ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/windows-isletim-sistemi-yetki-yukseltme-calismalari/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Windows%20%C4%B0%C5%9Fletim%20Sisteminde%20Yetki%20Y%C3%BCkseltme%20%C3%87al%C4%B1%C5%9Fmalar%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Sızma testlerinde Windows işletim sistemleri güvenlik uzmanlarının karşısına oldukça fazla çıkmaktadır. Windows işletim sistemleri üzerinde sınırlı hak seviyesinde oturum elde etmek genelde kolay olabilir ancak aynı network'te yer alan bir sonraki sisteme geçebilmek için bulunduğumuz sistemde en yüksek hak seviyesine çıkmamız gerekir.

(Page 3)

2)

Yazı boyunca Windows Server 2012 işletim sistemi üzerinde durulacaktır. Ayrıca PwnAble isimli bir servis ve daha önce zafiyeti duyurulmuş üçüncü parti bir yazılım kullanılacaktır.

(Page 3)

3)

Windows Sistemlerde Bilgi Toplama Amacıyla Kullanılan Araçlar

● accesschk

Sistemdeki kullanıcıların ve kullanıcı gruplarının hangi dosyalara, dizinlere, kayıt defteri girdilerine ve servislere erişim hakkına sahip olduğunu göstermeye yarayan bir tool'dur. Genellikle sistem yöneticileri bu tool'u kulllanır.

https://technet.microsoft.com/en-us/sysinternals/accesschk.aspx

● Process Explorer

Windows Görev Yönetinicisi aracının daha gelişmiş halidir. İleri düzeyde exe ve dll takibi yapabilmesi öne çıkan özelliklerindendir.

https://technet.microsoft.com/tr-tr/sysinternals/processexplorer

● Icacls

Windows sistemlerde kurulum ile beraber gelen bu araç ile dizin ve dosya izinleri bilgilerine erişilebilir ve aynı zamanda bu izinler değiştirilebilir.

NOT: Windows'ta dosyalar, servisler ve diğer tüm objeler DACLs değerlerine sahiptirler. DACLs demek kullanıcıların ve grupların ilgili obje üzerindeki yetkileri demektir. Icacls tool'u ise DACLs'ları okumaya ve değiştirmeye yarar.

(Page 4)

4)

Windows Sistemlerde Yanlış Yapılandırma Ayarlarını Tespit Eden Araçlar

● Windows Privesc Check
- Phyton dilinde geliştirilmiş hedef sistem üzerindeki yapılandırma hatalarından kaynaklanan zafiyetlerin tespitinde kullanılan açık kaynak kodlu bir araçtır. Yapılandırma ayarları kaynaklı zafiyet tespiti alanındaki en popüler araçlardan bir tanesidir. Bu araç aynı zamanda bazı üçüncü parti yazılımların güncelleştirme eksikliklerini de tespit edebilmektedir.

https://github.com/pentestmonkey/windows-privesc-check

● PowerUp
- Powershell ile geliştirilmiş açık kaynak kodlu bu araç ile hedef sistem üzerindeki yapılandırma hatalarından kaynaklanan zafiyetlerin tespiti gerçekleştirilir.

https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp

● WPC-PS
- Powershell ile geliştirilmiş açık kaynak kodlu bu araç ile de hedef sistem üzerindeki yapılandırma hatalarından kaynaklanan zafiyetlerin tespiti gerçekleştirilebilir.

https://github.com/silentsignal/wpc-ps

(Page 4-5)

5)

Windows Yapılandırma Hataları
Aşağıdaki başlıklarda bir Windows işletim sisteminde olabilecek yapılandırma hataları ve detaylarına yer verilmiştir.

a. Güvenli Olmayan Dosya ya da Dizin İzinleri

Windows işletim sistemlerinde herbir servisin/uygulamanın birbirinden bağımsız dizin ve alt dizinleri bulunur. Bu dizin ve alt dizinlerde servislerin/uygulamaların çalıştırılabilir dosyaları başta olmak üzere birçok başka dosya yer alır. Bu noktada genel olarak iki farklı yapılandırma zayıflığı ile karşılaşılmaktadır.

