Jurnal Nasional Informatika dan Teknologi Jaringan
E-ISSN : 2540-7600
P-ISSN : 2540-7597

PENGGUNAAN BRUTE FORCE ATTACK DALAM PENERAPANNYA PADA CRYPT8 DAN CSA-RAINBOW TOOL UNTUK MENCARI BISS

Indra Gunawan
AMIK Tunas Bangsa
Jl. Sudirman Blok A No. 1-3, Kota Pematang Siantar, Sumatera Utara 21127
Inthacuex36@gmail.com

***Abstrak*— Algoritma Brute Force merupakan suatu aritmatika untuk mencari dan mengetahui sebuah jenis sandi atau kode yang salh satunya sebuah kode acakan misalnya jenis acakan BISS (Basic Interoperable Scrambling System). Algoritma brute force yang umumnya dipakai untuk mencari kasus kode acakan seperti ini umumnya disebut Brute Force Attack. Brute force attack menggunakan sebuah himpunan karakter atau teks yang akan dipakai untuk referensi karakter-karakter dari kode yang ingin dicari. Himpunan karakter yang dipakai akan menjadi sebuah ukuran keefektifan dari algoritma itu sendiri. Semakin banyak anggota himpunan karakter ini, tentunya persentasi kode biss untuk sebuah kode biss dapat dicari akan tinggi. Namun, semakin banyak karakter yang ada di dalam himpunan itu harus dibayar dengan waktu pengerjaan yang lebih lama. Brute Force ini sudah mulai dikembangkan untuk mencari kode. Salah satu pengembangannya adalah pengumpulan chain sebagai database dan penggunaan Crypt8 dan CSA-Rainbow Tool yang menggunakan algoritma brute force sehingga memungkinkan untuk memangkas waktu yang diperlukan Brute Force Attack.**

***Keywords*— Brute Force Attack, Acakan, Biss, Cw, Chain.**

I. PENDAHULUAN

A. Definisi Brute Force

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian permasalahan kode cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter dan panjang kode tertentu tentunya dengan banyak sekali kombinasi kode. Algoritma brute force adalah algoritma yang lempang atau apa adanya. Pengguna hanya tinggal mendefinisikan karakter set yang diinginkan dan berapa ukuran dari kodenya. Tiap kemungkinan kode akan di generate oleh algoritma ini.

B. Definisi Crypt8

Sebuah kode dapat dibongkar dengan menggunakan program yang disebut sebagai Crypt8. Program Crypt8 adalah program yang mencoba menemukan 16 digit karakter kode crypt yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem acakan biss yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk kode yang rumit. Namun ini tidak berarti bahwa Crypt8 membutuhkan decrypt. Pada prakteknya, mereka kebayakan tidak melakukan itu. Umumnya, kita tidak dapat melakukan perekaman siaran yang teracak/scramble dengan menggunakan media penyimpanan (cth : flashdisk) selama 120 detik (waktu paling cepat yang biasa dilakukan). Namun, anda menggunakan tool-tool simulasi yang mempekerjakan algoritma yang sama yang digunakan untuk mengenkripsi kode orisinal. Tool-tool tersebut membentuk analisa komparatif. Program Crypt8 tidak lain adalah mesin-mesin ulet. Ia akan mencoba kata demi kata dalam kecepatan tinggi. Mereka menganut "Asas Keberuntungan", dengan harapan bahwa pada kesempatan tertentu mereka akan menemukan kata atau angka yang cocok.

C. Definisi CSA-Rainbow Tool

Merupakan sebuah aplikasi untuk mengkonversi 16 digit kode Crypt8 menjadi 16 digit kode CW (Chain Word) penting yang dapat digunakan untuk menentukan 16 digit kode acakan biss. Dari 16 digit kode CW, dapat membuka siaran yang teracak/scramble dengan mode acakan Biss.

D. Definisi Brute Force Attack

Serangan brute-force adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia. Sebagai contoh, untuk menyelesaikan sebuah persamaan kuadrat seperti $x^2+7x-44=0$, di mana x adalah sebuah integer, dengan menggunakan teknik serangan brute-force, penggunanya hanya dituntut untuk membuat program yang mencoba semua nilai integer yang mungkin untuk persamaan tersebut hingga nilai x sebagai jawabannya muncul. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan

