Uygulama 2 - SID Değerlerinin Elde Edilmesi

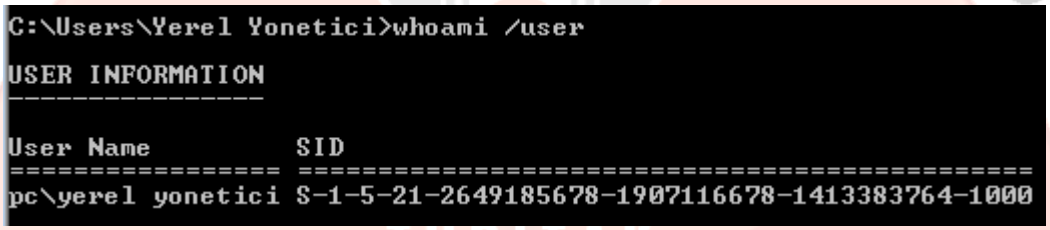
Önbilgilendirme

- Bu uygulama istemci WGE-PC üzerinde gerçekleştirilecektir.
- Bu uygulama, Yerel Yönetici oturumu açıkken gerçekleştirilecektir.

Oturumu Açık Olan Kullanıcının SID Değeri

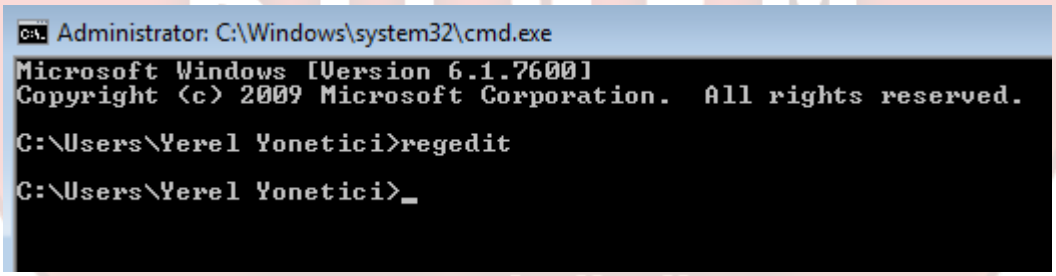
Oturumu açan kullanıcı hakkında ayrıntılı bilgi için "whoami" aracı kullanılabilir. Bu araç kullanılarak, mevcut kullanıcının SID değeri elde edilebilir. Bu işlem için aşağıdaki komut kullanılmalıdır.

whoami /user



Şekil - 1: Oturumu Açan Kullanıcının SID Değeri - 1

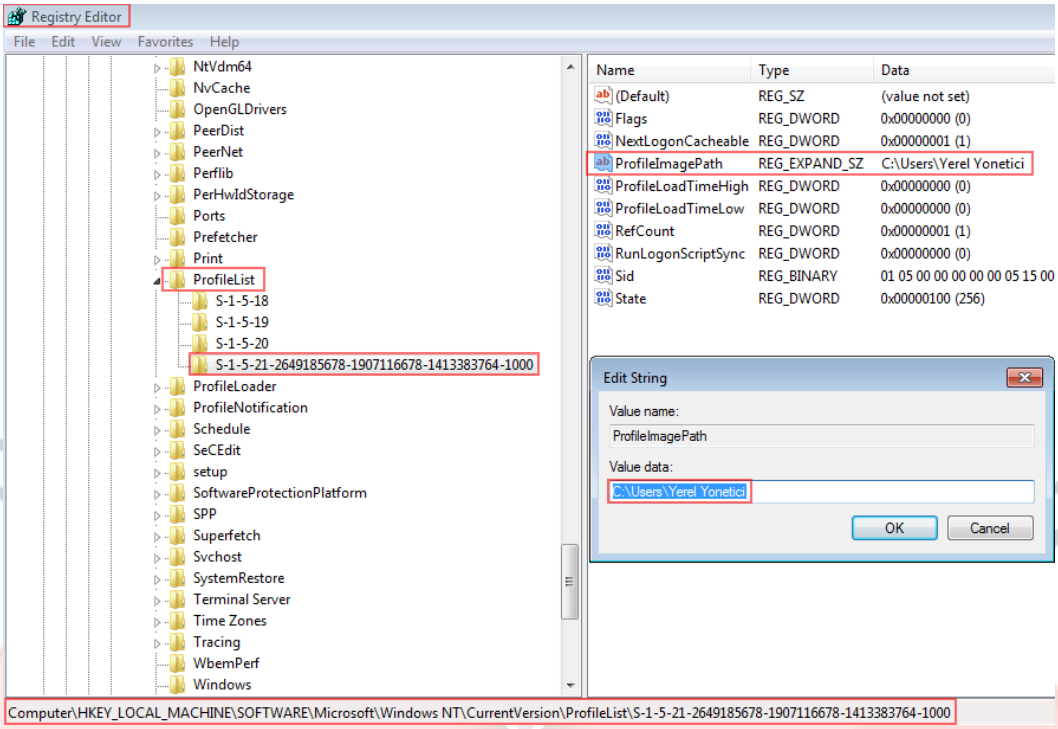
Oturumu açık olan kullanıcının SID değeri kayıt defterinden de elde edilebilir. Kayıt defterini açmak için komut satırından "regedit" komutu çalıştırılabilir.



