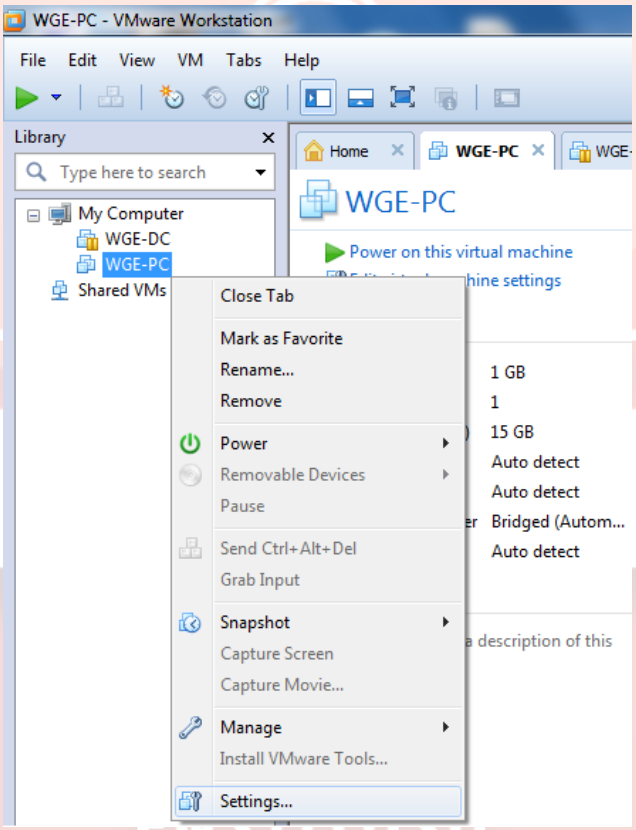
Uygulama 1 - 'Ease of Access' Özelliği ile Bilgisayarın Ele Geçirilmesi

Önbilgilendirme

- Bu uygulama istemci WGE-PC üzerinde gerçekleştirilecektir.
- Bu uygulama, bilgisayar kapalı iken gerçekleştirilecektir.

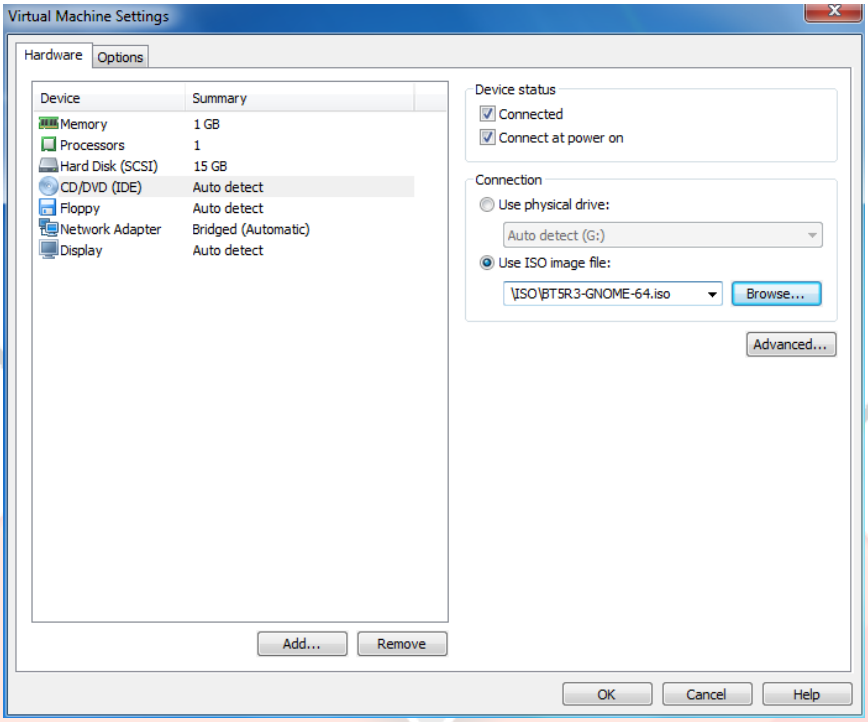
Bilgisayarın Boot Ayarlarının Yapılması

Uygulamalarla birlikte verilen “ISO" dizini altındaki BT5R3-GNOME-64.iso adlı ISO dosyası CD-ROM'a alınır. Bu işlem için önce sanal makina üzerinde sağ tıkla “Settings” seçilir.



