

TUGAS V
MATA KULIAH KEAMANAN JARINGAN KOMPUTER



Oleh :

Rofby Hidayadi 09011281020132

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D.

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2018

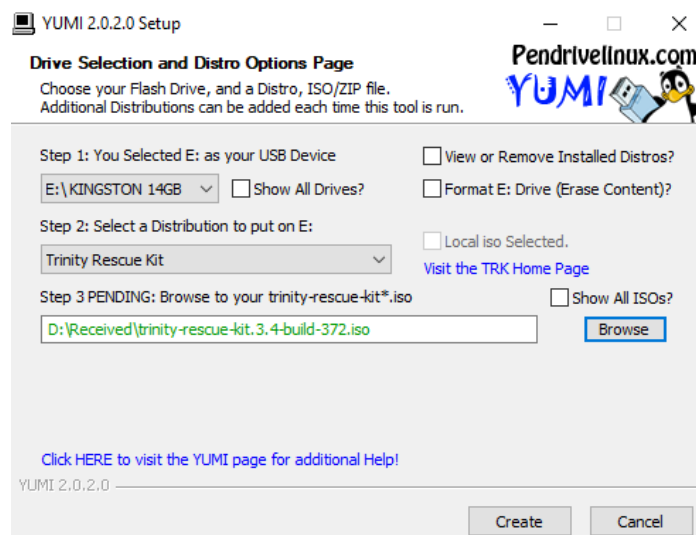
I. Judul Tugas

Hacking Computer Password

II. Prosedur

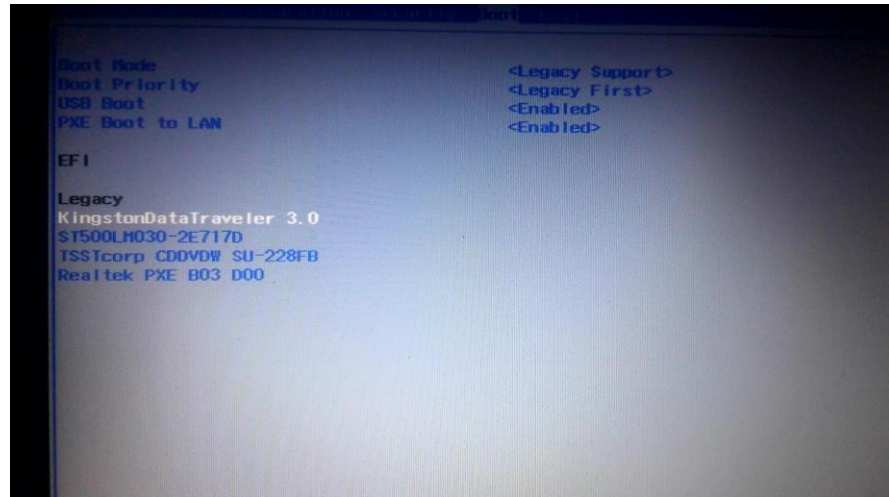
Untuk melakukan hack pada password komputer terdapat 2 cara, yaitu cara pertama dengan menggunakan USB Flash Drive (BIOS) dan menggunakan tool tambahan untuk mendapatkan file database SAM. Berikut adalah cara pertama dengan menggunakan USB Flash Drive (BIOS) dengan tools Trinity Rescue Kit. Adapun langkah-langkahnya adalah sebagai berikut :

1. Download ISO tools Trinity Rescue Kit.
2. Kemudian Burn ISO tools Trinity Rescue Kit yang telah didownload ke USB Flash Drive.



Gambar 1. Proses Burning ISO tools Trinity Rescue Kit

3. Lalu, masukkan USB Flash Drive ke PC/laptop target (PC/laptop dalam keadaan mati).
4. Selanjutnya, hidupkan PC/laptop target dan masuk ke menu BIOS dengan cara menekan F2 atau F10 (tergantung jenis PC/laptop target). Dilanjutkan memilih BOOT menu, kemudian aturlah agar system reboot dari USB Flash Drive.



