

**Hacking (Reset) Password Windows dengan chntpw pada
Live USB Linux BackBox 5.0
(Tugas Mata Kuliah Keamanan Jaringan Komputer)**



Nama: Azwar Hidayat

NIM: 09011281520126

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

2018

Hacking Password Window

Pada windows, ada beberapa cara melakukan *hacking password* diantaranya metode *bruteforce* dengan menggunakan *john the ripper*, menggunakan *cain and abel*, ataupun menggunakan *live usb linux*. Kali ini, hal yang akan coba dilakukan adalah *mereset password windows* menggunakan *chntpw* yang merupakan suatu *tools* yang ada pada linux di beberapa distro seperti *backbox* dan *kali linux* yang memanfaatkan file SAM yang ada di windows.

1. Membuat *bootable disk* dari *iso backbox* menggunakan *tools* salah satunya adalah *rufus*.
2. Setelah proses selesai, lalu masuk ke *boot menu* dan *boot* menggunakan *pendrive*.
3. Pada *boot menu*, pilih **try backbox without installing** lalu akan masuk ke *home* dari linux.
4. Buka terminal dan masuk ke *user root* dengan *command* **sudo su**, lalu kita buka isi dari hardisk yang dimiliki dengan *command* **ls /dev/sd***

```
backbox@backbox:~$ sudo su
root@backbox:/home/backbox# ls /dev/sd*
/dev/sda /dev/sda2 /dev/sda4 /dev/sda6 /dev/sda8 /dev/sdb1
/dev/sda1 /dev/sda3 /dev/sda5 /dev/sda7 /dev/sdb
```

Gambar 1. Langkah awal

5. Lalu *mount disk* dengan *command* **mount dev/sda beberapa /mnt**

```
root@backbox:/home/backbox# mount /dev/sda1 /mnt
root@backbox:/home/backbox# mount /dev/sda2 /mnt
root@backbox:/home/backbox# mount /dev/sda4 /mnt
```

Gambar 2. Mount Disk

6. Cek isi disk yang *dimount* apakah ada file yang kita cari dengan *command* **cd /mnt && ls**

```
root@backbox:/home/backbox# cd /mnt && ls
AMTAG.BIN          john              Python27
AppServ            logfile.log       Recovery
bootmgr            logs              $Recycle.Bin
BOOTNXT            Lyrics            [Smad-Cage]
cvavr2             MSOCache         swapfile.sys
Dev-Cpp            NST              System Volume Information
Documents and Settings OEN              Users
drv.log            pagefile.sys     WINDOWS
```

Gambar 3. Melihat isi hasil mount

7. Terlihat bahwa ada folder **WINDOWS** yang menyimpan file SAM, langkah selanjutnya adalah masuk ke dalam folder tersebut dengan *command* **cd** setelah itu **ls** untuk melihat detail isinya.

```

root@backbox:/mnt# cd WINDOWS/System32/config/
root@backbox:/mnt/WINDOWS/System32/config# ls
BBI
BBI{780ac98d-0bcf-11e7-a943-e41d2d128090}.TM.blf
BBI{780ac98d-0bcf-11e7-a943-e41d2d128090}.TMContainer000000000000000001.regtra
ns-ms
BBI{780ac98d-0bcf-11e7-a943-e41d2d128090}.TMContainer000000000000000002.regtra
ns-ms
BBI.LOG1
BBI.LOG2
bcdmigrate
BCD-Template
BCD-Template.LOG
BCD-Template.LOG1
BCD-Template.LOG2
COMPONENTS
COMPONENTS{4e07463c-0c1c-11e7-a943-e41d2d718a20}.TM.blf
COMPONENTS{4e07463c-0c1c-11e7-a943-e41d2d718a20}.TMContainer000000000000000001
.regtrans-ms
COMPONENTS{4e07463c-0c1c-11e7-a943-e41d2d718a20}.TMContainer000000000000000002
.regtrans-ms
COMPONENTS.LOG1
COMPONENTS.LOG2
DEFAULT
SAM
SAM{4e074611-0c1c-11e7-a943-e41d2d718a20}.TM.blf
SAM{4e074611-0c1c-11e7-a943-e41d2d718a20}.TMContainer000000000000000001.regtra
ns-ms
SAM{4e074611-0c1c-11e7-a943-e41d2d718a20}.TMContainer000000000000000002.regtra
ns-ms
SAM.LOG1
SAM.LOG2

