NETWORK SECURITY:
HACKING PASSWORD ADMINISTRATOR WITH CAIN AND ABEL FROM WINDOWS 7

BY

NAME	: DENI DANUARTA
NIM	: 09121001045
CLASS	: SK 8 PILIHAN
STUDY	: NETWORK SECURITY

DEPARTMENT OF COMPUTER ENGINEERING
FACULTY COMPUTER SCIENCE
SRIWIJAYA UNIVERSITY

I. Latar Belakang

Saat ini pentingnya sebuah keamanan yang merupakan hal yang lumrah karena pentingnya menjaga suatu informasi yang saat ini semakin merajarela penggunaannya. Hal ini di sebabkan karena adanya para hacking dan cracking yang siap untuk mengolah dan mencuri data dari suatu informasi. Walaupun kita meningkatkan keamanan yang kita seringkali data kita dicuri dengan melakukan social engineering baik dilakukannya dengan komunikasi maupun dengan menggunakan social engineering tools (SET).

Pada penulisan ini, pertahanan Personal Computer (PC) dengan menggunakan password user admin dapat mengetahui seberapa kuatnya penggunaan password sebagai media untuk mengamankan dri dari kebocoran informasi. Selain itu, kita dapat mengetahui bagaimana cara melihat password admin pada pengguna PC yang mayoritas penggunaan Operating Systemnya menggunakan windows.

II. Pembahasan

Pada penulisan dan pengujian saat ini kita menggunakan Virtualbox sebagai virtualisasi PC dengan Sistem Operasi Windows 7 Profesional yang mempunyai user administrator. Pada aplikasi hacking password dan user admin kita menggunakan Cain & Abel. Lalu kita menggunakan Pwdump7 untuk mengekstak hashes target tersebut dengan membuat dokumen dengan format .txt

A. Operating System

Operating Sistem adalah komponen pengolah piranti lunak dasar (essential component) tersistem sebagai pengelola sumber daya perangkat keras komputer (hardware), dan menyediakan layanan umum untuk aplikasiperangkat lunak. Sistem operasi adalah jenis yang paling penting dari perangkat lunak sistem dalam sistem komputer. Tanpa sistem operasi, pengguna tidak dapat menjalankan program aplikasi pada komputer mereka, kecuali program booting.

Sistem operasi mempunyai penjadwalan yang sistematis mencakup perhitungan penggunaan memori, pemrosesan data, penyimpanan data, dan sumber daya lainnya. Untuk fungsi-fungsi perangkat keras seperti sebagai masukan dan keluaran dan alokasi memori, sistem operasi bertindak sebagai perantara antara program aplikasi dan perangkat keras komputer, meskipun kode aplikasi biasanya dieksekusi langsung oleh perangkat keras dan seringkali akan menghubungi OS atau terputus oleh itu.