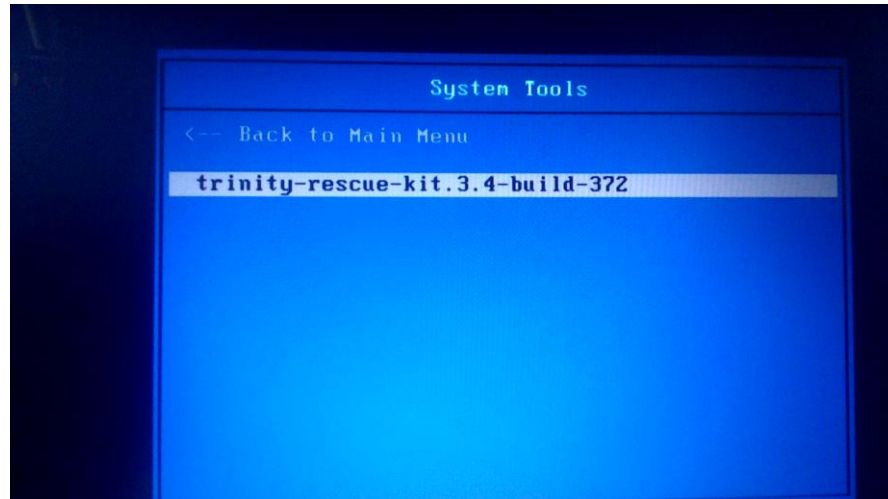
Gambar 2. Menu BIOS PC/Laptop Target

5. Kemudian simpan pengaturan tersebut dilanjutkan dengan reboot system.



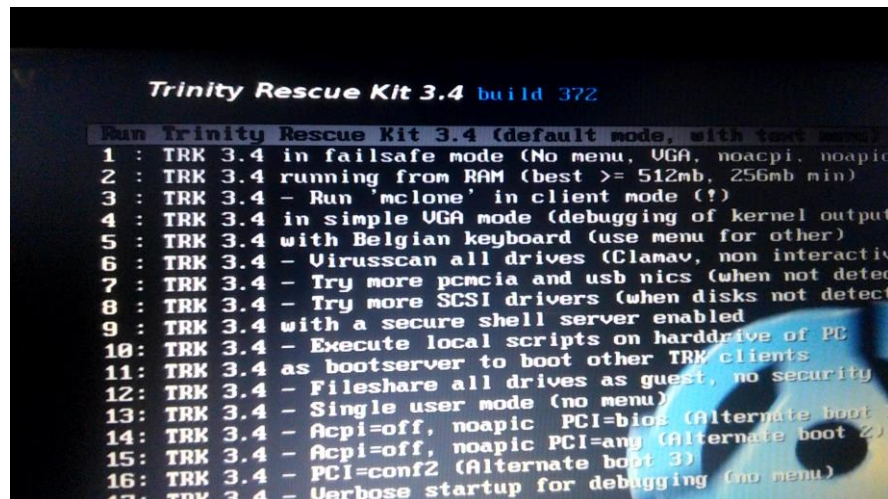
Gambar 3. Tampilan Setelah System Reboot

6. Lalu, pilih system tools yang dilanjutkan dengan memilih tools Trinity Rescue Kit.



Gambar 4. Tampilan Setelah System Tools

7. Selanjutnya, otomatis tools Trinity Rescue Kit akan running dan mencari file TRK USB Flash Drive.



Gambar 5. Menu Tools Trinity Rescue Kit

8. Setelah beberapa saat, akhirnya ditemukanlah Trinity Rescue Kit USB Flash Drive yang dimaksud.

```
usb 2-2: new high speed USB device us
scsi 1:0:0:0: Direct-Access Kings
sd 1:0:0:0: Attached scsi generic sgl
sd 1:0:0:0: [sdb] 7856128 512-byte lo
sd 1:0:0:0: [sdb] Write Protect is of
sd 1:0:0:0: [sdb] Assuming drive cache
sd 1:0:0:0: [sdb] Assuming drive cache
sdb: sdb1
sd 1:0:0:0: [sdb] Assuming drive cache
sd 1:0:0:0: [sdb] Attached SCSI remove
input: ImPS/2 Logitech Wheel Mouse as
md: Waiting for all devices to be avai
md: If you don't use raid, use raid=no
md: Autodetecting RAID arrays.
md: Scanned 0 and added 0 devices.
md: autorun ...
md: ... autorun DONE.
RAMDISK: gzip image found at block 0
UFS: Mounted root (ext2 filesystem) rec
Freeing unused kernel memory: 508k free
INIT: version 2.88...
```

