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 lmu Komputer

Universitas Sriwijaya

2018

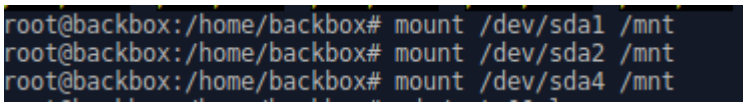
Hacking Password Window

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***

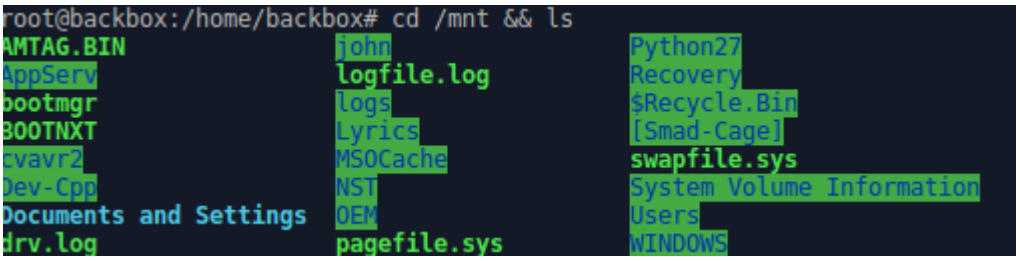
Gambar 1. Langkah awal

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



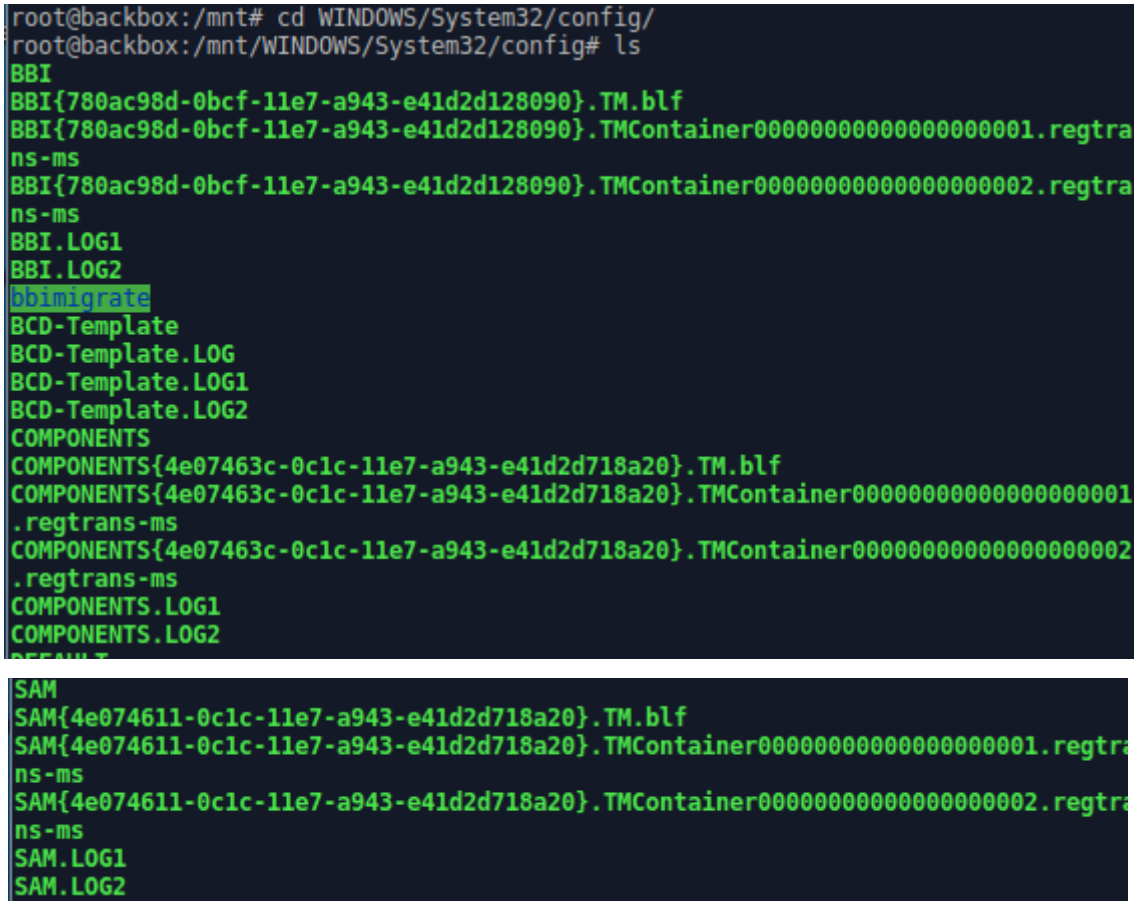
Gambar 2. Mount Disk

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



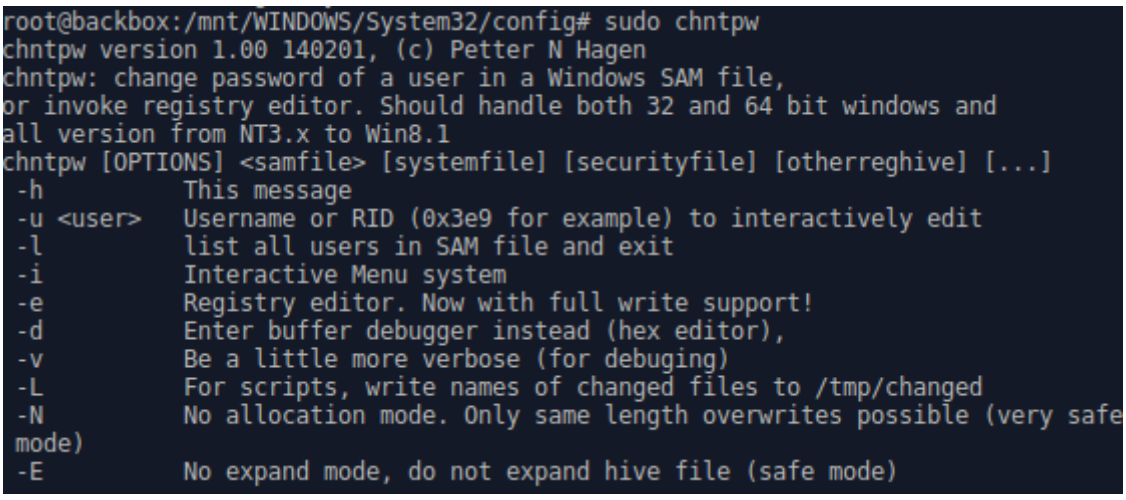
Gambar 3. Melihat isi hasil mount

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.