B. Cain & Abel

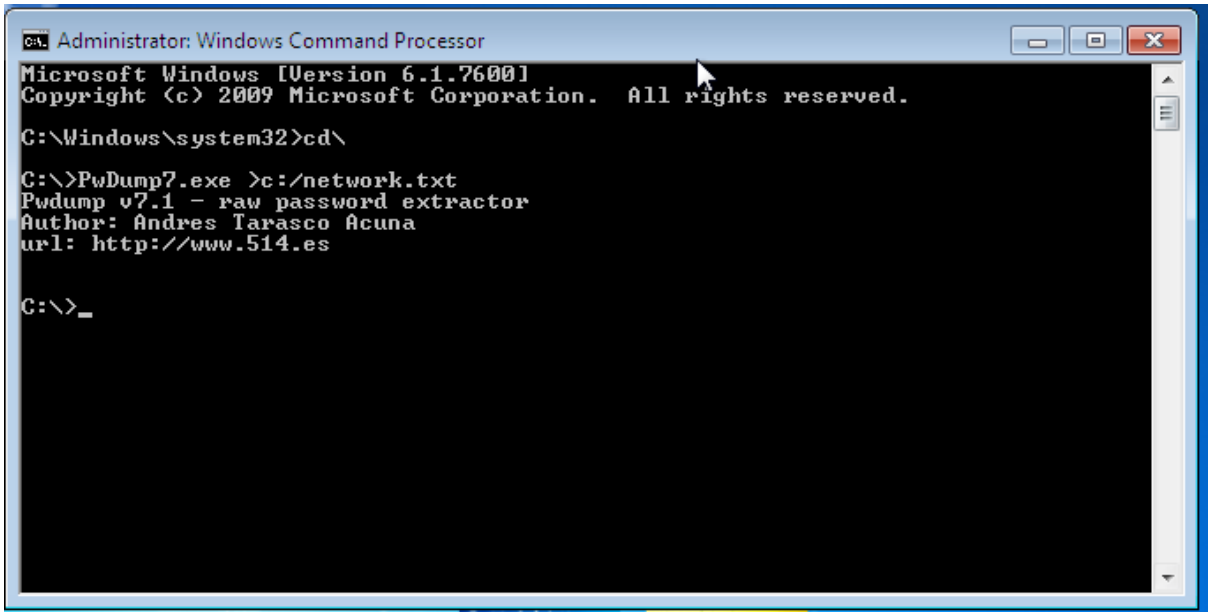
Cain & Abel adalah sebuah software yang dapat digunakan untuk melakukan hacking via LAN atau yang dikenal dengan sniffing. Sniffing adalah sebuah aksi hacking/cracking yang dilakukan terhadap setiap paket request dan reply pada jaringan lokal. Pada network security sniffing merupakan metode yang sering digunakan untuk mendapatkan informasi baik berupa password, data-data penting dan lain sebagainya. Penggunaan Cain & Abel adalah salah satu Social Engineering Tools. (SET).

C. Pwdump7

Pwdump7 adalah suatu aplikasi yang mengambil hash untuk mendekripsikan suatu kriptografi. Pada penulisan saat ini Pwdump menggunakan kriptografi SHA. SHA adalah serangkaian fungsi kriptografi hash yang dirancang oleh National Security Agency (NSA) dan diterbitkan NIST sebagai US Federal Information Processing Standard.

