Pengenalan Aplikasi John The Ripper dan Hacking Password Sistem Operasi
(Tugas Mata Kuliah Keamanan Jaringan Komputer)

Nama: Azwar Hidayat

NIM: 09011281520126

Jurusan Sistem Komputer

Fakultas lmu Komputer

Universitas Sriwijaya

2018

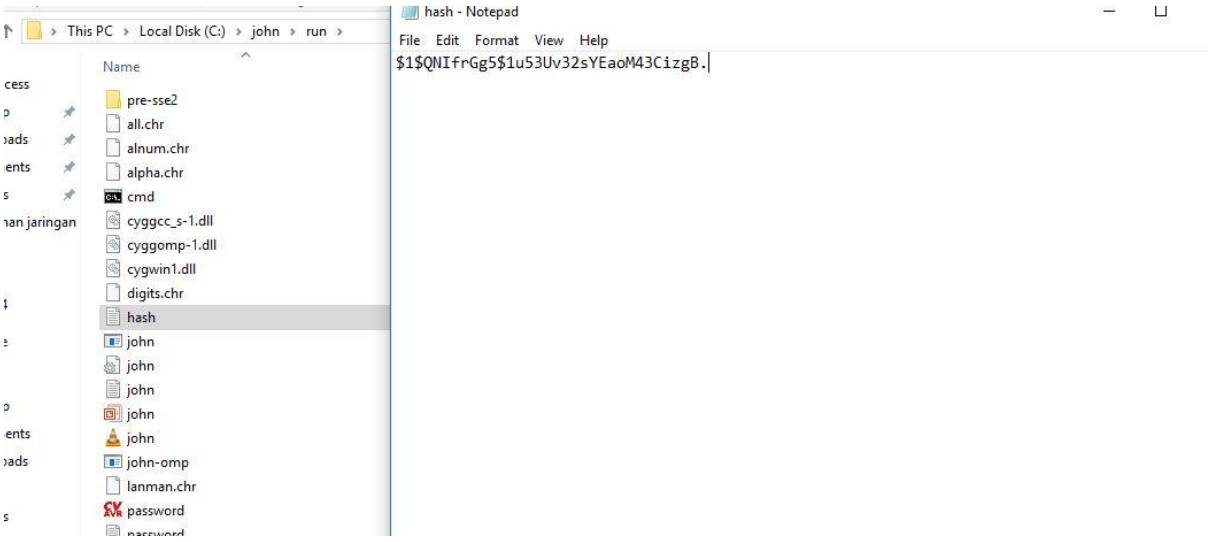
1. Hack Dasar :

Menggunakan aplikasi / tools john the ripper untuk mengetahui sebuah password yang telah di enkripsi md5

Langkah 1 : membuat password dan akun yang akan di hash (username : azeha dan password : 1q2w3e4r)

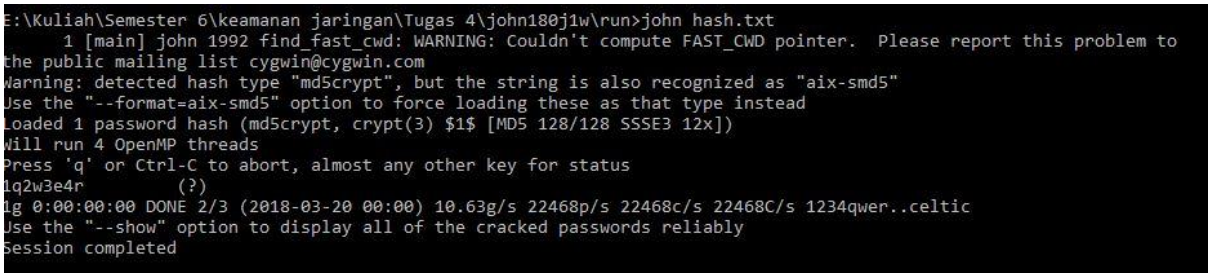
Gambar 1. Sebuah akun yang telah dibuat dan telah dienkripsi ke md5

Langkah 2 : buat file hash.txt di tempat john the ripper lalu jalankan john the ripper.



Gambar 2. File Hash.txt yang telah dibuat

Langkah 3 : jalankan john dan mulai membaca enkripsi tersebut. Bila berhasil akan memunculkan hasil seperti ini.