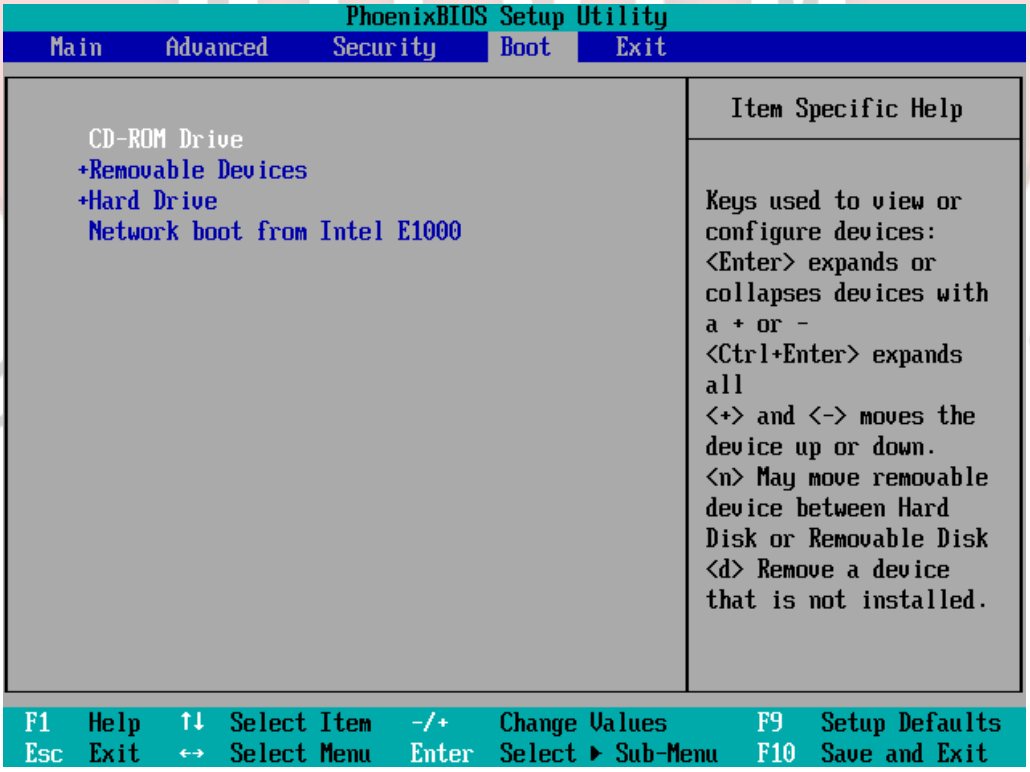
Şekil - 1: BackTrack İmajının CD-ROM'a Gösterilmesi

Sonrasında bilgisayar açıldığında da CD-ROM'u görmesi sağlanır. Bu işlem için önce donanımlar arasından “CD/DVD (IDE)” seçilir, daha sonra “Use ISO image file:” ile uygulamalarla birlikte verilen ISO dizini altındaki BT5R3-GNOME-64.iso dosyası aşağıdaki seçildikten sonra OK ile ISO tanıtma işi tamamlanmış olur.