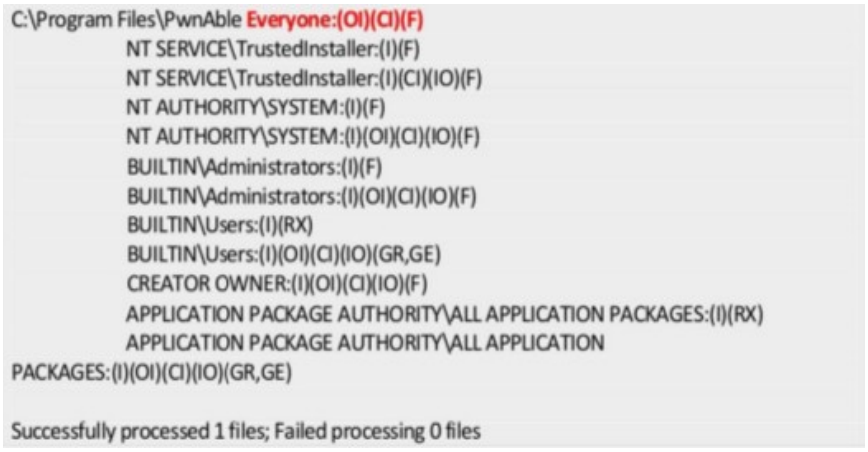
i) Hedef servisin bulunduğu dizinin, alt dizinlerinin veya servis ile ilgili dosyaların izinlerinin güvenilir olarak belirlenmemesi

ii) Direkt olarak servisin çalıştırılabilir dosyasının izninin güvenilir olarak belirlenmemesi

Yukarıda değinilen icacls adlı tool ile hedef dizin ve dosya izinlerini hakkında bilgi alınabilir. Örneğin aşağıda PwnAble adlı servisin dizin ve çalıştırılabilir dosyasının izni icacls tool'u ile sorgulanmıştır.

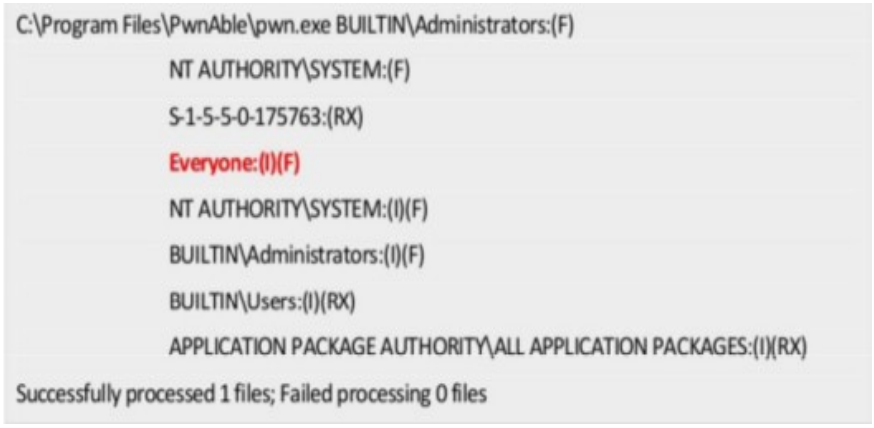
```
> icacls 'C:\Program Files\PwnAble'          // Dizin Sorgulanır
```

Output:



> icacls 'C:\Program Files\PwnAble\pwn.exe' // Çalıştırılabilr dosya sorgulanır

Output:



Sorguların çıktısından da anlaşılabileceği üzere hedef servisin (PwnAble'ın) dizinine ve çalıştırılabilir dosyasına ait izinler Everyone (I)(F) olarak ayarlanmış. Demek ki herhangi bir kullanıcı PwnAble servisinin dizini üzerinde ve çalıştırılabilir dosyası üzerinde işlem yapabilir durumdadır. Buna bir örnek vermek gerekirse mesela PwnAble servisine ait çalıştırılabilir dosyaya saldırgan müdahale edip kendi dosyası ile (örn; meterpreter ile) değiştirebilir ve kurban PwnAble'ı çalıştırıyorum derken meterpreter'i tetikleyerek saldırganın meterpreter session'ı elde etmesine sebep olabilir. Böylece saldırgan sistemi ele geçirebilir.