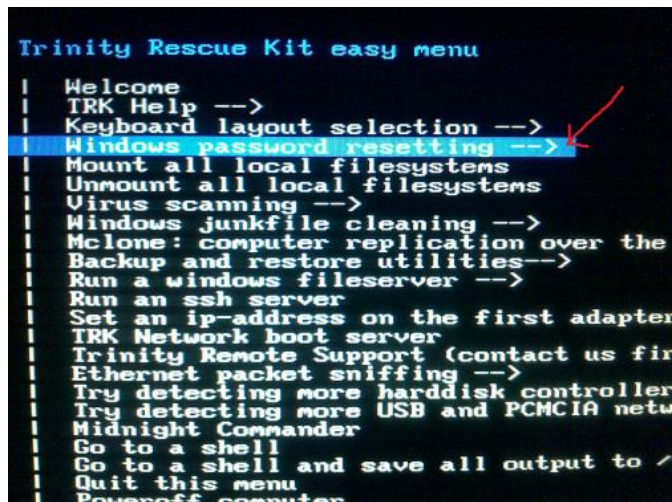
Gambar 7. Trinity Rescue Kit USB Flash Drive

9. Selanjutnya, ketikkan sdb1 pada console.

```
please use A
sticks (sleep 5
rives once more
found (e.g. 'sda1'): sdb1_
```

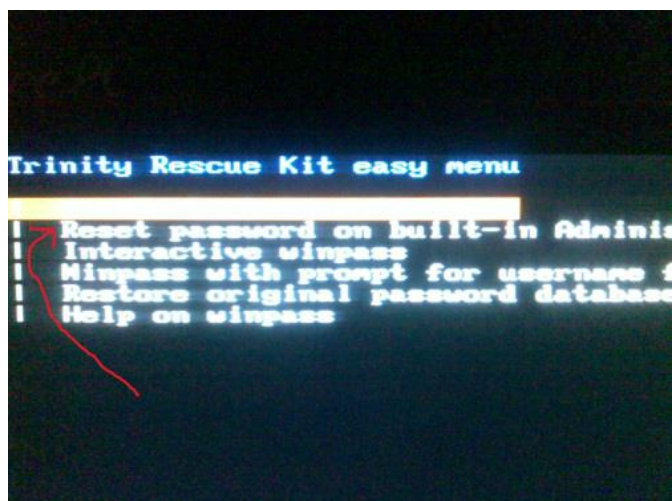
Gambar 8. Ketikkan sdb1 Pada Console

10. Kemudian, sistem akan otomatis masuk ke Trinity Rescue Kit Easy Menu. Lalu, pilih Windows Password Resetting.



Gambar 9. Trinity Rescue Kit Easy Menu

11. Lalu, pilih Reset Password On Build-in Administrator (Default Action).



Gambar 10. Menu Reset Password

12. Lalu, tools Trinity Rescue Kit akan mencari letak File System Windows PC/laptop target yang akan direset passwordnya. Disini ditemukan dilokasi 1 yaitu berisi data sda2/windows. Selanjutnya, ketikkan 1 pada console.

```
Reset password on built-in Administrator
| Interactive winpass
| Winpass with prompt for username first
| Restore original password database
| Help on winpass

(command: winpass)
Searching and mounting all filesystems on
Remounting NTFS partitions with ntfs-3g
Result of mounting:
/dev/sda1 on /sda1 type fuseblk (rw,noatime
size=4896)
/dev/sda2 on /sda2 type fuseblk (rw,noatime
size=4896)
/dev/sda3 on /sda3 type fuseblk (rw,noatime
size=4896)
Windows NT/2K/XP installation(s) found in:
1: /sda2/Windows
Make your choice or 'q' to quit [1]: 1_
```

Gambar 11. File System Windows PC/Laptop Target

13. Kemudian secara otomatis akan masuk ke User Edit Menu. Lalu, ketikkan 1 untuk memilih Clear (Blank) User Password pada console.

```
] Domain trust ac | [ ] Wks trust a
[X] Pwd don't expir | [ ] Auto lockou
[ ] (unknown 0x10) | [ ] (unknown 0x
Failed login count: 20, while max tri
Total login count: 1
** No NT ND4 hash found. This user pr
** No LANMAN hash found either. Sorry

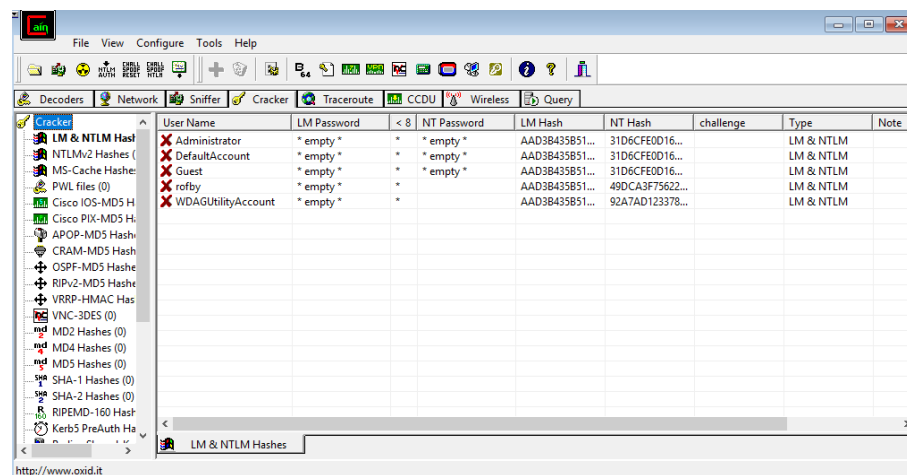
-- -- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (can
3 - Promote user (make user an admini
4 - Unlock and enable user account [p
q - Quit editing user, back to user s
Select: [q] > 1_
```