Gambar 3. Hasil dari hashing file

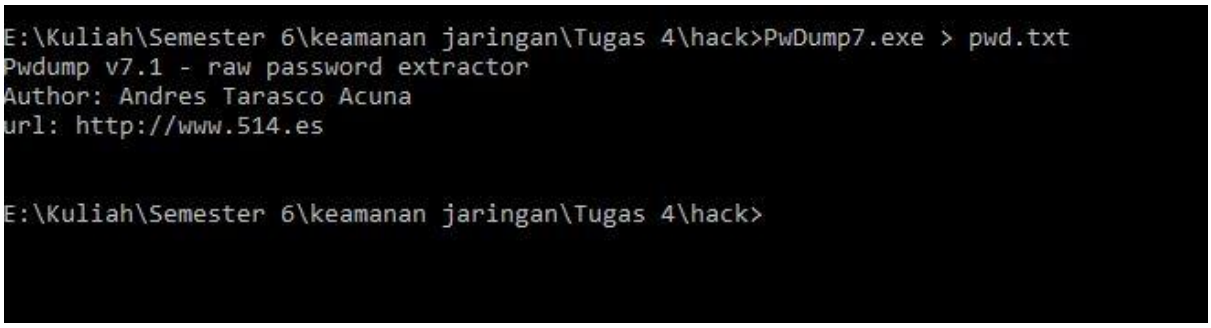
2. Windows

Terdapat dua cara untuk hacking password windows. Salah satunya adalah melakukan bruteforce masih dengan aplikasi/tools yang sama yaitu John The ripper. Kelemahan melakukan bruteforce ini adalah lamanya password yang akan didapatkan oleh user mengingat sangat banyaknya kombinasi. Alternatif lain adalah dengan melakukan bootable windows.

Yang digunakan kali ini adalah cara bruteforce .

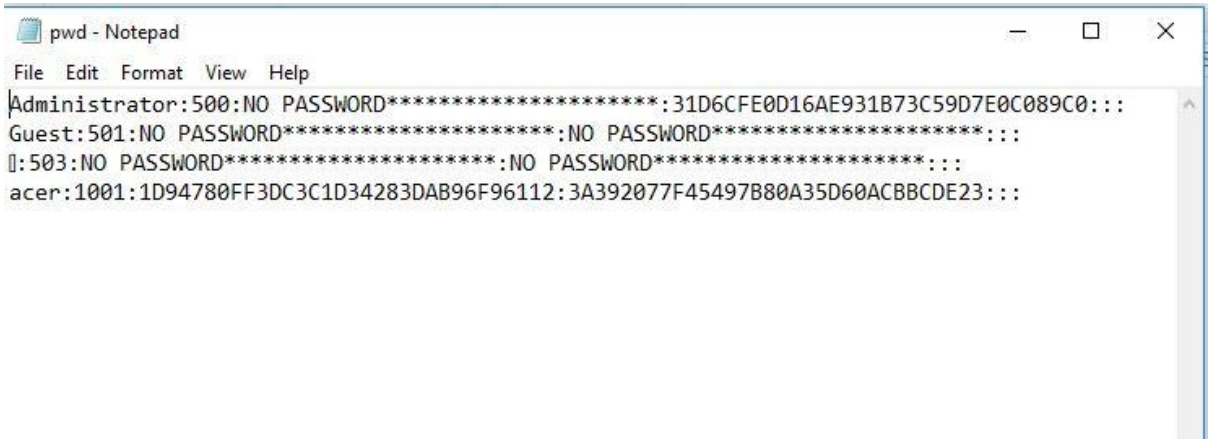
Langkah awal : Siapkan aplikasi tambahan yaitu pwdump7 untuk generate kode enkripsi dari password windows yang digunakan.

Langkah kedua : jalankan lalu ketikkan command ini *PwDump7 >pwd.txt*



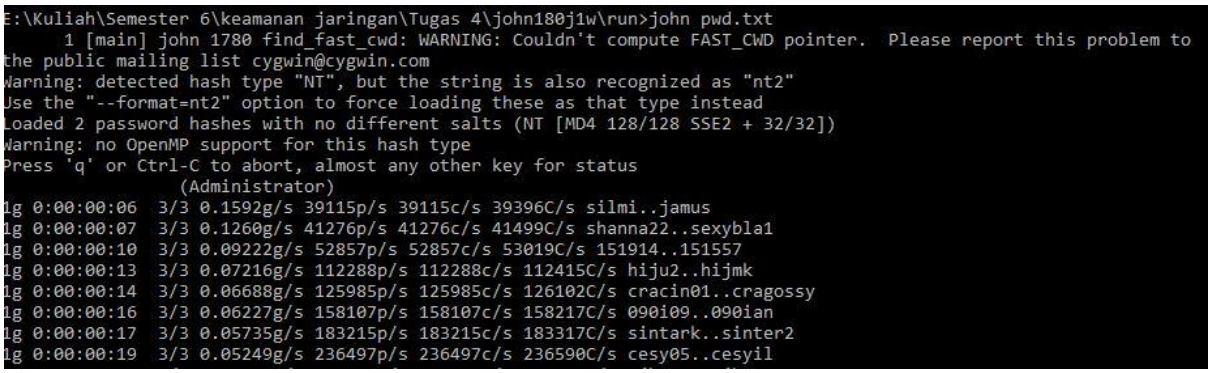
Gambar 4.Melakukan operasi PwDump

Setelah dari hasil ini maka akan diperoleh file sebagai berikut :



