

Uygulama 3 - SAT Deęerinin Elde Edilmesi

Önbięilendirme

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

SAT Deęerinin Elde Edilmesi

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

whoami /all /fo list

```
C:\Users\Yerel Yönetici>whoami /all /fo list
USER INFORMATION
-----
User Name: pc\yerel yönetici
SID:      S-1-5-21-2649185678-1907116678-1413383764-1000

GROUP INFORMATION
-----
Group Name: Everyone
Type:      Well-known group
SID:      S-1-1-0
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: BUILTIN\Administrators
Type:      Alias
SID:      S-1-5-32-544
Attributes: Mandatory group, Enabled by default, Enabled group, Group owner

Group Name: BUILTIN\Users
Type:      Alias
SID:      S-1-5-32-545
Attributes: Mandatory group, Enabled by default, Enabled group

Group Name: NT AUTHORITY\INTERACTIVE
Type:      Well-known group
SID:      S-1-5-4
Attributes: Mandatory group, Enabled by default, Enabled group
```

řekil - 1: Kullanıcının Kimlik ve Grup Bięilerinin Listelenmesi

Kullanıcı ve grup bięileri haricinde, kullanıcının sahip olduęu ayrıcalıklar da elde edilebilir.

```
PRIVILEGES INFORMATION
-----
Privilege Name: SeIncreaseQuotaPrivilege
Description:    Adjust memory quotas for a process
State:          Disabled

Privilege Name: SeSecurityPrivilege
Description:    Manage auditing and security log
State:          Disabled

Privilege Name: SeTakeOwnershipPrivilege
Description:    Take ownership of files or other objects
State:          Disabled

Privilege Name: SeLoadDriverPrivilege
Description:    Load and unload device drivers
State:          Disabled

Privilege Name: SeSystemProfilePrivilege
Description:    Profile system performance
State:          Disabled

Privilege Name: SeSystemtimePrivilege
Description:    Change the system time
State:          Disabled
```

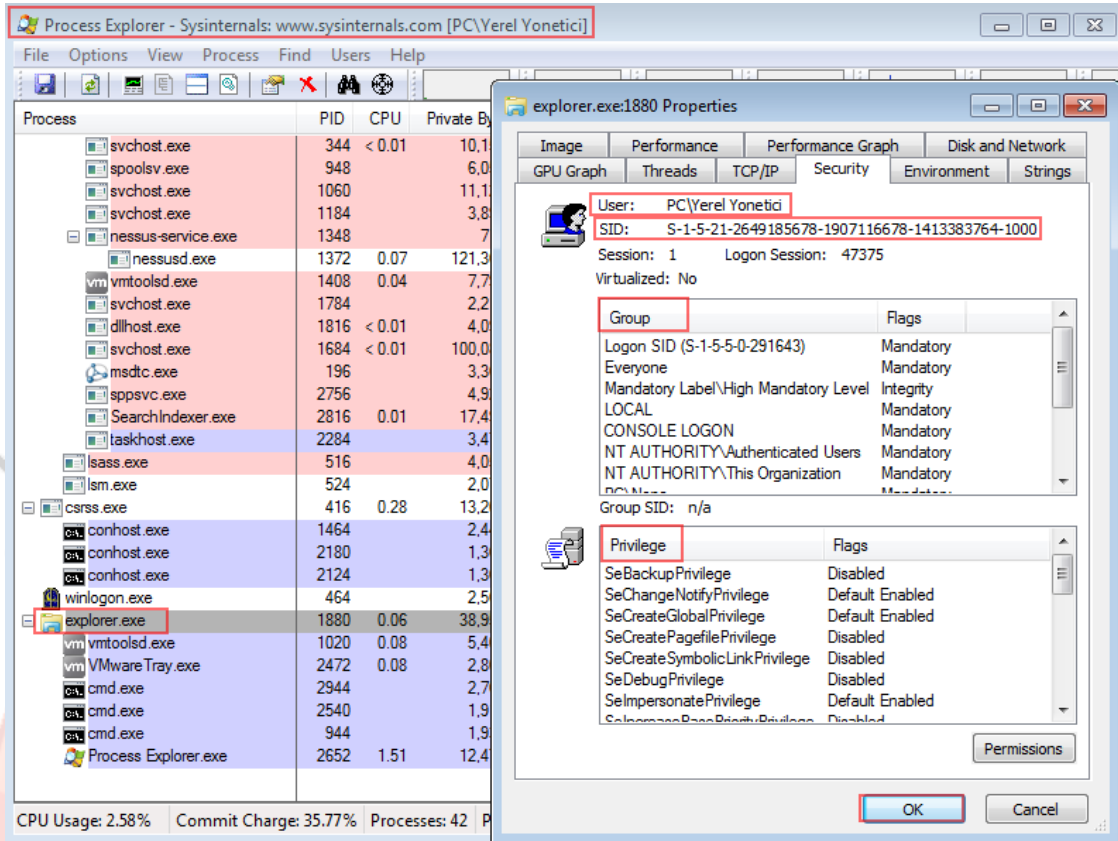
Şekil - 2: Kullanıcının Ayrıcalık Bilgisinin Listelenmesi

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.

**SİBER GÜVENLİK
ENSTİTÜSÜ**



Şekil - 3: Prosesteki Jeton Bilgilerinin İncelenmesi

BİLGEM

SİBER GÜVENLİK
ENSTİTÜSÜ