Gambar 12. Clear (Blank) User Password

14. Selanjutnya, keluar dari tools Trinity Rescue Kit dan lakukan reboot pada PC/laptop target (jangan lupa untuk mengubah kembali pengaturan BOOT pada Menu BIOS ke default). Maka, PC/laptop target yang awalnya memiliki password, setelah dilakukan langkah-langkah diatas password tersebut akan hilang atau clear.

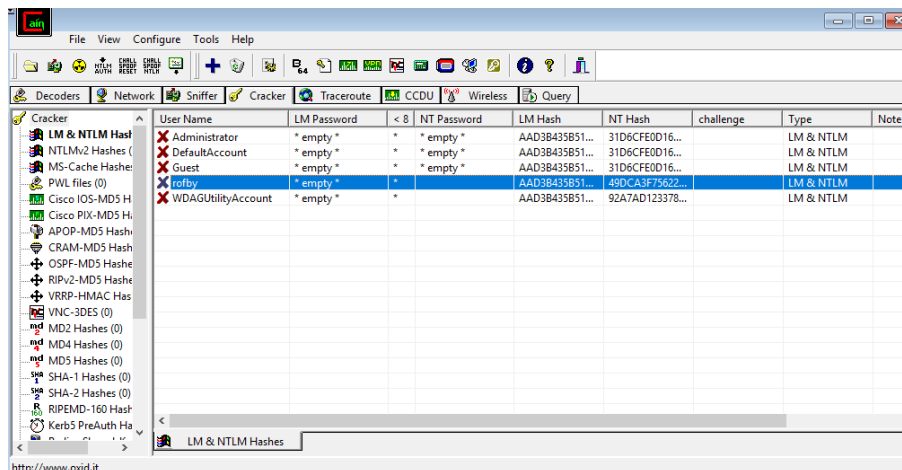
Berikut ini merupakan cara kedua dengan mendapatkan file database SAM dengan menggunakan *tool* Cain & Able yang bisa didapatkan di <http://www.oxid.it/cain.html>. Adapun langkah-langkahnya adalah sebagai berikut :

1. Instal Cain & Able.
2. Setelah berhasil menginstal, bukalah aplikasi Cain & Able tersebut.
3. Klik menu Cracker > LM & NTLM Hashes > Klik kanan pada mouse lalu pilih add to list. Kemudian akan muncul berbagai macam user pada komputer.