b. Güvenli Olmayan Kayıt Defteri Değerleri

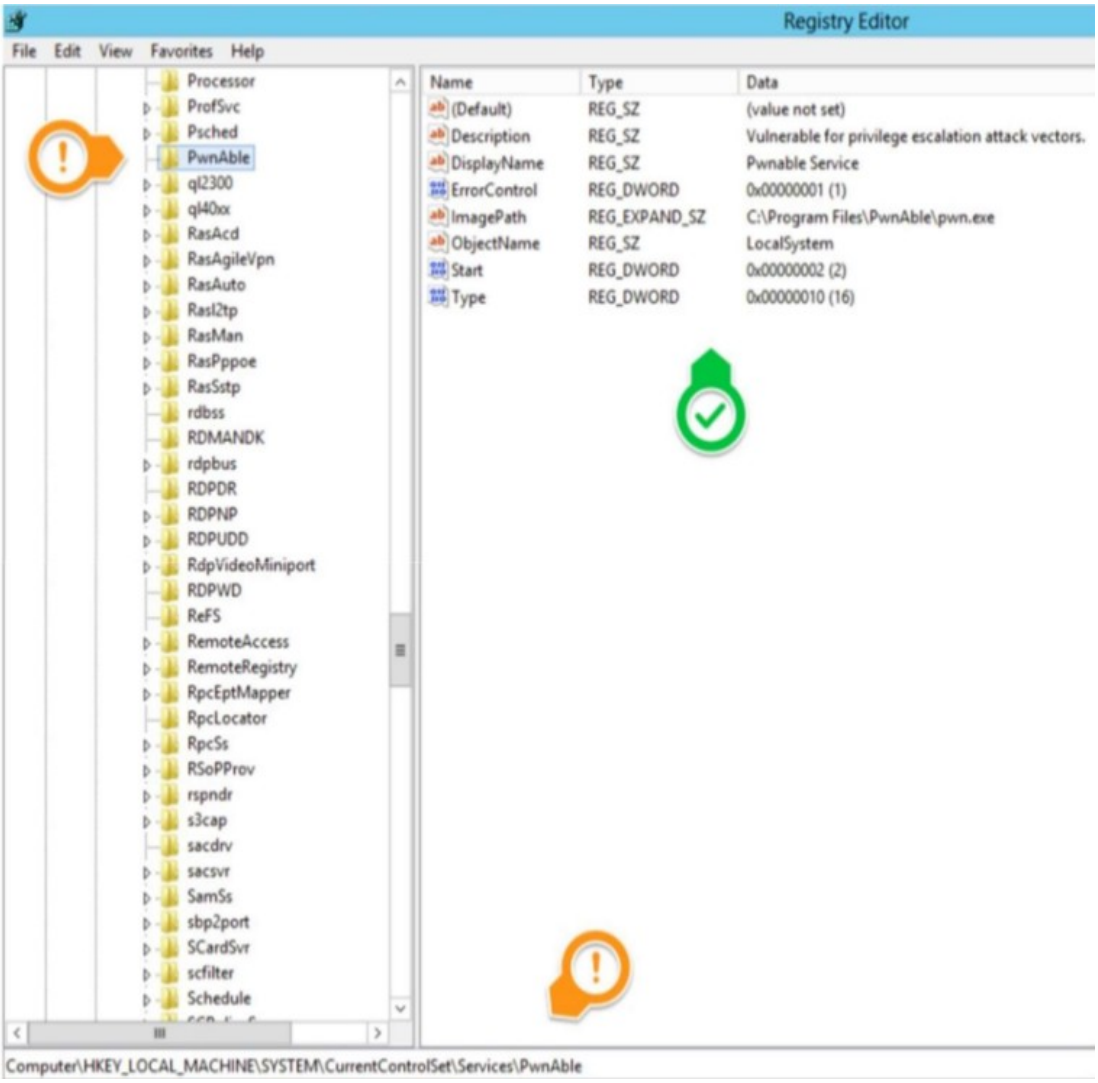
Windows işletim sistemlerinde servisler ile ilgili veriler kayıt defterinin