mottonya: "When in doubt, use brute-force" (jika ragu, gunakan brute-force). Secara sederhana, menebak kode dengan mencoba semua kombinasi karakter yang mungkin. Brute force attack digunakan untuk menjebol akses ke suatu host (server/workstation/network) atau kepada data yang terenkripsi. Metode ini dipakai para cracker untuk mendapatkan account secara tidak sah, dan sangat berguna untuk memecahkan enkripsi. Enkripsi macam apapun, seperti Blowfish, AES, DES, Triple DES dsb secara teoritis dapat dipecahkan dengan brute-force attack. Pemakaian kode sembarangan, memakai kode yang cuma sepanjang 3 karakter, menggunakan kata kunci yang mudah ditebak, menggunakan kode yang sama, menggunakan nama, memakai nomor telepon, sudah pasti sangat tidak aman. Namun brute force attack bisa saja memakan waktu bahkan sampai berbulan-bulan atau tahun bergantung dari bagaimana rumit kodenya. Brute Force attack tidak serumit dan low-tech seperti algoritma hacking yang berkembang sekarang. Seorang penyerang hanya cukup menebak anama dan kombinasi kode sampai dia menemukan yang cocok. Mungkin terlihat bahwa brute force attack atau dictionary attack tidak mungkin berhasil. Namun yang mengejutkan , kemungkinan berhasil brute force attack menjadi membaik ketika site yang ingin diretasi tidak dikonfigurasikan dengan baik.

II. METODE PENELITIAN

A. Metode yang Dipakai Brute Force Attack

Brute Force attack adalah sebuah metode untuk menjebol kode rahasia (yaitu, mendekripsi sebuah teks yang telah terenkripsi) dengan mencoba semua kemungkinan kunci yang ada. Feasibility dari sebuah brute force attack tergantung dari panjangnya cipher yang ingin dipecahkan , dan jumlah komputasi yang tersedia untuk penyerang. Salah satu contohnya bernama Cain's Brute Force Code Cracker mencoba semua kombinasi yang mungkin dari karakter yang telah didefinisikan sebelum atau set karakter yang kustom melawan sebuah kode yang telah terenkripsi di brute force dialog. Kuncinya adalah mencoba semua kemungkinan kode dengan formula seperti berikut. KS = L(m) + L(m+1) + L(m+2) + ... + L(M).

L = jumlah karakter yang kita ingin definsikan m = panjang minimum dari kunci M = panjang maksimal dari kunci Contohnya saat kita ingin meretas sebuah Lan Manager paswords (LM) dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter, maka brute fore cracker harus mencoba KS = 26^1 + 26^2 + 26^3 + ... + 26^7 = 8353082582 kunci yang berbeda. Jika ingin meretas kode yang sama denganset karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ01234567 89! @#$%^&*()-_+=~`[]{}|\:;"'<>,.?/", jumlah kunci akan dihasilkan akan naik menjadi 6823331935124.

Brute Force attack melakukan perbandingan string matching antara pattern dengan text per karakter dengan pseudocode berikut : do if (text letter == pattern letter) compare next letter of pattern to next letter of text else move pattern down text by one letter while (entire pattern found or end of text) Exhaustive key search cracking mungkin saja memerlukan waktu yang sangat panjang untuk berhasil, tetapi jika character setnya sidah benar sesaui kode, maka tinggal hanyalah jadi masalah waktu.

Perbandingan panjang kunci dengan jumlah permutasi Key size dalam bits Permutasi 8 28 40 240 56 256 64 264 128 2128 256 2256 2.2 Algoritma Simetrik Symmetric cipher dengan kunci 64 bit atau tidak terlalu rentan terhadap brute force attack. DES, blok cipher digunakan secara luas yang menggunakan 56-bit kunci, dirusak oleh proyek EFF (Electronic Frontier Foundation) pada tahun 1998, dan pesan RC5 kunci 64- bit baru-baru ini sudah berhasil dipecahkan. Banyak orang berpikir bahwa organisasi-organisasi yang didanai dengan baik, terutama lembaga SIGINT(Signals and Intellegence) pemerintah seperti US NSA(National Security Agency), berhasil dapat menyerang sebuah sandi kunci simetris dengan kunci 64-bit dengan menggunakan Brute Force Attack. Untuk aplikasi yang memerlukan keamanan jangka panjang, 128 bit, pada tahun 2004, saat ini sedang dipikirkan panjang kunci yang cukup dan kokoh untuk sistem baru menggunakan algoritma kunci simetrik. NIST(National Institute of Standards) telah merekomendasikan bahwa 80-bit desain akan berakhir pada tahun 2015. Bahkan dalam situasi adalah 128-bit atau kunci yang lebih besar digunakan dengan cipher yang dirancang dengan baik seperti AES, Brute Force dapat dilakukan untuk meretas jika kunci tidak dihasilkan dengan benar. Banyak keamanan produk komersial dan shareware yang bangga mengiklankan "keamanan 128-bit" kunci berasal dari sebuah kata sandi yang dipilih pengguna atau passphrase. Karena pengguna jarang menggunakan kode dengan hampir 128 bit entropi, sistem seperti seringkali cukup mudah untuk dibobol dalam prakteknya. Beberapa produk keamanan bahkan membatasi jumlah masukan karakter maksimum pengguna sampai ke panjang yang terlalu kecil untuk sebuah passphrase.

