C:\ diski altında oluşturacağımız bir klasörü kurulum yolu olarak verirsek, oluşturduğumuz bu klasör sistem klasörü olmadığından uygulamamız da sıkıntısız çalışacaktır.

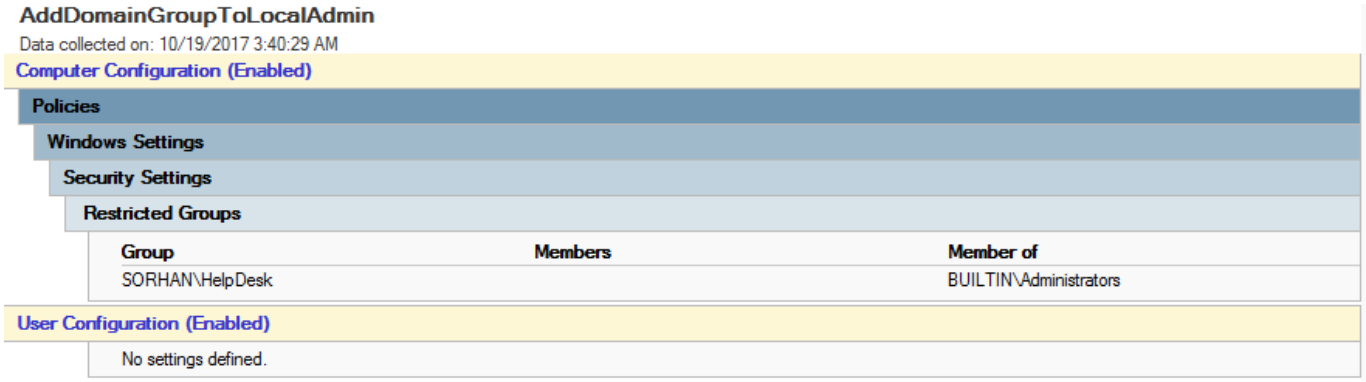
Domain Yapısındaki Grupları Client Local Gruplara Ekleme

Domain yapılarında yapılan işlemlerden biri de kullanıcılardan local adminlik dediğimiz yönetici haklarının alınmasıdır. Bu işlemi yapmada ki amaç, kullanıcının bilgisayarı amacı dışında kullanmasına engel olmaktır. Bu işlemi yaparken de, özellikle bilgi işlem departmanının local admine atanması gerekmektedir. Bu atamayı yapmanın çeşitli yolları olmaktadır;

- Bilgi teknolojileri departmanının hepsini, Domain Admins grubuna dahil etmek: Bu seçenek güvenlik tehlikesini client bazından çıkarıp direk bütün yapı seviyesine çıkarır. Departmanda yer alan özellikle stajyer ve yeteri bilgiye sahip olmayan yeni çalışanların oluşturacağı güvenlik tehdidi göz ardı edilemez. Bu seçenek kabulümüz değil dolayısıyla
- Her kurulan yeni client bilgisayara, kurulumdan sonra BT departmanındaki bütün kişileri elle yöneticiler grubuna

eklemek. Bu yönteminde dezavantajları: Kişileri tek tek eklerken kişiler unutulabilir, departman değiştiren kişiler bilgisayarlarda yönetici olarak kalmaya devam edecek…

- BT departmanı için domain yapısında bir grup oluşturup departman kişileri bu gruba üye edilir. Bu işlemden sonra Group Policy üzerinden oluşturulan bu grup clientlara otomatik olarak yönetici grubuna eklenir. Bu işlem için gereken group policy kuralı aşağıdaki gbidir.