```

Gambar 4. Ls direktori system32 windows

8. Pada gambar diatas, terlihat ada file **SAM** yang mana menyimpan informasi *password* dari *user*. Lalu, langkah selanjutnya adalah membuka *chntpw* dengan *command sudo chntpw*

```

root@backbox:/mnt/WINDOWS/System32/config# sudo chntpw
chntpw version 1.00 140201, (c) Petter N Hagen
chntpw: change password of a user in a Windows SAM file,
or invoke registry editor. Should handle both 32 and 64 bit windows and
all version from NT3.x to Win8.1
chntpw [OPTIONS] <samfile> [systemfile] [securityfile] [otherreghive] [...]
-h          This message
-u <user>   Username or RID (0x3e9 for example) to interactively edit
-l          list all users in SAM file and exit
-i          Interactive Menu system
-e          Registry editor. Now with full write support!
-d          Enter buffer debugger instead (hex editor),
-v          Be a little more verbose (for debugging)
-L          For scripts, write names of changed files to /tmp/changed
-N          No allocation mode. Only same length overwrites possible (very safe
mode)
-E          No expand mode, do not expand hive file (safe mode)

```

Gambar 5. Sudo chntpw

9. Lalu masuk ke *chntpw* mode *interactive* menu dengan *command chntpw -i*
10. Setelah itu, pada menu *chntpw* pilih nomor **1** untuk melakukan edit data user dan password

```

<=====> chntpw Main Interactive Menu <=====>

Loaded hives: <SAM>

 1 - Edit user data and passwords
 2 - List groups
  - - -
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 1

===== chntpw Edit User Info & Passwords =====

| RID - |----- Username -----| Admin? | - Lock? --|
| 03e9 | acer                      | ADMIN  | dis/lock  |
| 01f4 | Administrator             | ADMIN  | dis/lock  |
| 01f7 | DefaultAccount           |        | dis/lock  |
| 01f5 | Guest                     |        | dis/lock  |

```

Gambar 6. Chntpw Main Interactive Menu

11. Akan muncul seperti gambar diatas setelah dipilih pilihan nomor 1, selanjutnya kita akan diminta untuk memasukan RID untuk melakukan edit user info dan password. Pada percobaan ini, acer merupakan user uji yang diberikan password. Oleh karena itu, RID acer perlu dimasukkan kedalam command seperti gambar berikut

```

===== chntpw Edit User Info & Passwords =====

| RID - |----- Username -----| Admin? | - Lock? --|
| 03e9 | acer                      | ADMIN  | dis/lock  |
| 01f4 | Administrator             | ADMIN  | dis/lock  |
| 01f7 | DefaultAccount           |        | dis/lock  |
| 01f5 | Guest                     |        | dis/lock  |

Please enter user number (RID) or 0 to exit: [3e9] 03e9
===== USER EDIT =====

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

```

Gambar 7. Edit user info dan password

12. Setelah itu akan didapatkan informasi yang memuat tentang akses user tersebut

```

00000220 = Administrators (which has 2 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)  |

```

Gambar 8. User Info

13. Selanjutnya, kita akan menghapus kan password dengan memilih pilihan 1, hingga muncul *password cleared* dan proses selesai.

```
- - - - 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] > 1
Password cleared!
```

Gambar 9. Clear (blank) password

14. Setelah proses selesai, maka proses penghapusan pun selesai untuk mengeluarkan dari menu *edit user info* pilih q

```
- - - - 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
```

Gambar 10. Quit

15. Untuk keluar dari *chntpw* pilih q, lalu *save changes* pada **SAM File**

```
<=====> chntpw Main Interactive Menu <=====>
Loaded hives: <SAM>

1 - Edit user data and passwords
2 - List groups
- - -
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM>
Write hive files? (y/n) [n] : y
0 <SAM> - OK
```

Gambar 11. Quit chntpw

16. Selanjutnya reboot system dan masuk ke windows tanpa password

Keunggulan reset dengan chntpw dibanding menebak password menggunakan metode bruteforce

- Hanya membutuhkan waktu singkat
- Lebih efisien dalam penggunaannya
- Lama pengerjaan tidak bergantung dengan tingkat kerumitan password dari user.

Kelemahan

- Tidak mendapatkan passwordnya melainkan melakukan reset / penghapusan password dari itu sehingga akan sangat mudah terlacak apabila komputer tersebut telah di hack.