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services

dizini altında tutulur. Örneğin PwnAble servisinin verileri şu dizinde olacaktır:

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ **PwnAble**

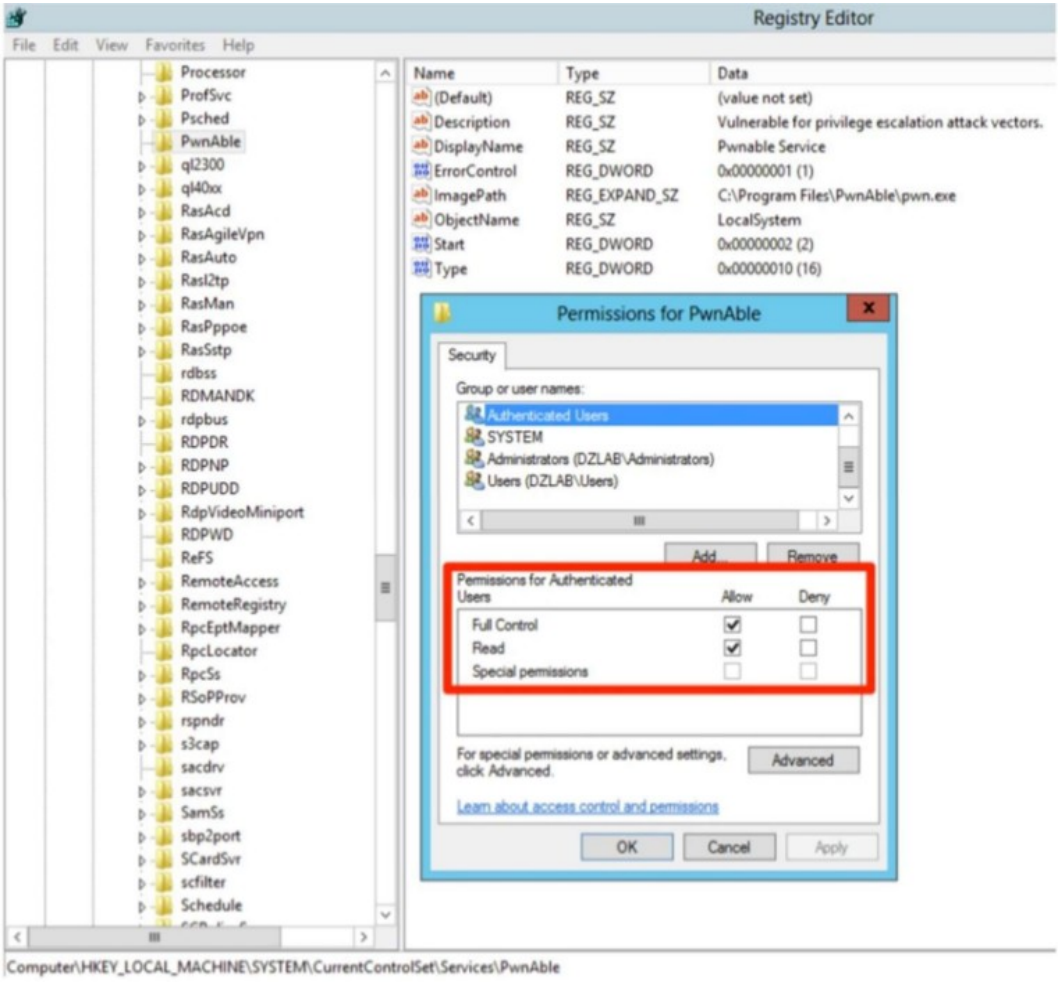
Aşağıda ise PwnAble servisinin kayıt defterinde seçildiği anı görmektesiniz.



