Uygulama 3 - SAT Değerinin Elde Edilmesi

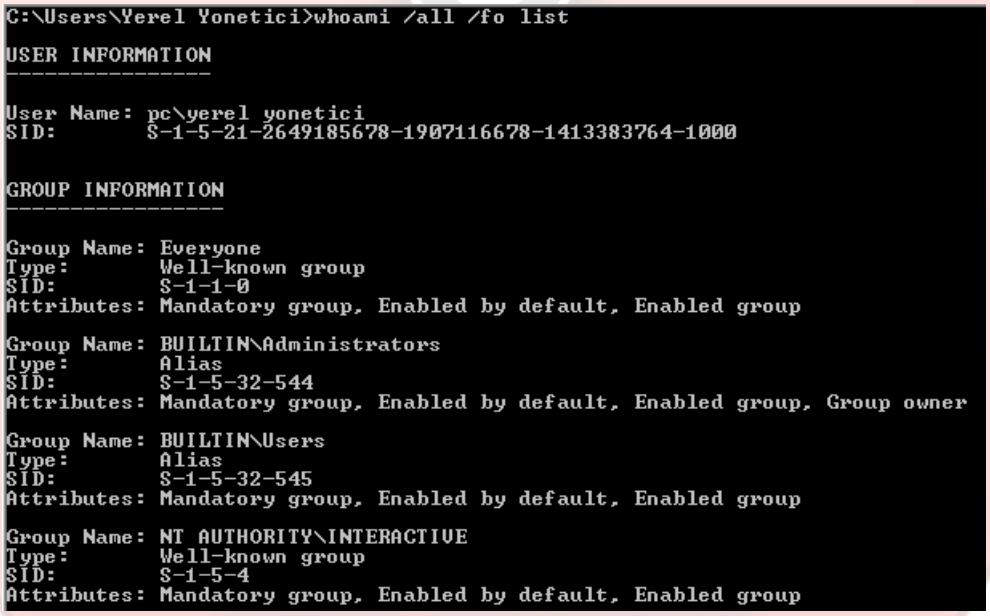
Önbilgilendirme

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

SAT Değerinin Elde Edilmesi

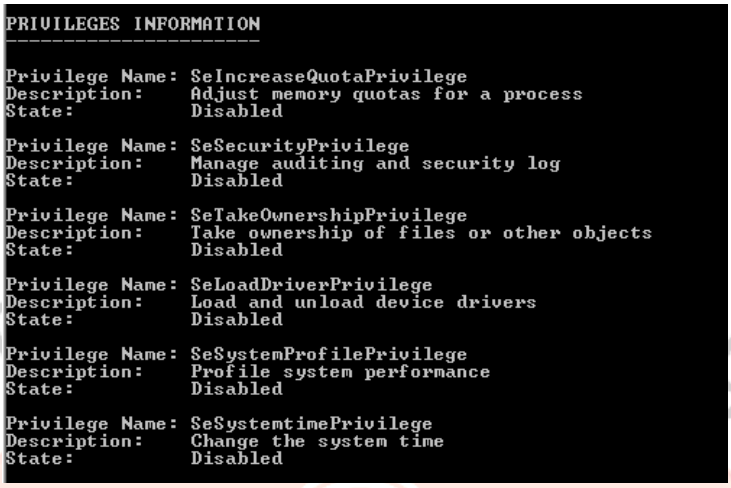
Bir kullanıcıya ait bütün jetonların (Security Access Token (SAT)) elde edilebilmek için "whoami" kullanılabilir. Bu işlem için aşağıdaki komut kullanılmalıdır.

whoami /all /fo list



Şekil - 1: Kullanıcının Kimlik ve Grup Bilgilerinin Listelenmesi

Kullanıcı ve grup bilgileri haricinde, kullanıcının sahip olduğu ayrıcalıklar da elde edilebilir.