Şekil - 2: Kayıt Defteri'nin Komut Satırından Açılması

Kayıt Defteri'ndeki aşağıdaki anahtar (key) değeri altında S-1-5-21 ile başlayan anahtar değeri oturumu açık olan kullanıcının SID değeri olup bu anahtar altında oturumu açık olan kullanıcı ile ilgili bir takım bilgiler bulunmaktadır.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList



Şekil - 3: Oturumu Açan Kullanıcının SID Değeri - 2

Tüm Yerel Kullanıcıların SID Değeri

"WMIC" aracı kullanılarak yerel bilgisayardaki tüm kullanıcıların SID değeri elde edilebilir. Bu işlem için aşağıdaki komut kullanılmalıdır.

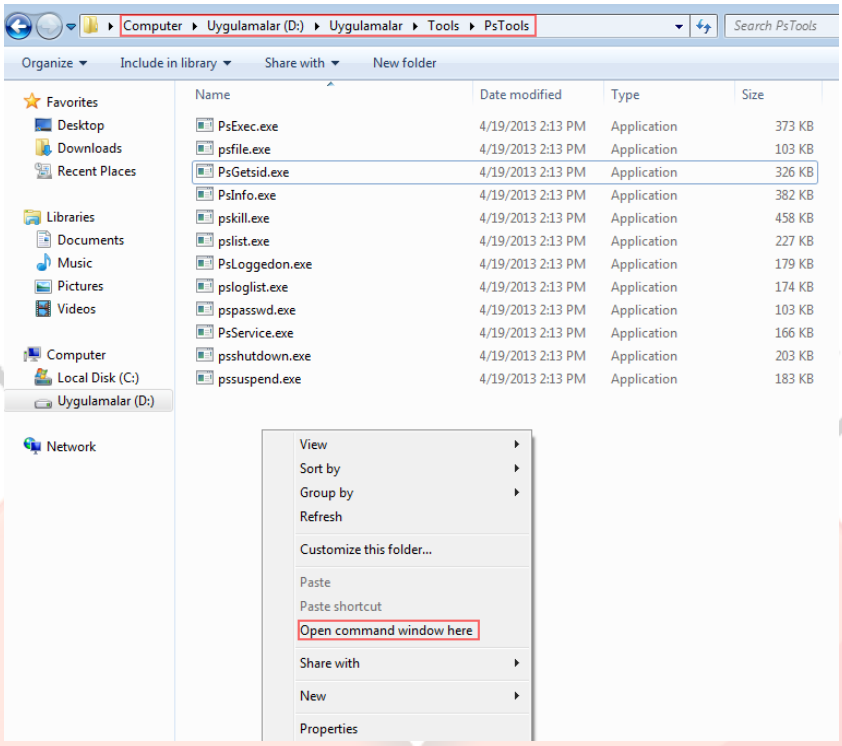
```
wmic useraccount get name, sid
```

```
C:\Users\Yerel Yonetici>wmic useraccount get name,sid
Name             SID
Administrator    S-1-5-21-2649185678-1907116678-1413383764-500
Guest            S-1-5-21-2649185678-1907116678-1413383764-501
test             S-1-5-21-2649185678-1907116678-1413383764-1002
Yerel Yonetici   S-1-5-21-2649185678-1907116678-1413383764-1000
```

Şekil - 4: Yerel Kullanıcıların SID Değeri

Bilgisayarın SID Değeri

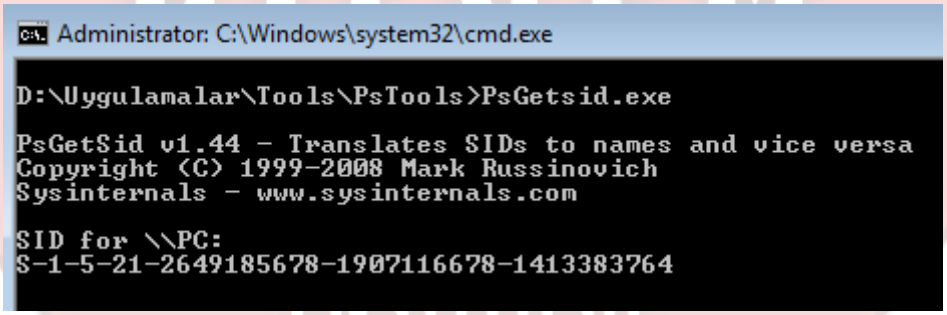
PsGETSid aracı kullanılarak yerel bilgisayarın SID değeri elde edilebilir. Bu araç D: diski içerisindeki Uygulamalar/Tools/PsTools dizini içerisinde yer almaktadır. Bu klasörde SHIFT tuşuna basılarak fareye sağ tıklandığında, "Open command windows here" seçeneği ile komut satırı açılır.



Şekil - 5: Farklı Bir Disk Üzerinde Komut Satırının Başlatılması

Açılan komut satırında "PsGetsid" aracı kullanılarak bilgisayarın SID değeri elde edilir. Bu işlem için aşağıdaki komut kullanılmalıdır.

PsGetsid.exe



Şekil - 6: Bilgisayarın SID Değeri