İlk ünlem işareti PwnAble klasörünün seçildiğini göstermektedir. İkinci ünlem işareti PwnAble'ın kayıt defterinde yer aldığı dizini göstermektedir:

HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ **PwnAble**

Tick işareti ise PwnAble servisine ait kayıt defterinde yer alan verileri göstermektedir. PwnAble servisinin izinlerine kayıt defteri üzerinden bakacak olursak



görüldüğü üzere mavi ışıkla belirtilmiş Authenticated Users grubuna Full Control izni verilmiştir. Bu, işletim sistemi üzerinde oturumu olan herhangi bir kullanıcının ilgili kayıt defteri değerlerini değiştirebileceği anlamına gelmektedir. Örneğin sisteme kısıtlı haklarla sızan bir saldırgan Full Control izni sayesinde PwnAble servisinin sıralanan verilerinden ImagePath değerine kendi uygulamasının dizin yolunu girerek manipule edebilir ve böylelikle saldırgan kendi zararlı uygulamasını PwnAble servisinin haklarında çalışabilecek seviyeye çıkararak sisteme hükmedebilir.

c. Güvenli Olmayan Servis İzinleri

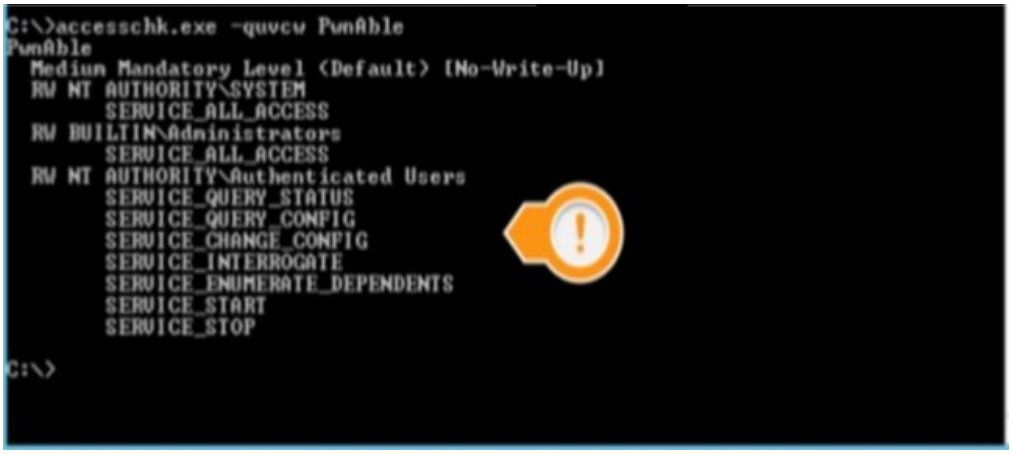
Windows işletim sistemlerinde servis ekleme, ayarlarını değiştirme gibi haklar sadece Administrator grubunda olan kullanıcılarda bulunur. Fakat bazı durumlarda Administrator grubuna dahil olmayan kullanıcılar için de servisler üzerinde işlem yapabilme hakkı tanınabilir. İşte bu tanınan haklar dikkat edilmediği takdirde saldırganların işine yarabilir ve saldırganların kendi script'lerini (servislerini) Administrator seviyesinde çalıştırmalarına yol açabilir. Böylece sistem hack'lenebilir.

Örneğin Administrator grubunda olmayan “halil” kullanıcısı NT AUTHORITY\SYSTEM gibi yüksek seviyeli bir yetkide çalışan PwnAble servisini başlatma, durdurma ve yapılandırma yetkilerine sahip olsun ve saldırgan da halil oturumuyla sisteme sızmış olsun.

Böylesi bir senaryoda saldırgan sisteme sızdığında örneğin PwnAble servisi üzerindeki yetkisini öğrenmek isteyecektir. Bunun için accesschk tool'unu aşağıdaki gibi kullanabilir:

```
> cd c:                                  // C dizinine geçilir.
C:\ > accesschk.exe -quvcw PwnAble       // accesschk tool'u çalıştırılır.
```