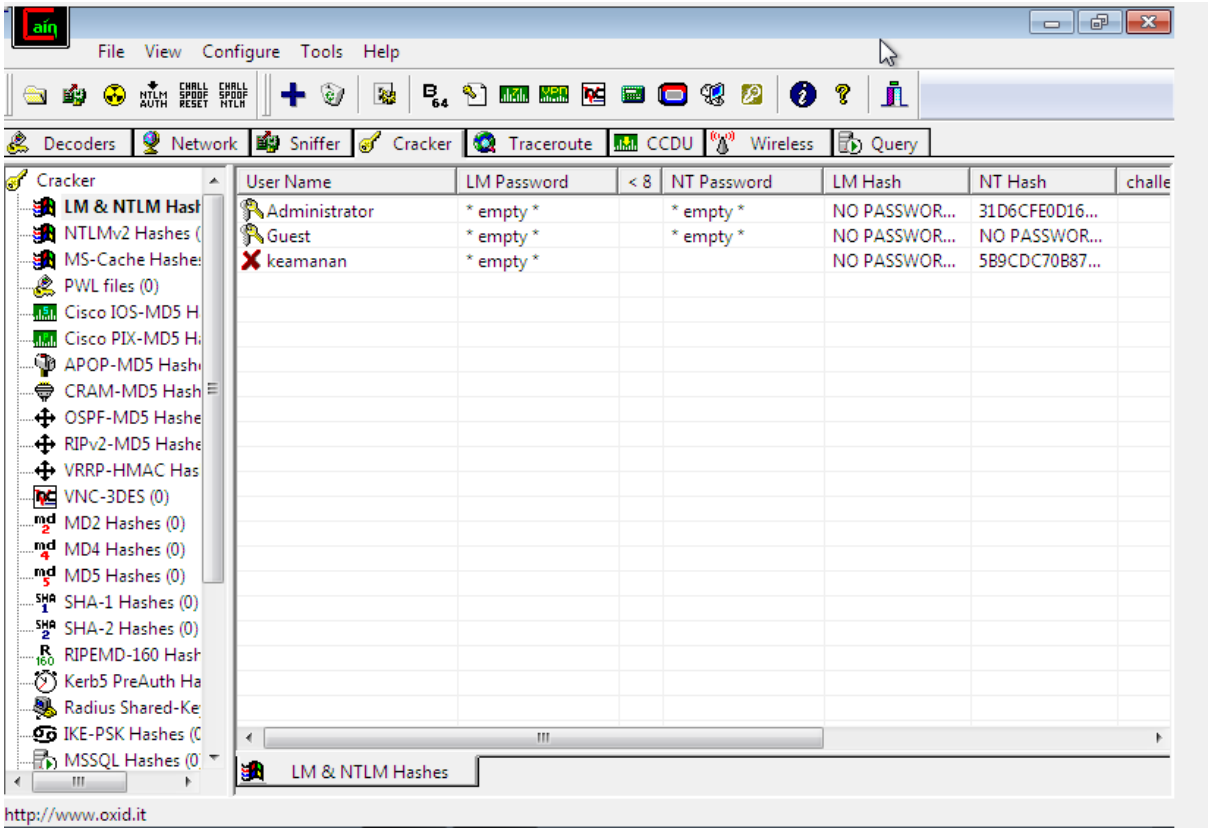
III. Hasil dan Analisa

A. Hasil

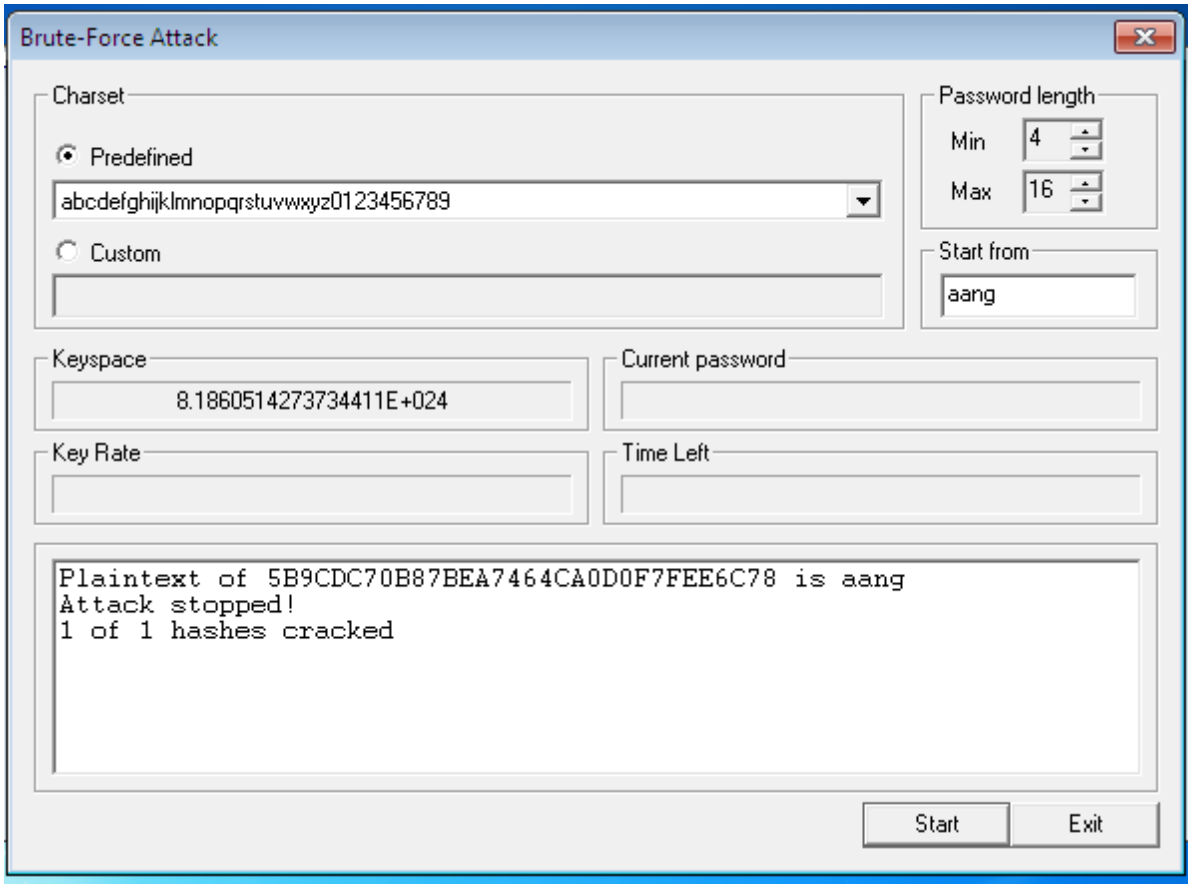


Gambar 1 Extract data hash pada komputer dengan menggunakan Pwdump7

Gambar 2 Hasil Extract Data Hash



Gambar 3 Pengolahan data hash yang di extract



Gambar 4 Cracking Password NTLM dengan serangan Brute Force

B. Analisa

Pada penulisan ini kita dapat menganalisa hasil yang kita dapat pada gambar diatas. Pada **Gambar 1** kita dapat mengextract data hash dengan menggunakan Command Prompt yang ada pada windows. Fungsi Hash pada data tersebut adalah sebagai pencarian dan perbandingan data dalam database mengambil kata kunci pada suatu sistem. Biasanya kata kunci tersebut adalah data yang bersifat privasi seperti Password, User Administrator dan lain sebagainya dengan menggunakan algoritma-algoritma tertentu untuk memetakan kunci nilai hash.

Gambar 2 berisi data hash yang telah di extract dengan menggunakan Pwdump7. Analisa pada gambar tersebut adalah data tersebut adalah open ssl dengan menggunakan SHA-1 (Secure-Hash Algorithm-1). Ukuran dari data tersebut adalah 20byte dengan panjang karakternya yaitu 40 karakter. Ini menjadi standar bagi National Institute of Standard and Technology untuk fungsi Hash satu arah dengan kombinasi huruf kecil dan angka.

Selanjutnya pada **Gambar 3**, pengelolahan data yang di extract dengan menggunakan Cain & Abel sebagai aplikasi yang mengenkripsikan suatu data baik berupa data hash dan lain-lain. Analisa dari gambar tersebut adalah data hash mempunyai Relative Identifier (RID) yang berisi bahwa data tersebut merupakan bagian dari Windows NT Lan Manager (NTLM) yang berarti bahwa data tersebut menggunakan teknik otentifikasi Chalenge / Response.