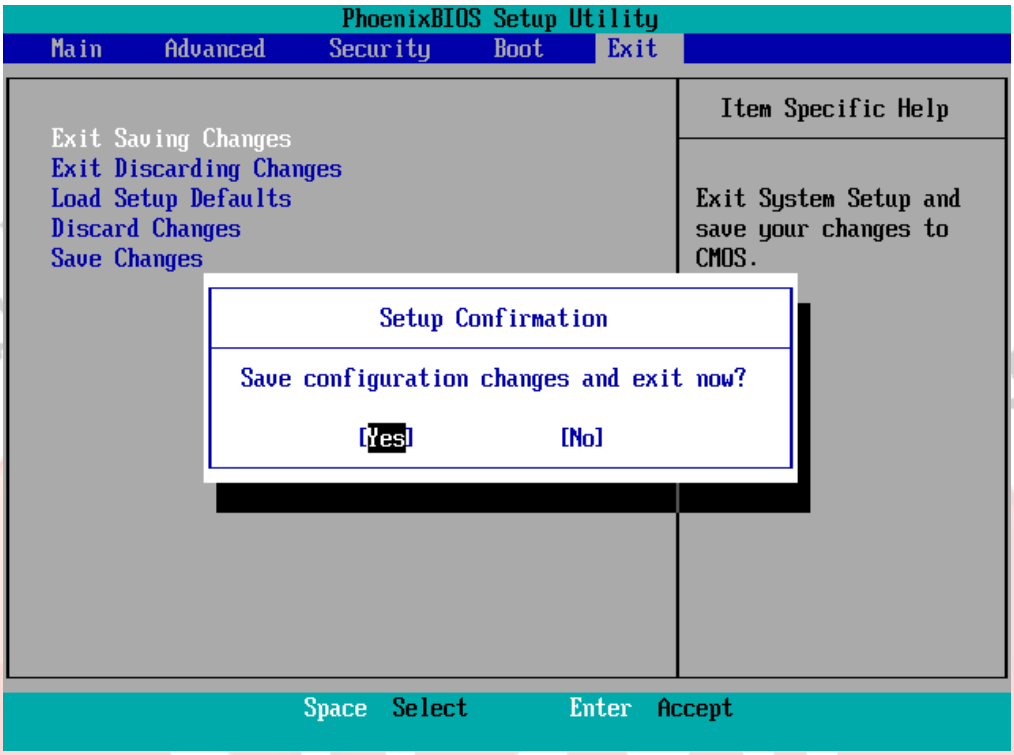
Şekil - 2: CD-ROM Ayarlarının Gerçekleştirilmesi

Sonrasında bilgisayarı açmak için "Power on this Virtual Machine" seçeneği ile bilgisayar başlatılır. Bilgisayar açılmaya başlarken açılma ekranına tıklayarak aktif hale getirdikten sonra F2 tuşuna ard arda basarak BIOS seçeneklerine gelinir. BIOS ayarlarındaki Boot sekmesinde, ok tuşları ve +/- tuşları kullanılarak CD-ROM sürücüsü en üste çıkarılarak bilgisayarın CD-ROM'dan başlatılması sağlanır.



Şekil - 3: BIOS Ayarlarının Gerçekleştirilmesi- 1

Sonrasında gerçekleştirilen ayarların kaydedilmesi için "Exit" sekmesinde "Exit Saving Changes" seçeneğine gelinir ve "Enter" tuşuna basılır. Gelen uyarı mesajında "Yes" ile adım ilerletilir ve bilgisayar yeniden başlar.



Şekil - 4: BIOS Ayarlarının Gerçekleştirilmesi - 2

Not: Değişikliklerin kaydedilmesi için F10 tuşuna da basılabilir.