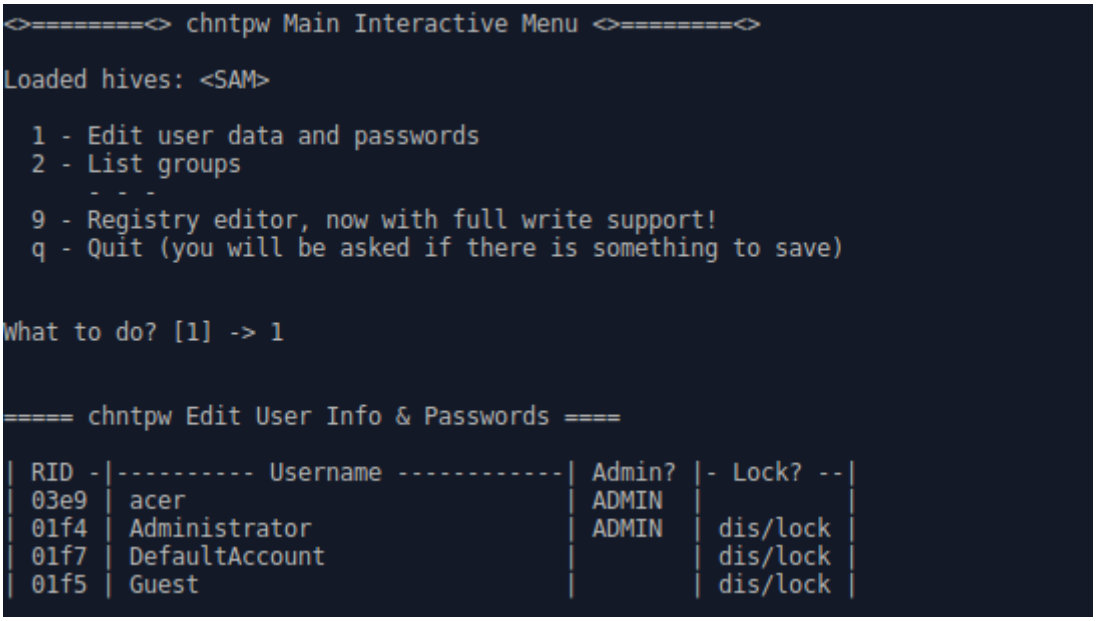
Gambar 4. Ls direktori system32 windows

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**



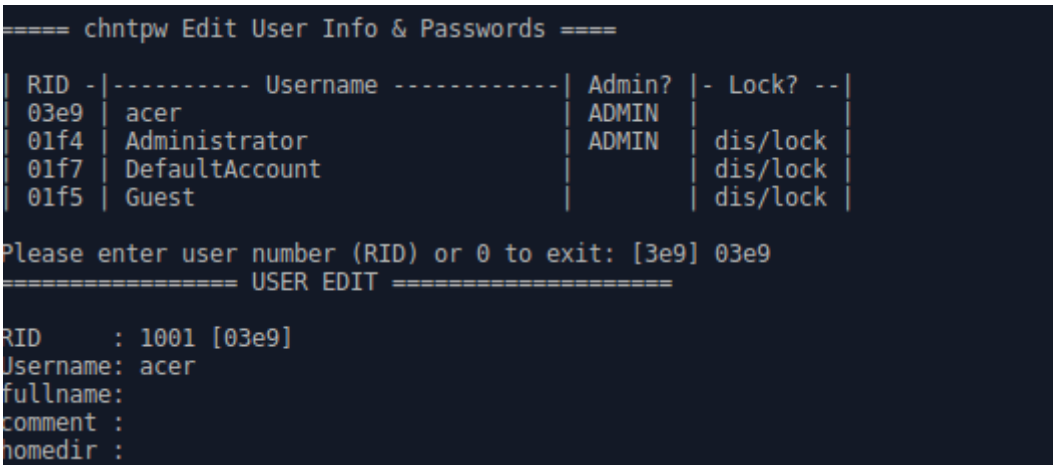
Gambar 5. Sudo chntpw

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



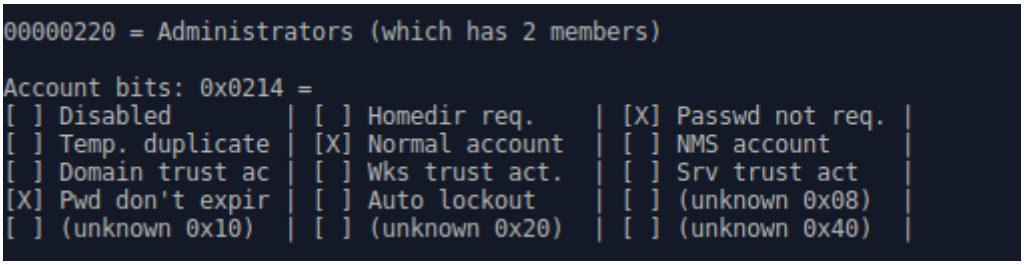
Gambar 6. Chntpw Main Interactive Menu

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



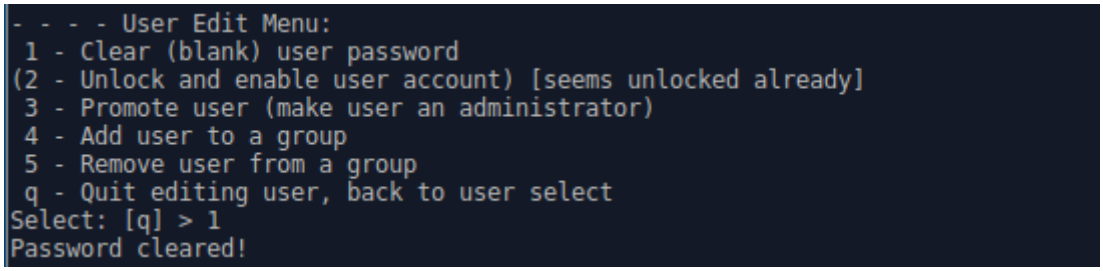
Gambar 7. Edit user info dan password

