Vicko Bhayyu / 09011181520036

Keamanan Jaringan Komputer

Cracking Password Windows

Percobaan kali ini akan dilakukan cracking password windows. Cracking password windows digunakan untuk mendapatkan password account user windows yang disimpan ke dalam database SAM. Database SAM ini berisi hash dari password yang telah dibuat. Pada percobaan cracking password windows ini menggunakan tools dari software Cain & Abel.



Gambar 1. Icon dari Program Cain & Abel



Gambar 2. Tampilan Awal Software Cain & Abel

Diatas merupakan tampilan awal saat kita membuka software cain & abel. Untuk melakukan cracking password windows kita akan memilih menu cracker yang ada gambar kunci.



Gambar 3. Menu Cracker pada Cain & Abel

Setelah memilih menu cracker, terdapat banyak sub-menu pada bagian kiri software. Selanjutnya kita memilih sub-menu LM & NTLM Hashes.



Gambar 4. Memilih sub-menu LM & NTLM Hashes

Setelah memilih sub-menu tersebut, selanjutnya menekan tombol + yang ada pada menu bar diatas menu cracker.



Gambar 5. Menu selanjutnya yang muncul setelah menekan tombol +

Selanjutnya muncul sebuah menu yang menanyakan untuk menambahkan NT Hashes. Kali ini kita memilih dari import Hashes from local system, lalu menekan tombol Next.



Gambar 6. Muncul User name yang ada pada Windows

Setelah import, maka muncul beberapa username yang terdapat pada Windows. Selanjutnya kita memilih akun yang diberi password. Penulis menggunakan akun ‘vickzjr’ pada Windows nya.



Gambar 7. Pemilihan akun user.



Gambar 8. Menu Brute Force Attack

Setelah akun user dipilih, maka kita akan melakukan Brute Force Attack untuk mendapatkan password. Klik kanan pada akun, pilih brute-force attack, pilih NTLM Hashes



Gambar 9. Tampilan Brute-Force Attack NTLM Hashes

Terlihat diatas ada beberapa tombol. Kita dapat mendeskripsikan charset apa saja yang digunakan pada password. Penulis memilih charset default yang berisi lower-case a-z dan 0 – 9.

Lalu kita atur panjang password yang kita punya. Penulis membuat password sepanjang 6 digit.

Start from bisa dikosongkan, atau diisi untuk mulai dari mana brute force attack dilakukan.

Setelah itu tekan tombol start.



Gambar 10. Brute Force Attack sedang berjalan

Setelah tombol start ditekan, maka program akan melakukan brute force attack untuk menebak password. Proses ini memerlukan waktu, jika telah selesai ditemukan password yang tepat. Program akan berhenti.



Gambar 11. Password telah ditemukan

Tampilan diatas merupakan jika software telah menemukan password yang sesuai dengan NTLM Hashes yang kita punya. Penulis membuat password 123456.

Brute Force Attack tidak direkomendasikan jika memiliki password dengan panjang yang banyak. Program akan mencoba kombinasi dari a-z dengan panjang karakter 14. Proses itu akan menjadi sangat lama



Gambar 12. Brute Force attack password 14 digit

Terlihat diatas time left untuk menebak password sepanjang 14 digit. Sangat-sangat lama dilakukan jika proses ini dilakukan.

Sekian informasi yang disampaikan penulis. Semoga bermanfaat.