BackTrack Ara Yüzüne Geçiş Sağlanması

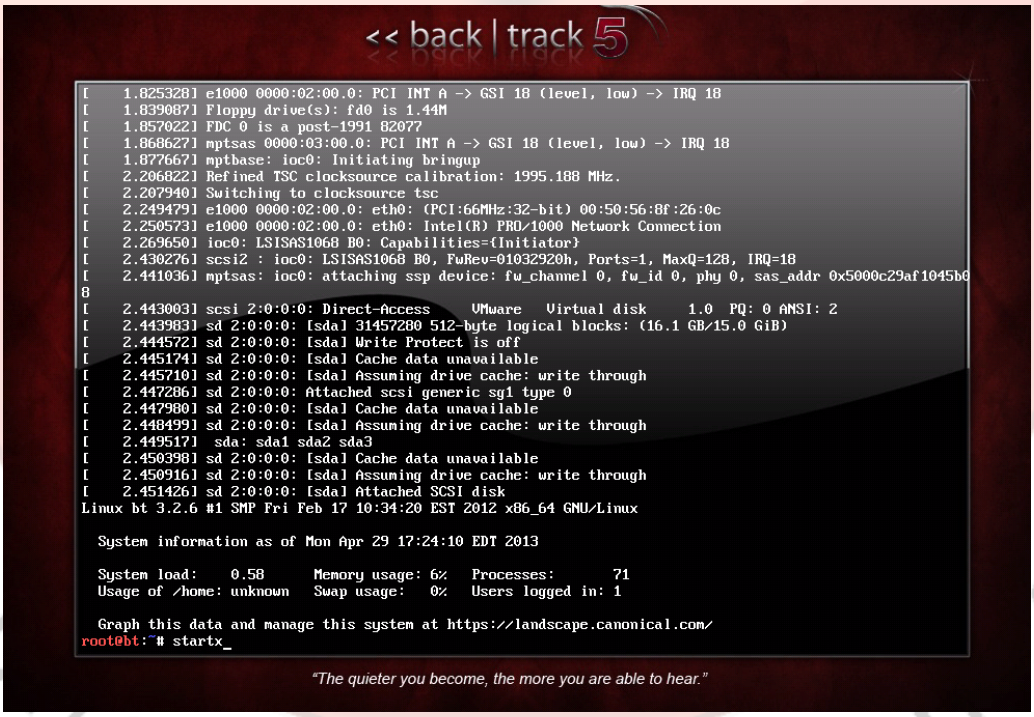
Bilgisayar yeniden başladıktan sonra ilk olarak aşağıdaki ekran ile karşılaşılır. Bu ekranda Enter tuşuna basılarak işletim sistemine girilir veya bir süre sonra işletim sistemi kendini başlatacaktır.

Şekil - 5: BackTrack Ara Yüzüne Geçilmesi - 1

Eğer aşağıdaki gibi bir ekran ile karşılaşılırsa, "Default Boot Text Mode" seçilirek "Enter" tuşuna basılır.

Şekil - 6: BackTrack Ara Yüzüne Geçilmesi - 2

Gelen ekranda "startx" komutu çalıştırılarak ara yüze geçiş yapılır.



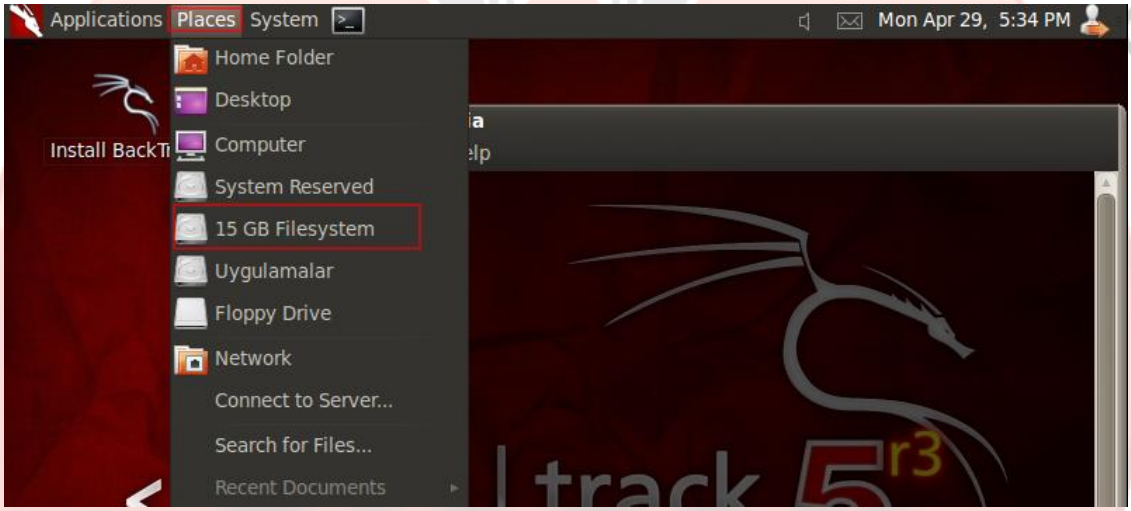
Şekil - 7: BackTrack Ara Yüzüne Geçilmesi - 3