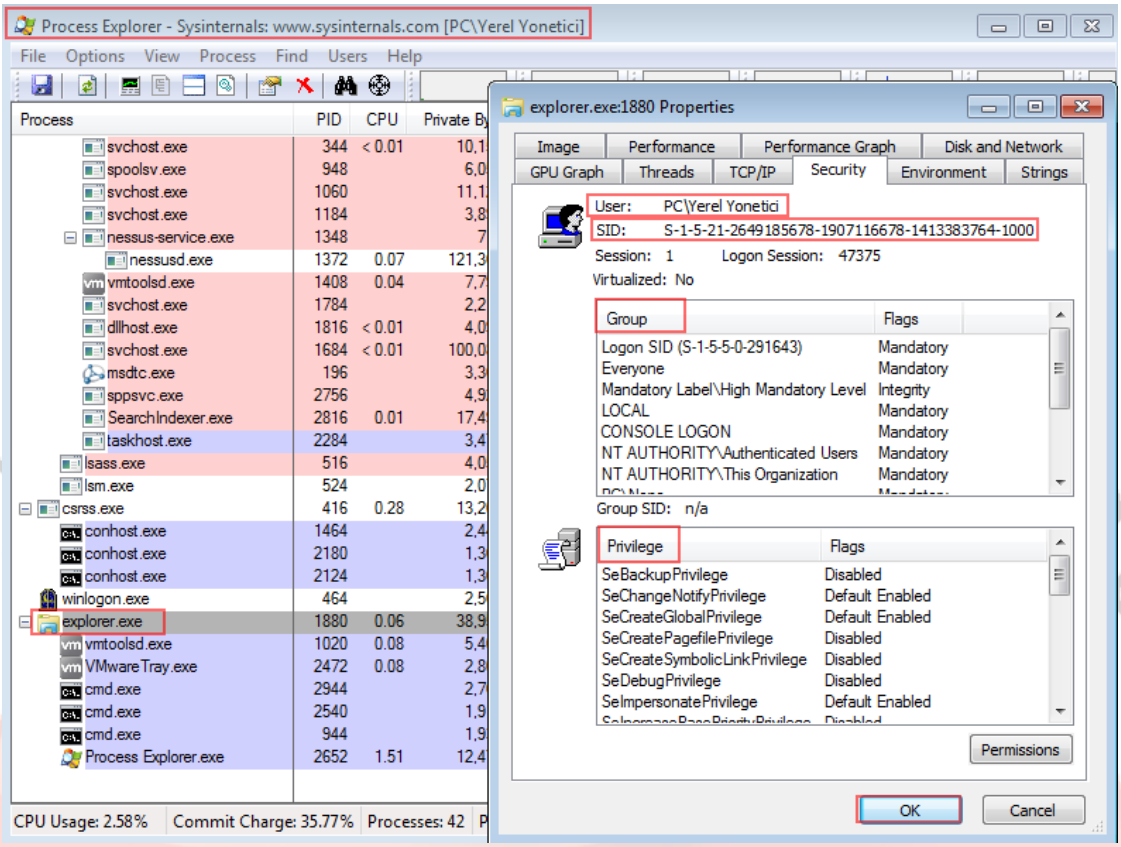


Şekil - 2: Kullanıcının Ayrıcalık Bilgisinin Listelenmesi

Prosesteki Jetonun İncelenmesi

Kullanıcının SID değeri, üye oldukları grupların SID değeri ve kullanıcıların ayrıcalıkları kullanıcının jetonunu oluşturur. Kullanıcı oturum açtığında bu bilgiler oluşturulur ve kullanıcı bir proses çalıştırdığında jetonundaki bilgilerine bakılarak o prosesi çalıştırıp çalıştıramayacağı kontrol edilir. Çalıştırma hakkı varsa, kullanıcının jetonu, prosese eklenir.

Proseslerin ayrıntılı incelenmesi için Process Explorer adlı program kullanılabilir. Bu program, D: diski içerisindeki Uygulamalar dizini içerisinde yer almaktadır. Bu program sağ tıklanarak yönetici haklarıyla açılarak çalışan prosesler incelenebilir. "explorer.exe" prosesinin özelliklerinden Security sekmesinde, o prosesi çalıştıran kullanıcının jeton bilgileri görüntülenebilmektedir.



Şekil - 3: Prosesteki Jeton Bilgilerinin İncelenmesi