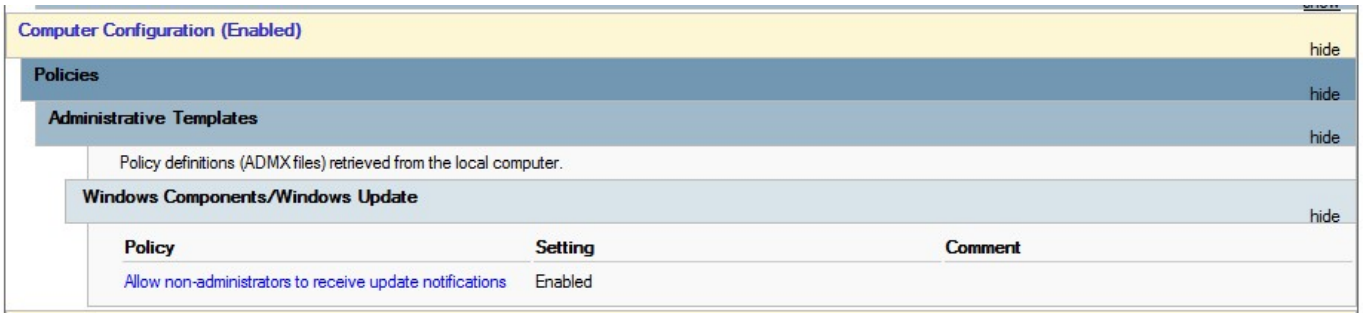
Kuralın sol tarafında yer alan “Group” başlığı clientlara eklenecek olan domain üzerinde tanımlı olan gruptur. SORHAN burada domain adını temsil etmektedir. HelpDesk de BT departmanı grubudur. Sağ tarafta yer alan “Member of” başlığı da grubun client tarafında nereye ekleneceğini ifade eder. BUILTIN ifadesi client makineyi ifade eder ve sabittir. Administrators ifadesi de clent makine üzerinde tanımlı Administrators grubunu ifade eder.

GP Üzerinden Herkese Güncelleme Yetkisi Verme

Bilişim sistemlerinin en önemli konularının başında sistemin güvenliğidir. Konu güvenlik olunca da makinelerde yetkilendirme devreye giriyor. Her şirkette olması gereken yetki kısıtlarından biri de bilgisayarlarda local adminliklerin olmaması kuralıdır. Kullanıcılardan local admin yetkileri alındıktan sonra ortaya bir sıkıntı daha çıkmaktadır: o da güncellemeleri yüklemek için kullanıcılardan yönetici izni istemek…

Güncelleme yüklenmeyince sistem açıklarını kapatan güncellemeler sisteme yüklenmemektedir.

Çözümümüz şu olacak: Group policy üzerinden bütün kullanıcılara güncelleme yükleme izni vermemiz gerekmektedir. İlgili GP ve gerekli değeri aşağıdaki resimdeki gibidir.



SAP Şifre Karmaşıklığı Zorlama

Her veri barındıran sistemin olmazsa olmazı güvenlik ve güvenliğin akla ilk geleni şifreler ve en önemli konu şifre karmaşıklığı. Şifre karmaşıklığının önemi üzerine ne kadar kullanıcıya uyarıda bulsanız da gene de kullanacakları şifre 123456, qwerty, qazws gibi basit şifreler oluyor. Bu noktada bilgi işlem departmanına düşen iş şifre karmaşıklığını kullanıcının insafına bırakmayıp sistem parametrelerini ayarlamaktır.

SAP'de şifre karmaşıklığı RZ10 sistem parametreleri ekranında aşağıdaki şekilde ayarlanmaktadır. Burada dikkat edilmesi gereken nokta değişikliğin devreye girmesi için sistemin yeniden başlatılması gerekmektedir.

RZ10 transection koduna giriş yapılır ve aşağıda yer alan parametreler isteye göre düzenlenir.

Parametre Adı	Değer	Açıklama
login/min_password_diff	3	Son üç şifre ile aynı şifre kullanılamaz
login/min_password_digits	1	En az bir rakam bulunmalı
login/min_password_lowercase	1	En az bir küçük harf bulunmalı
login/min_password_uppercase	1	En az bir büyük harf bulunmalı

NOT: Sahada aktif kullanılan el terminallerinde parametre değişikliği sonrasında sıkıntı yaşamamak adına işlem öncesinde el terminallerinde kullanılan şifreleri yeni politikaya göre düzenlemeye gidebilirsiniz.