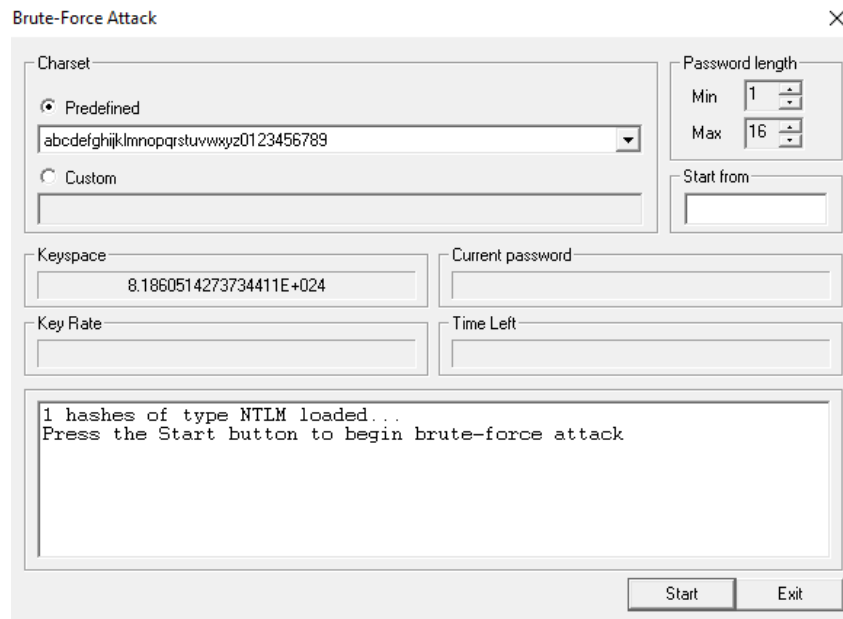
Gambar 1. Add to list user computer

4. Kemudian pilih *username* komputer, dalam hal ini adalah *username* dengan nama “rofbby”.

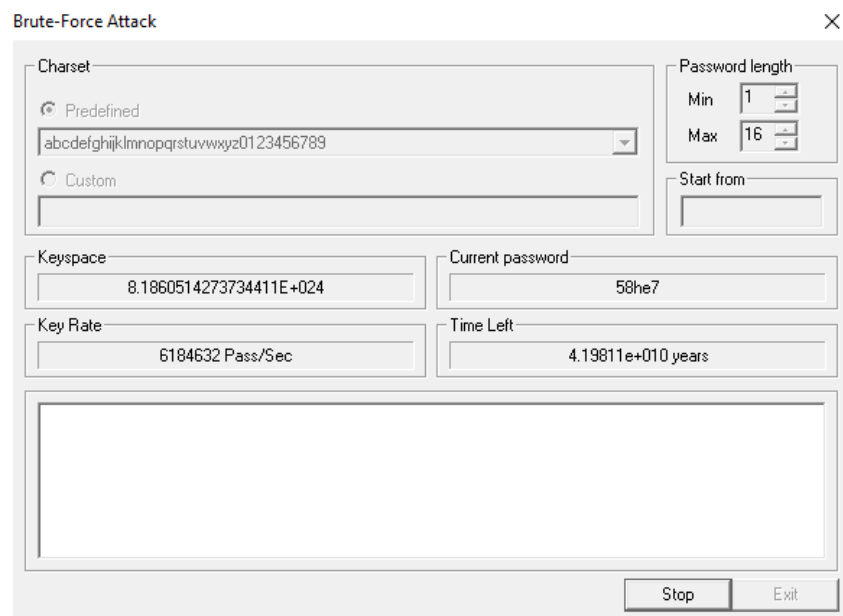


Gambar 2. Username komputer

5. Lalu klik kanan pada *username* yang dipilih > Brute-Force Attack > NTLM Hashes > Start.



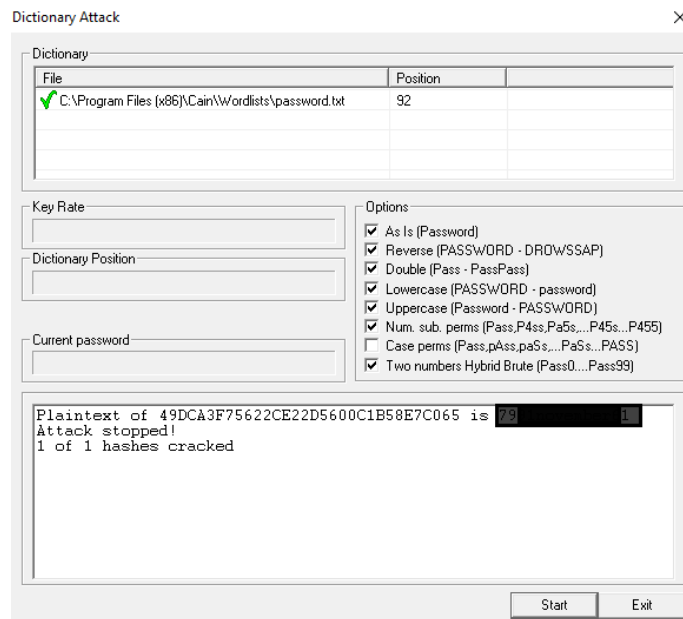
Gambar 3. Menu Brute-Force Attack



Gambar 4. Finding password

Seperti yang diketahui perlu waktu yang lama untuk menemukan password yang cocok. Cara lain agar dapat lebih cepat menemukan passwordnya adalah dengan menggunakan Dictionary Attack yang artinya kita menyisipkan dictionary password berupa kumpulan kemungkinan password yang diharapkan merupakan password yang sebenarnya.

6. Lalu klik kanan pada *username* yang dipilih > Dictionary Attack > NTLM Hashes > Add to List Dictionary Password > Start.



Gambar 5. Password ditemukan

III. Referensi

<http://www.oxid.it/cain.html>