Windows İşletim Sistemine Ait Dosya Sistemine Erişilmesi

BackTrack ara yüzü açıldıktan sonra, komut satırı açılır ve Windows işletim sistemine ait olan dosya sistemine erişilir. Bu amaçla /media dizinine gidilir.

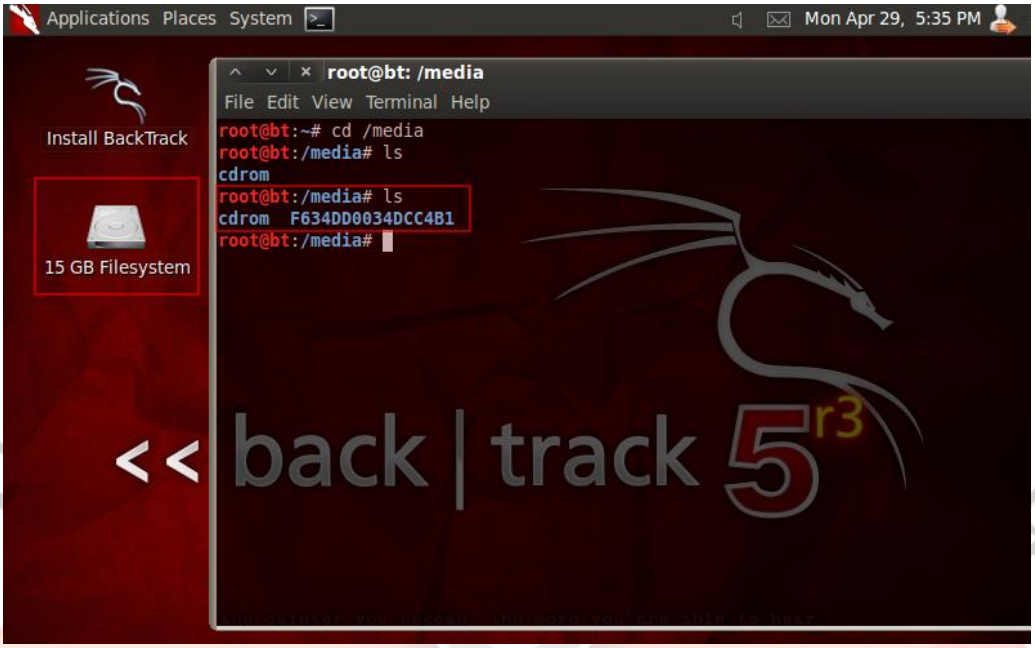
Şekil - 8: Dosya Sistemine Erişim Sağlanması - 1

Not: Eğer bu dizin altında Windows işletim sistemine ait disk listelenmezse mount işlemi gerçekleştirilmelidir. Bu işlemin en kolay yolu üst menüdeki Places seçeneğindeki Windows işletim sistemine ait dosya sistemini seçmektir.



Şekil - 9: Dosya Sistemine Erişim Sağlanması - 2

Mount işlemi sonrasında masaüstüne Windows işletim sistemine ait dosya sisteminin eklenecek ve /media dizini altında bu dosya sistemi listelenecektir.



Şekil - 10: Dosya Sistemine Erişim Sağlanması - 3

Not: Gelen dosya sistemine ait etiket adı her sistem için farklılık gösterebilir.