Sql İle Kimlik No Kontrol

Kişi kaydı bulunan bilgi sistemlerinin hemen hemen hepsinin en önemli alanı kimlik numarasıdır. Kimlik numaraları de rastgele oluşturulmuş bir sayı değil de belli bir algoritmaya göre oluşturulmuş bir numaradır.

Aşağıdaki sql fonksiyonun kullanarak sisteminize kaydedilen kayıtların uygun kayıtlar olup olmadığını sorgulayabilirsiniz. Bir fikir olarak mesela, tabloya yazılacak bir trigger ile bütün kayıtlar otomatik olarak sorgulanabilir.

Fonksiyonun kullanımına örnekler:

Bir kaydı kontrol etmek için örnek

Kayıt tablosunda kimlik numaraları hatalı olan kayıtları getirmek için de aşağıdaki gibi bir sorgulama yapılabilir.

Cisco Cihazlara Giriş Şifresi Verme

Network cihazlarında olmazsa olmazımız güvenliktir, güvenliğin ilk adımı da şifrelerdir. Cisco cihazlarında kullanılan çeşitli şifreler bulunmaktadır.

- Console Şifresi
  Cihaza console üzerinden bağlantı sırasında istenen şifredir. User Moda giriş için kullanılır. Console şifresi tanımlamak için yazılması gereken kodlar aşağıdaki gibidir.

Komut	Açıklama
CihazYeniAdi(config)#line console 0	console konfigurasyon ekranına giriş yapar
CihazYeniAdi(config-line)#password Password	Giriş için şifreyi “Password” olarak belirler
CihazYeniAdi(config-line)#login	Şifreyi aktifleştirir, login komutu girilmezse şifre aktifleşmeyecektir.
CihazYeniAdi(config-line)#exit	çıkış yapar

- Ayrıcalıklı EXEC modu Şifresi
  Kullanıcı modundan enable komutu ile ayrıcalıklı moda geçiş için kullanılacak olan şifredir. password ve secret olmak üzere iki türü bulunmaktadır.

  - password şifresi
    Ayrıcalıklı moddan ayrıcalıklı moda geçişte kullanılır. Konfigurasyon dosyasında düz metin olarak tutulur. Ayarlamak için aşağıdaki kodları yazmak gerekmektedir. Aktifleştirme için login komutu şart değildir.

    Daha önceki adımda User şifresini belirlediğimiz için user moda girişte öncelikli olarak şifreyi istiyor.

    CihazYeniAdi(config)#enable password 123456 : Şifreyi 123456 olarak belirler.

  - secret şifresi
    password şifresi ile aynı işlemi yapar ancak konfigurasyon dosyasında şifreli olarak tutulur. Ayarlamak için “CihazYeniAdi(config)#enable password 123456” komutunda password yerine secret kelimesi yazılır.
    Password ve secret beraber etkinleştirilirse secret baskın çıkar.
    CihazYeniAdi(config)#enable secret 123456

Şifreler ayarlanıp show running-config komutu ile çalışan konfigurasyon dosyası gösterildiğinda:

```
CihazYeniAdi#show running-config
Building configuration…

Current configuration : 1141 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CihazYeniAdi
!
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jJVK/
enable password 123456
…..
```

Görüldüğü gibi password ve secret ikisi de 123456 olarak ayarlanmasına rağmen secret şifrelenmiş olarak görünüyor.

- Telnet (VTY) Şifresi
  Cihaza telnet bağlantısı yapılırken sorulacak olan şifredir. Telnet şifresi yapılandırılmamış bir cihaza kesinlikle telnet bağlantısı yapılamaz. Telnet şifresi yapılandırmak için gerekli olan kodlar aşağıdaki gibidir:

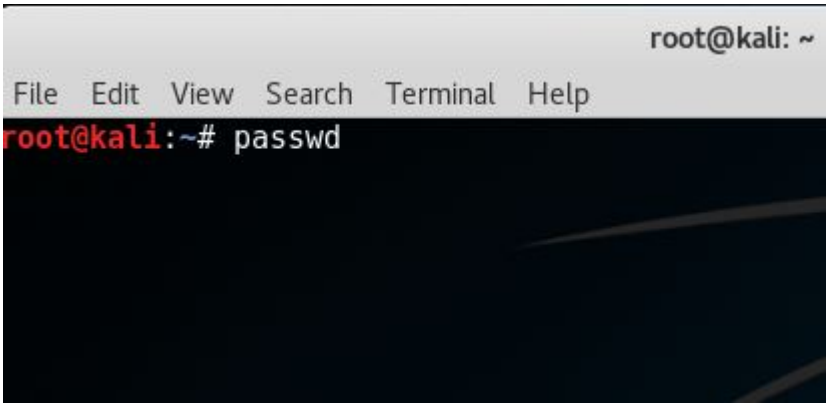
Yapılan bütün bu işlemler RAM üzerinde tutulmaktadır. yapılandırılan şifrelerin kalıcı hale gelmesi için ayarların ROM üzerine kaydedilmesi gerekmektedir. Bunun için gerekli olan kod aşağıdadır.

Kali Linux Kullanıcı Şifresi Değiştirme

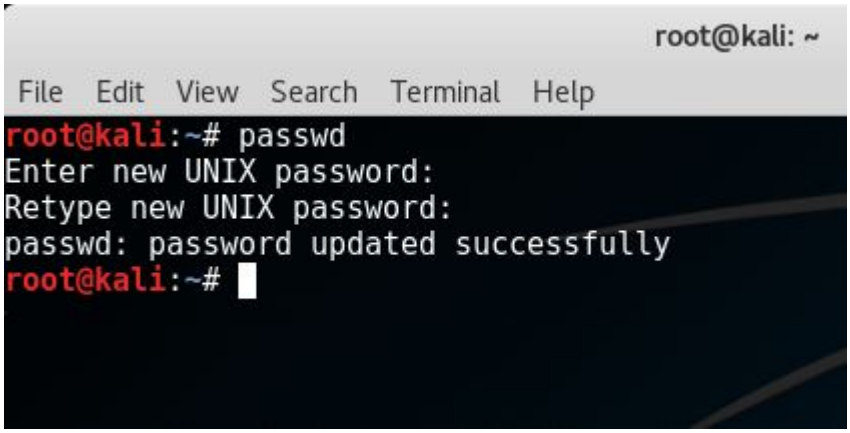
Kali Linux üzerinde kullanıcı şifresi değiştirmek için;

- Root şifresi değiştirme

1. Terminalde **passwd** yazarak Enter'a basın

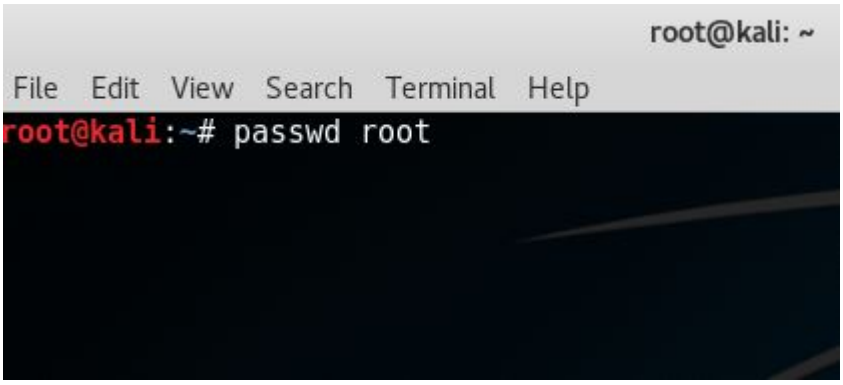


2. Yeni şifreyi yazıp Enter'a basın ardından şifreyi doğrulamak için tekrar yazıp Enter'a basın.



- Root dışında bir kullanıcının şifresini değiştirme

1. Terminalde **passwd kullaniciAdi** yazıp Enter'a basın.



2. Yeni şifreyi yazıp Enter’a basın ardından şifreyi doğrulamak için tekrar yazıp Enter’a basın.