Dan terakhir pada **Gambar 4**, adalah hasil dari pengolahan data yang telah di deskripsikan. Ini dapat dianalisakan bahwa data tersebut menggunakan serangan Brute-Force yang memungkinkan kita untuk mendapatkan hasil password yang kita inginkan dengan cara mencocokan semua kunci yang kemungkinan merupakan password tersebut. Hasilnya password pada User Administrator adalah “aang” dengan Plaintextnya yaitu 5B9CDC70B87BEA7464CA0D0F7FEE6C78. Ini tidak membutuhkan waktu lama untuk mencocokan data karena jumlah karakter passwordnya adalah 4 karakter dengan hanya kombinasi abcdefghijklmnopqrstuvwxyz. Jika di kombinasikan dengan:

- ABCDEFGHIJKLMNOPQRSTUVWXYZ,
- 0123456789,
- ~!@#$%^&*()_+|}{“:?><,./’;\][=.

Maka data yang akan kita serang dengan bruteforce akan memakan waktu yang lama bahkan bertahun-tahun lamanya dengan kesulitan mencari kunci yang tepat yang berarti kuatnya suatu password tersebut. Walaupun begitu tidak ada pertahanan yang aman di dunia ini selagi dibuat manusia.

REFERENSI

- http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/How-Cracked-Windows-Password-Part2.html
- https://en.wikipedia.org/wiki/Hash
- https://en.wikipedia.org/wiki/Secure_Hash_Algorithm
- https://en.wikipedia.org/wiki/SHA-1
- http://www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7