Berikut adalah beberapa contoh kode atau passphrase yang dihasilkan dengan metode yang memberikan keamanan 128-bit:

- kode 28-huruf acak dengan semua huruf tunggal kasus: "sqrnf oikas ocmpe vflte krbqa jwf"
- 20 karakter acak kode dengan huruf campuran- kasus, angka dan karakter khusus: ". iTb \ /&/-} itu / P; ^ +22 q"
- 10 acak-dipilih-kata Diceware(hardware number generator) dengan kata sandi: " serf bare gd jab weld hum jf sheet gallop neve"

Hampir tidak ada yang menggunakan kode yang sekompleks ini. Salah satu solusinya adalah untuk menerima kekuatan yang lebih rendah. 16 huruf atau 6 kata diceware akan memberikan keamanan yang 75-bit, cukup untuk melindungi terhadap semua semua kecuali kriptoanalisis paling kuat. Solusi lain adalah dengan menggunakan fungsi derivasi kunci (KDF) atau "key stretcher" yang melakukan pekerjaan

komputasi yang signifikan dalam mengkonversi kode menjadi kunci, membuat penyerang brute force mengulang ini bekerja untuk setiap percobaan kunci. Dalam prakteknya, teknik ini dapat menambah 10 sampai 20 bit kekuatan untuk kode, cukup untuk memungkinkan sebuah passphrase yang cukup diingat untuk digunakan, tetapi tidak cukup untuk mengamankan kata sandi yang pendek kebanyakan orang pakai. Sayangnya, masih sedikit yang menggunakan produk keamanan teknologi KDF. Mungkin solusi terbaik adalah untuk menyimpan kunci yang dihasilkan secara acak dan kekuatan dalam dan bagian internal dilindungi oleh kode atau PIN.

B. Algoritma Asimetrik

Situasi yang berkaitan dengan algoritma kunci asimetrik lebih rumit dan tergantung pada algoritma enkripsi tiap individu. Jadi, panjang kunci saat ini dapat dipecahkan untuk algoritma RSA adalah minimal 512 bit (telah dilakukan secara publik), dan perkembangan penelitian terbaru menunjukkan bahwa 1024 bit bisa dipecahkan dalam waktu dekat untuk jangka menengah. Untuk algoritma kurva eliptik paling asimetris, panjang kunci terbesar saat pecah diyakini agak pendek, mungkin sesedikit 128 bit atau lebih. Sebuah pesan yang dienkripsi dengan bit kunci 109 oleh algoritma enkripsi kurva eliptik yang umum rusak oleh kekerasan pencarian kunci pada awal 2003.

C. Kelas Serangan

Dalam hal ini memperlihatkan aprosimaksi waktu yang diperlukan sebuah komputer atau sebuah cluster komputer untuk menebak kode. Gambar - gambar di bawah adakah aprosimaksi dan waktu maksimal untuk menebak sebuah kode menggunakan keysearch attack biasa. Mungkin saja kadang ada sebuah tebakan beruntung yang benar tanpa harus mencoba kombinasinya.

Kelas serangan dibagi menjadi :

- Kelas A. 10,000 kode/sec Typical for recovery of Microsoft Office passwords on a Pentium 100
- Kelas B. 100,000 kode/sec Typical for recovery of Windows Password Cache (.PWL Files) passwords on a Pentium 100
- Kelas C. 1,000,000 kodes/sec Typical for recovery of ZIP or ARJ passwords on a Pentium 100
- Kelas D. 10,000,000 kode/sec Fast PC, Dual Processor PC.
- Kelas E. 100,000,000 kode/sec Workstation, or multiple PC's working together.
- Kelas F. 1,000,000,000 kode/sec Typical for medium to large scale distributed computing, Supercomputers.

Dengan contoh ketahanan waktu pembobolan sebuah kode jika diserang oleh brute force :

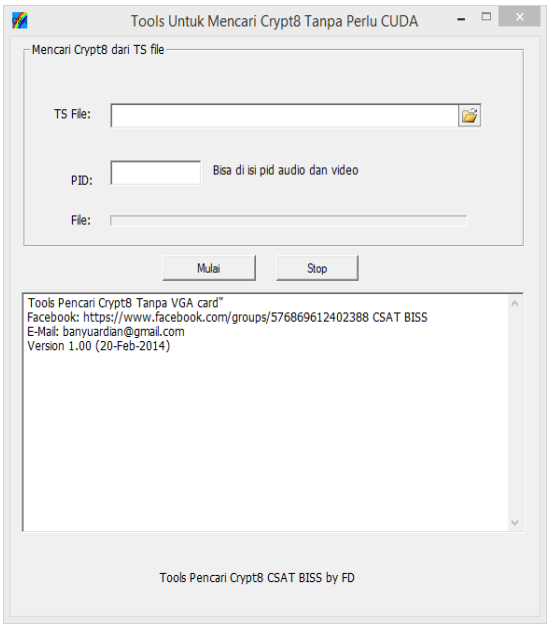
- 10 Karakter set
- 6 karakter set (upper case ATAU lower case dan angka)
- 52 karakter set (upper case dan lower case)

dan berbagai contoh lain misalnya gabungan upper case, lower case, angka dan simbol-simbol yang sering digunakan.