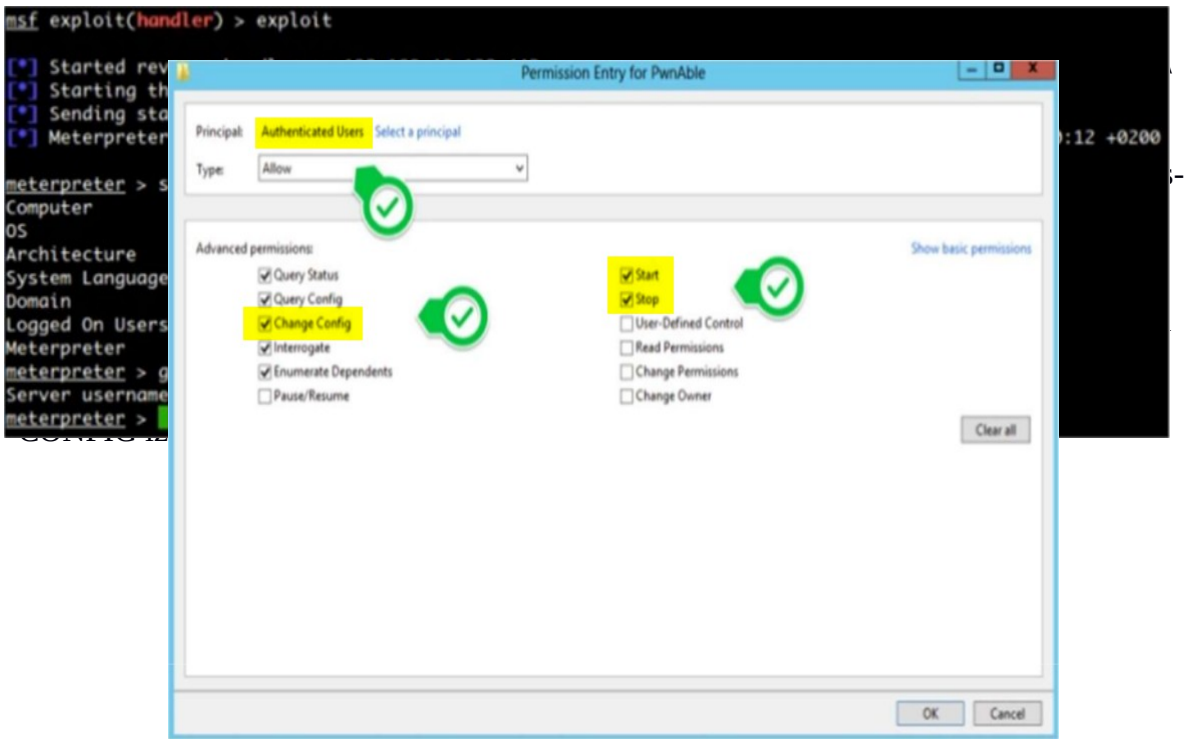
Output:



Görüldüğü üzere halil kullanıcısı olarak PwnAble servisi üzerinde CHANGE_CONFIG, START ve STOP haklarına sahipmişiz. Yetkisi en üst seviyede olan bir servisi (PwnAble'ı) manipule edebilme iznine sahip olduğumuza göre sırasıyla aşağıdaki komutları CMD ekranına girebiliriz ve böylelikle önce PwnAble servisini durdururuz (STOP), sonra PwnAble servisinin çalıştırılabilir dosyasını meterpreter ile değiştiririz (CHANGE_CONFIG) ve son olarak da PwnAble servisini tekrar başlatırız (START).

```
> sc stop PwnAble
> sc config binPath=”C:\Users\halil\Desktop\meterpreter.exe”
> sc start PwnAble
```

Böylece NT AUTHORITY\SYSTEM yetkisine sahip nur topu gibi bir meterpreter'imiz olmuş olur (NOT: Bu süreç esnasında bir hata meydana geliyormuş, ne hakkında olduğundan PDF bahsediyor. Anlaşılmadığından buraya not alınmamıştır).



(Bu pencereye nasıl ulaşıldığı hakkında bir bilgi verilmemiş)

İşte yukarıdaki gibi bir işlem yapıldığı için saldırgan basit bir account olan halil ile PwnAble servisini manipule edebilmiştir ve onun izinleriyle meterpreter oturumunu üst seviyede bir yetkiyle çalıştırabilmiştir.

d. Servislere Ait Çalıştırılabilir Dosyaların Path'lerinin Unquoted Halde Bırakılması