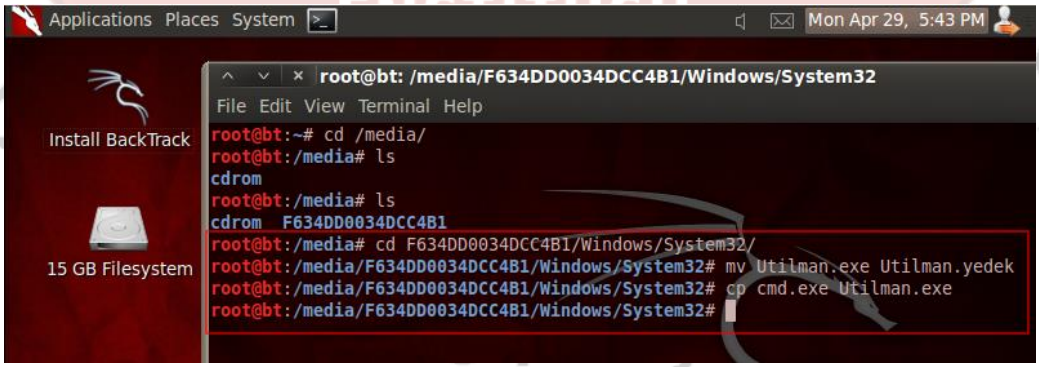
Utilman Aracının CMD Aracı ile Değiştirilmesi

Windows işletim sisteminin dosya sistemine erişim sağlandıktan sonra, önce "Utilman.exe" aracı "Utilman.yedek" olarak değiştirilir, sonrasında "cmd.exe" aracının kopyası "Utilman.exe" olarak oluşturulur. Bu işlemleri gerçekleştirmek için gerekli komutlar aşağıdaki gibidir.