III. IMPLEMENTASI

A. Crypt8

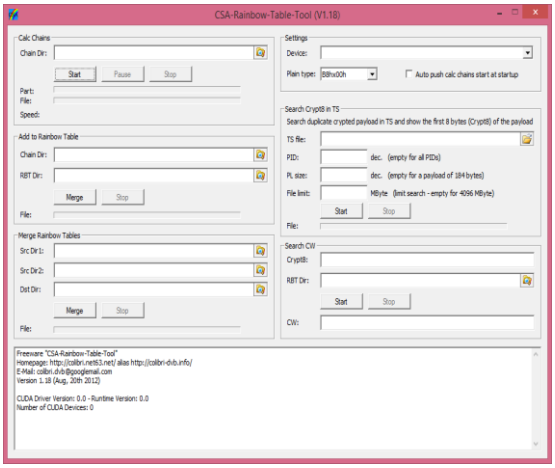
Crypt8 akan membantu untuk menemukan 16 digit kode yang dibutuhkan sebelum dikonversi menjadi CW. Perangkat (Hardware) yang dibutuhkan adalah 1 buah reciever dengan kualitas dan support MPEG4/Full HD (1080px), media penyimpanan (Flashdisk) dengan besar minimal 8 GB, 1 unit PC yang bertindak sebagai pengumpul chain dan harus stanbay dan dapat di-*sharing* ke PC/Laptop lain, 1 unit PC/Laptop yang yang digunakan sebagai pengkonversi Crypt8. Cara kerjanya adalah dengan menggunakan Flashdisk, lakukan perekaman siaran yang diacak/*Scramble* dengan jenis acakan biss. Rekam siaran selama 120 detik sehingga menghasilkan beberapa file yang salah satu jenis filenya adalah berekstensi .ts.



Gbr.1 Software Crypt8

B. CSA-Rainbow Tool

CSA-Rainbow Tool akan mengkonversi 16 digit Crypt8 menjadi 16 digit CW. Cara kerjanya adalah dengan memasukkan kode digit Crypt8 kedalam software CSA-Rainbow Tool.



Gbr.2 Software CSA-Rainbow Too

Jika 16 digit kode Crypt8 sudah dimasukkan kedalam CSA-Rainbow Tool, selanjutnya lakukan pengkonversian kode sehingga menjadi 16 digit kode CW.

Gbr.3 16 Digit CW Found

Peralatan yang digunakan untuk melakukan pencarian 16 digit Scrypt8 dan 16 digit CW berupa Personal Computer, Laptop, Digital Reciever dan Televisi.

Gambar.4 Peralatan pencari 16 digit CW

IV. KESIMPULAN

Walaupun sudah kuno, teknik penyerangan yang membosankan ini bisa berhasil seperti yang lebih baru dan menarik. Walaupun dianggap low-tech, brute force attack dapat menjadi sangat efektif dalam membahayakan sebuah Aplikasi keamanan acakan biss kecuali mempunyai mekanisme defense tersendiri. Cara efektif untuk mengalahkan brute force attack adalah mengharuskan semua user mengganti jenis acakan yang awalnya acakan biss menjadi jenis acakan yang lebih sulit untuk diretas, seperti jenis acakan powervu, tanderbride, Nationdate, Tongfang, Xcript, dll.

REFERENSI

[1] Algoritma Brute Force Bagian 2 - Algoritma Brute Force (lanjutan).ppt. Munir, Rinaldi.
[2] Makalah IF3051 Strategi Algoritma – Sem. I Tahun 2010/2011
[3] http://cyberarmyloebas.blogspot.com/2013/11/mendapatkan-crypt8-ts-file-csa-rainbow.html tanggal akses 21 September 2014
[4] http://colibri.bplaced.net/csa_rainbow_table.htm tanggal akses 21 September 2014
[5] http://forumsatelit.com/english-corner/the-csa-rainbow-table-tool tanggal akses 21 September 2014
[5] DVB TS Vollverschlüsselung geknackt – Getunnelter TS, Nohl, Karsten and Schlüsselrate , Kunterbuntes.