Windows işletim sistemlerinde bir servisin kayıt defterindeki dizin yolu içerisinde eğer boşluk varsa ve bu dizin yolu tırnak işaretleri arasına alınmamışsa bu bir zafiyet teşkil eder. Bu zafiyet Windows işletim sistemlerindeki CreateProcess adlı bir fonksiyonun servis path'ini alan parametresinin işleniş tarzından kaynaklanmaktadır. (CreateProcess için bkz. https://msdn.microsoft.com/en-us/library/windows/desktop/ms682425(v=vs.85).aspx) Örneğin pwn process.exe adlı bir servisimiz olsun ve dizini de şu şekilde olsun:

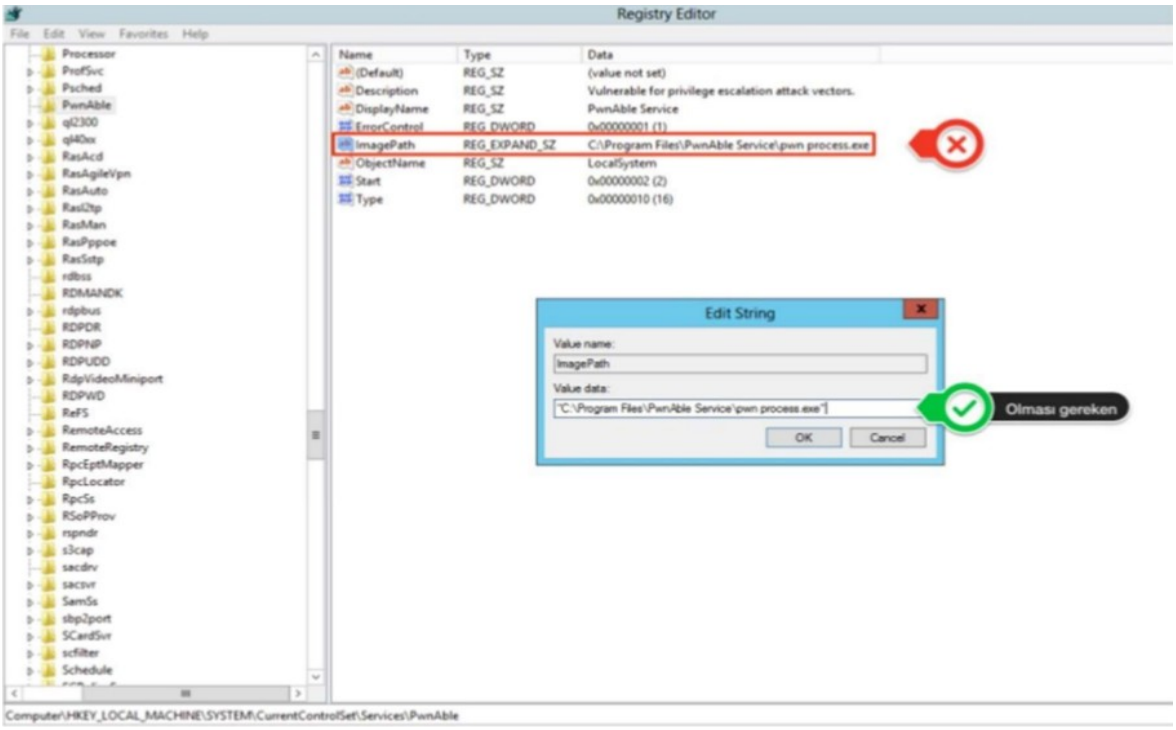
C:\Program Files\PwnAble Service\pwn process.exe

İşletim sistemi bu dizini aldığında ilgili servisin çalıştırılabilir dosyasına erişebilmek için her boşlukta exe'yi buldum mu kontrolü yapacaktır. Yani yukarıdaki dizini aldığı takdirde sırasıyla aşağıdaki dizin yollarını deneyecektir:

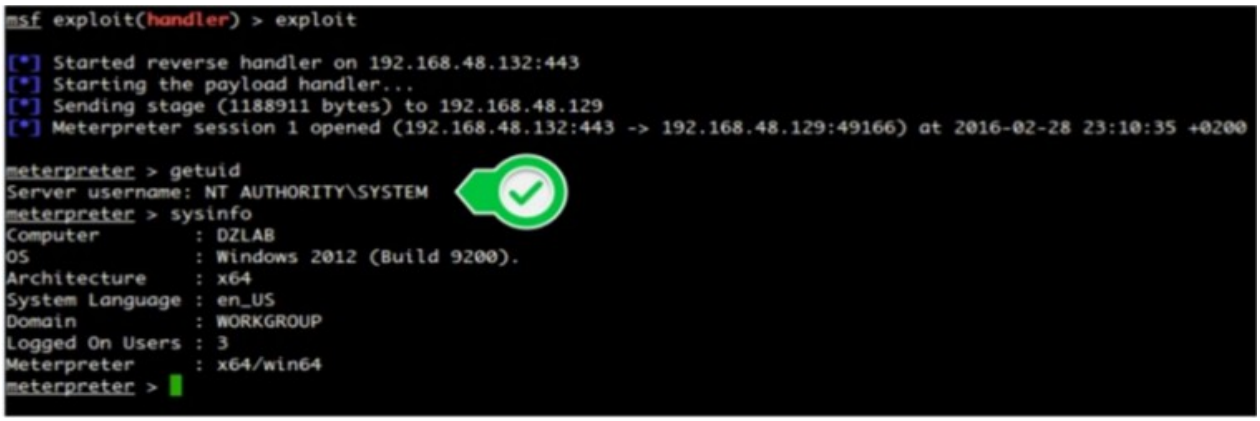
C:\Program.exe // “Program Files”ın ilk kelimesi
C:\Program Files\PwnAble.exe // “PwnAble Service”in ilk kelimesi
C:\Program Files\PwnAble Service\pwn.exe // “pwn process”in ilk kelimesi
C:\Program Files\PwnAble Service\pwn process.exe
Herbir boşlukta servisin çalıştırılabilir dosyası için bir varsayım yapılır ve varsayılan exe dosyası var mı diye kontrol edilir. Bu işlem exe dosyası bulunana kadar devam eder. Denemelerin en sonunda servisin exe'si bulunacağından sistem onu çalıştırır ve servis böylece başlatılmış olur. Böylesi bir durumda saldırgan eğer bu okunan ara dizinlerden birisine uygun isimli bir payload ekleyebilirse sistemi ele geçirmiş olur. Nasıl mı? Örneğin

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

yukarıdaki servis dizin yolu kayıt defterinde tırnaksız bir şekilde yer alıyor olsun.



Bu durumda zafiyet sebebi olan CreateProcess fonksiyonu path'i okurken önce C:\Program.exe'yi deneyektir. Şayet saldırgan C sürücüsüne Program.exe isimli bir meterpreter payload'u koyabilirse işte o zaman CreateProcess fonksiyonu direkt saldırganın bu dosyasını çalıştıracaktır ve servisin gerçek dizin yolu olan C:\Program Files\PwnAble Service\ dizini altındaki pwn process.exe'ye bakmayacaktır. Böylece saldırgan kendi makinasının komut satırında PwnAble servisinin yetkisine sahip bir meterpreter session'ı elde edecektir.



NOT: Normalde C sürücüsünün kök dizinine dosya atabilmek güçtür. Çünkü izin gerektirir. Dolayısıyla meterpreter payload'unu PwnAble servisinin bulunduğu dizinin içerisine koyarak yine aynı işlem gerçekleştirilebilir. Şöyle ki PwnAble servisine ait çalıştırılabilir dosyanın dizini şuydu:

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

Eğer pwn process.exe'sinin bulunduğu dizinin içerisine pwn.exe isimli bir meterpreter payload'u koyarsak CreateProcess fonksiyonu path'deki boşluk dolayısıyla önce pwn.exe'yi deneyeceğinden meterpreter tetiklenmiş olacaktır ve esas

servis olan pwn process.exe'ye bakılmayacaktır. Böylece meterpreter payload'ı PwnAble servisinin yetkisiyle hedef sistemde çalışır olacaktır.

e. Getsystem Komutu ile Hak Yükseltmek

Herhangi bir Windows işletim sisteminde Meterpreter oturumu elde edildikten sonra hedef account Local Administrator grubuna aitse bu durumda Meterpreter'in getsystem komutu kullanılarak en yüksek hak seviyesi olan NT AUTHORITY\SYSTEM'e çıkılır.