cd <Dosya Sistemi Adı>/Wİindows/System32

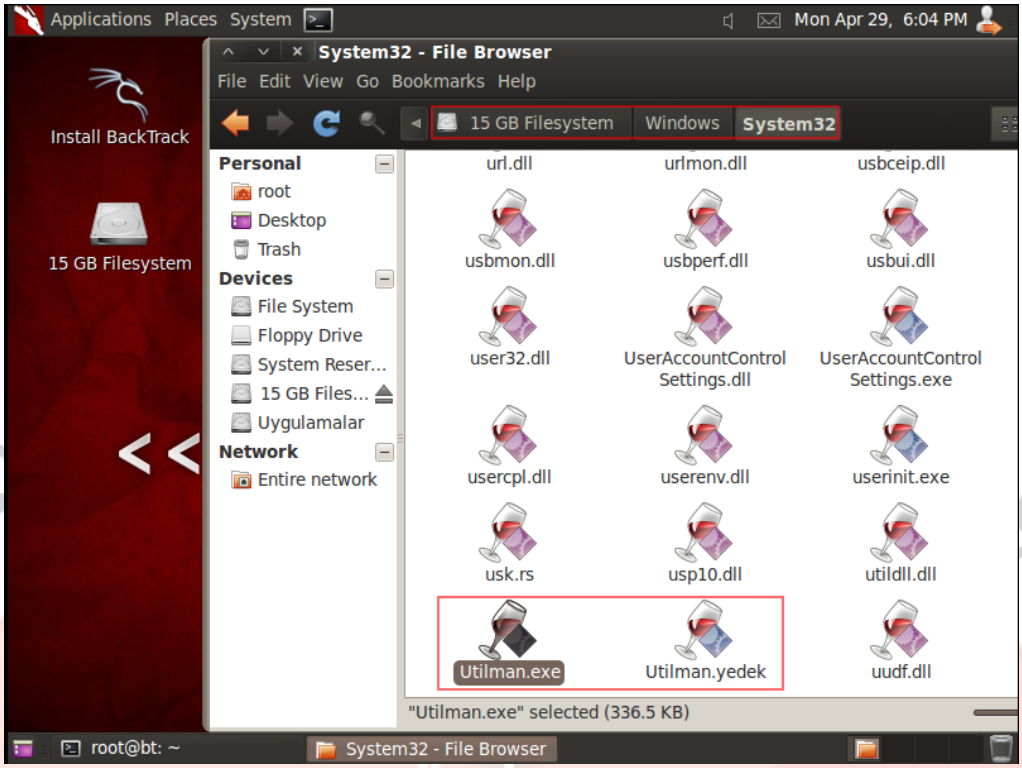
mv Utilman.exe Utilman.yedek

cp cmd.exe Utilman.exe



Şekil - 11: Utilman Aracının CMD Aracı İle Değiştirilmesi - 1

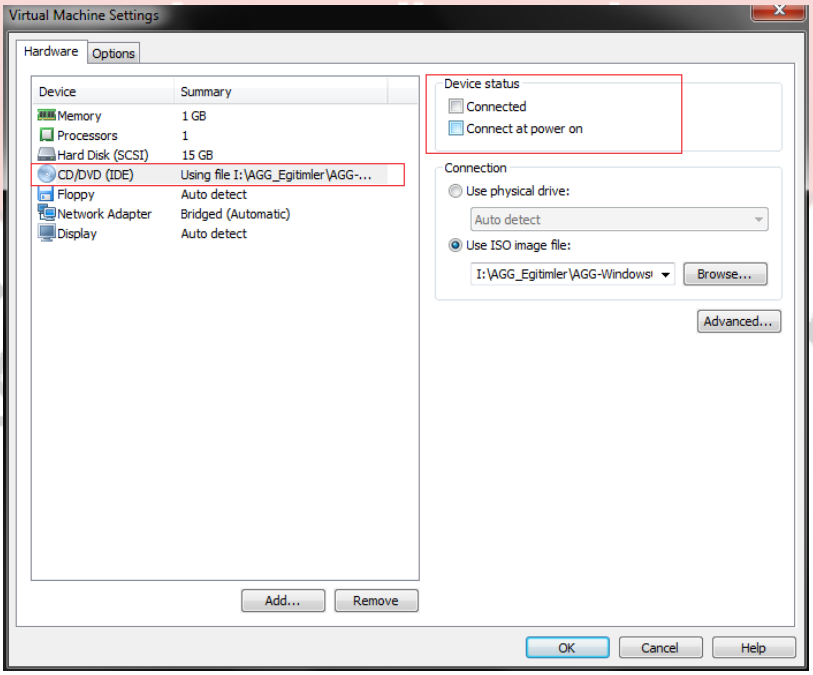
Masaüstünde oluşan dizinden Windows/System32 dizine girildiğinde Utilman.exe ve Utilman.yedek dosyalarının mevcut olduğu gözlenmektedir.



Şekil - 12: Utilman Aracının CMD Aracı İle Değiştirilmesi - 2

CD-ROM Ayarlarının Varsayılan Hale Döndürülmesi

Utilman aracı yerine CMD aracı getirildikten sonra, CD-ROM ayarı eski haline getirilmelidir. Bu amaçla aygıt durumundan "Connect" ve "Connect at power on" seçenekleri seçilmemiş hale getirilir. Ayrıca, seçilen aygıt tipi olarak "Client Device" belirtilir.