Gambar 5.Hasil dari PWD

Langkah ketiga masukkan ke folder john the ripper lalu tunggu sampai proses bruteforcenya selesai dan pssword anda ketemu



Gambar 6. Hasil dari Bruteforce file pwd.txt

3. Linux:

Pada percobaan ini, linuxlah yang sedikit lebih mudah untuk membajak password yang digunakan. Hal ini dikarenakan password yang digunakan terdapat di dalam folder etc.

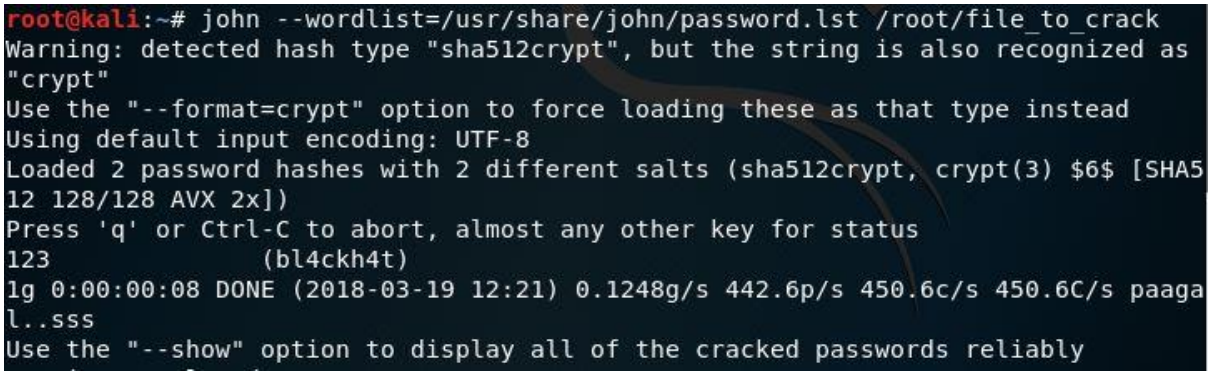
Langkah pertama: Pada percobaan disini menggunakan sebuah akun baru untuk login. Jadi, digunakan command seperti gambar dibawah ini.

Gambar 7. Pembuatan akun baru untuk masuk ke dalam linux.

Langkah kedua : Mengubah unshadow file /etc/passwd menjadi shadow dengan command berikut.

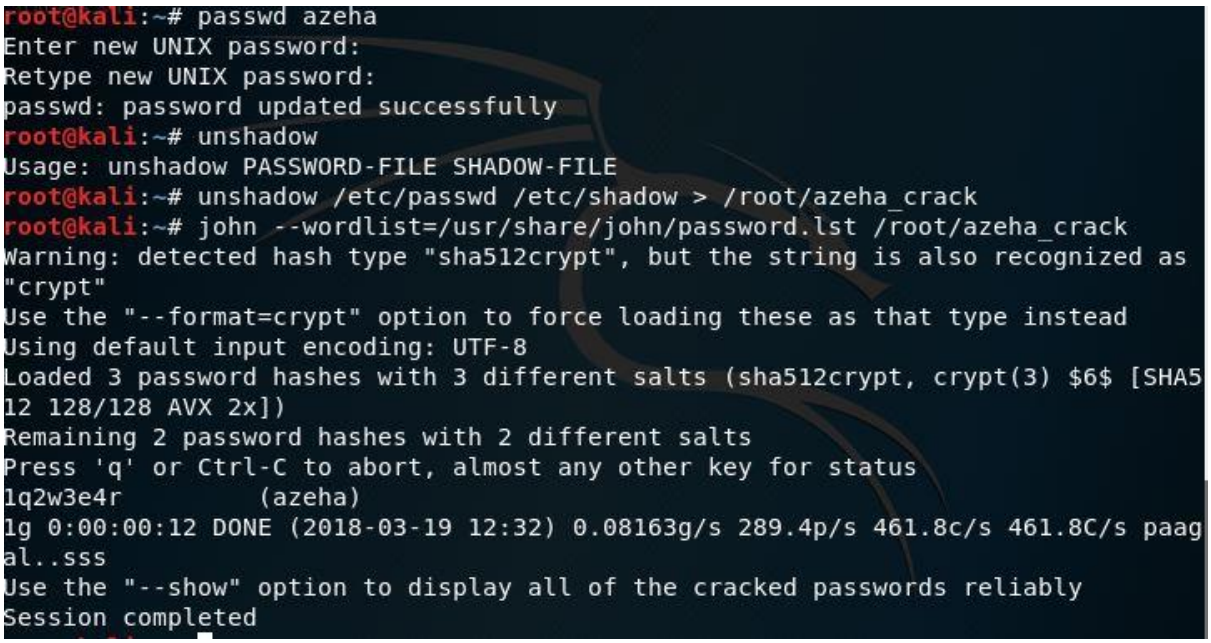
Gambar 8. Pengubahan unshadow menjadi shadow