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



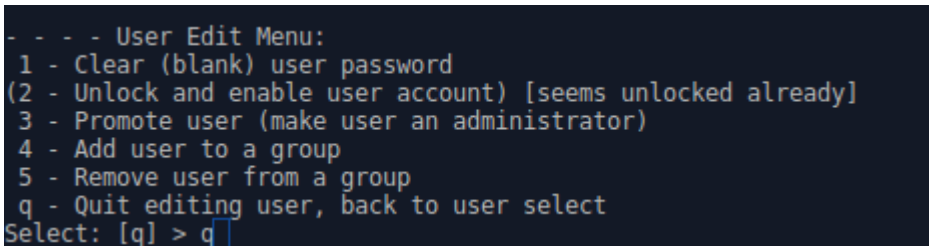
Gambar 8. User Info

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



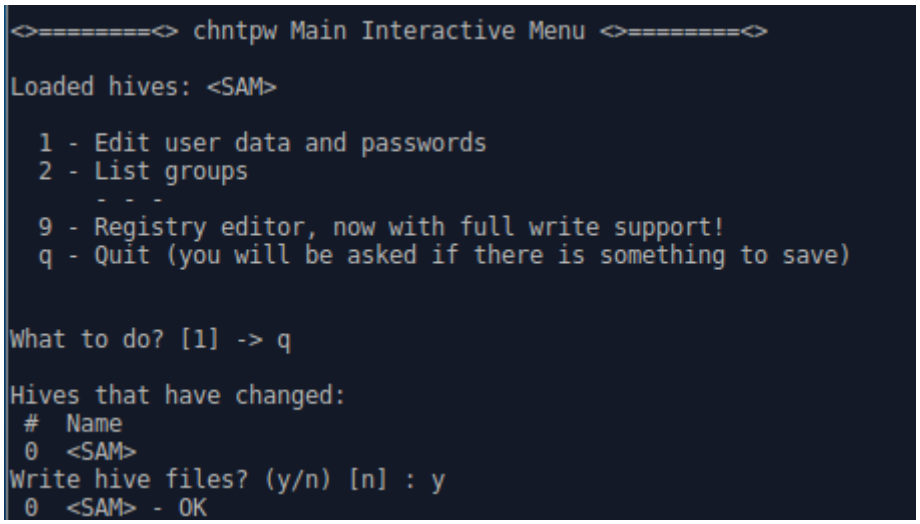
Gambar 9. Clear (blank) password

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



Gambar 10. Quit

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



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 penggunaanya
- 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.