Şekil - 13: CD-ROM Ayarlarının Gerçekleştirilmesi - 1

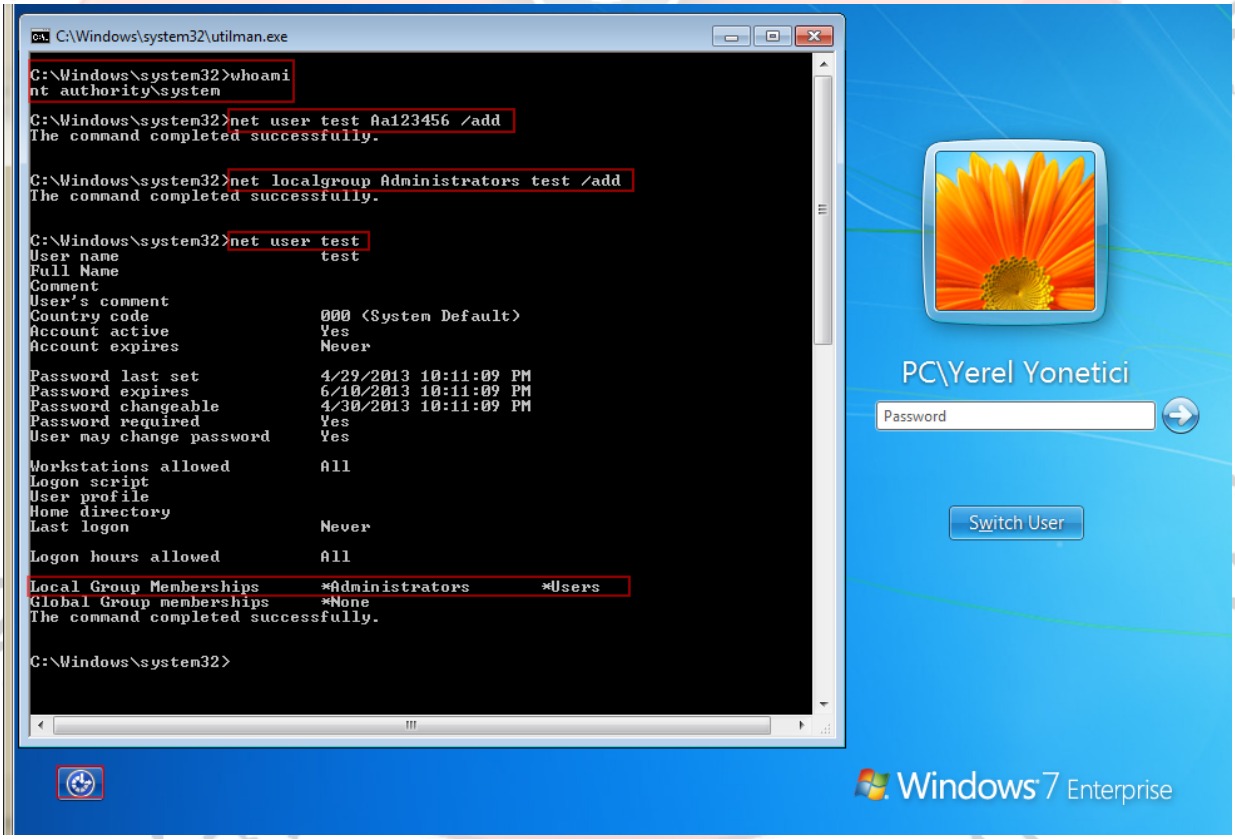
Bu işlem sonrasında CD-ROM'un çıkarılacağına dair bir uyarı mesajı ile karşılaşılır. Bu uyarı mesajı "Yes" ile onaylanır.

Bu adımdan sonra, bilgisayar yeniden başlatılır.

Uygulamanın Test Edilmesi

Yukarıdaki adımlar uygulandıktan ve bilgisayar açılış ekranı geldikten sonra, "Ease of Access" butonuna basıldığında komut satırı başlatılacaktır. Komut satırı, SYSTEM adı verilen Administrator kullanıcısından bile daha yetkili bir kullanıcı hakları ile çalışmaktadır. Bu haklarla bilgisayarda kayıt değerleri değiştirilebilir, yerel yönetici olabilecek bir kullanıcı oluşturulabilir, bilgisayarda keşfedilmesi zor açıklıklar bırakılabilir.

Aşağıdaki örnekte bilgisayarda test isimli bir kullanıcı oluşturularak yerel yönetici grubuna eklenmiştir.



Şekil - 14: Uygulamanın Test Edilmesi