Langkah kedua : hack password menggunakan john the ripper wordlist dictionary dengan command berikut ini. Bila berhasil akan didapat hasil seperti ini.



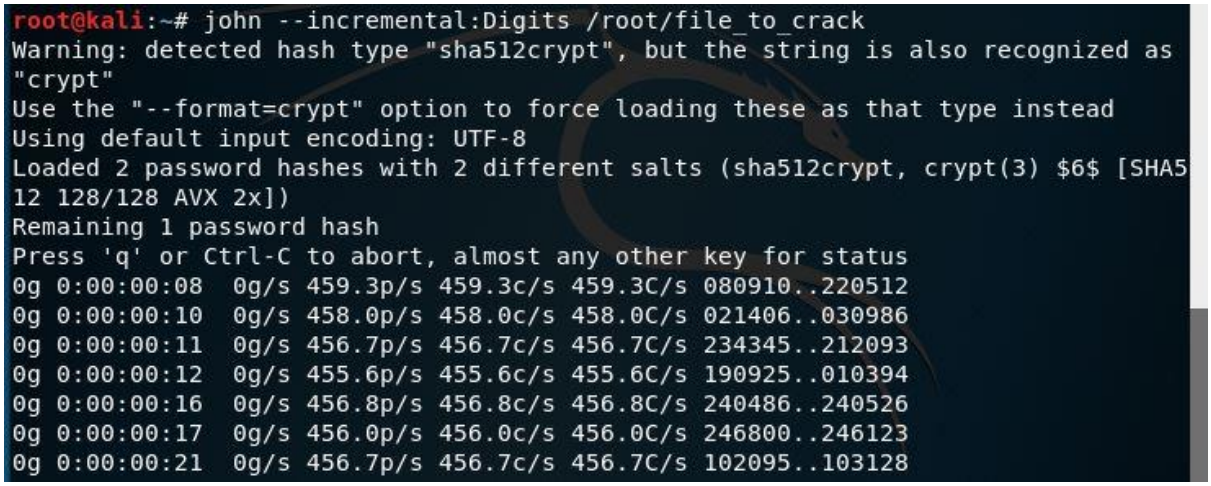
Gambar 9. Hasil tracing password dengan john the ripper

Pada gambar diatas, di dapatkan hasil 123 sebagai password user dan hasilnya benar. Metode ini dapat digunakan bila password yang digunakan ada di dalam wordlist dari John The Ripper itu. Untuk pembuktian, dicobalah password yang menggunakan kombinasi huruf dan angka. Hasil yang didapat seperti gambar dibawah ini.



Gambar 10. Hasil Tracing Password dengan kombinasi angka dan huruf

Dengan pembuktian diatas terbukti bahwa bila password yang digunakan terdapat di dalam wordlist John the ripper maka akan didapat hasil yang sesuai dan juga cepat. Bagaimana bila password yang digunakan tidak terdapat di dalam wordlist ? Hal ini masih bisa terpecahkan dengan metode bruteforce yang terdapat pada aplikasi/tools john the ripper itu sendiri. Tentu saja kelemahan dari metode ini adalah lambatnya didapatkan hasil karena tools mencoba semua kombinasi password yang mungkin.



Gambar 11. Bruteforce Password dengan john the ripper

Metode Bruteforce yang digunakan dalam john the ripper adalah increment. Increment dapat terdiri dari beberapa kombinasi diantaranya :

1. Lower (mencoba kombinasi dari kumpulan huruf kecil)
2. Alpha (mencoba kombinasi dari kumpulan huruf kapital)
3. Digits (mencoba kombinasi dari kumpulan angka)
4. Alnum (mencoba kombinasi dari alphanumeric character)
5. Increment lansung (kombinasi gabungan dari semuanya)

Oleh karena itu, dengan metode bruteforce ini akan didapatkan password tidak dalam waktu singkat karena tools mencoba berbagai kombinasi yang mungkin.