

Brute Force Attack dan Penerapannya pada Password Cracking

Krisnaldi Eka Pramudita - 13508014
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
¹if18014@students.if.itb.ac.id

ABSTRACT

Makalah ini akan mengulas tentang algoritma *brute force* dalam lingkup teknologi informasi dan penerapannya dalam membobol atau meretas sebuah password misalnya password untuk login facebook. Algoritma brute force yang umumnya dipakai untuk meretas kasus password seperti ini umumnya disebut Brute Force Attack.

Brute force attack menggunakan sebuah himpunan karakter atau teks yang akan dipakai untuk referensi karakter-karakter dari password yang ingin dibobol/diretas.

Himpunan karakter yang dipakai akan menjadi sebuah ukuran keefektifan dari algoritma itu sendiri. Semakin banyak anggota himpunan karakter ini, tentunya persentasi password cracking untuk sebuah password dapat diretas akan meninggi. Namun, makin banyak karakter yang ada di dalam himpunan itu harus dibayar dengan waktu pengerjaan yang lebih lama.

Brute Force ini sudah mulai dikembangkan untuk meretas password. Salah satu pengembangannya adalah dictionary attack yang menggunakan algoritma brute tetapi himpunan karakternya berasal dari sebuah kamus (misalnya KBBI) sehingga memungkinkan untuk memangkas waktu yang diperlukan Brute Force Attack pada umumnya walaupun ber-drawback tidak ditemukannya password.

Index Terms— *brute force, brute force attack, password, dictionary attack*

I. PENDAHULUAN

1.1 Definisi Brute Force

Algoritma *brute force* adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung, dan dengan cara yang jelas/lempang. Penyelesaian permasalahan password cracking dengan menggunakan algoritma *brute force* akan menempatkan dan mencari semua kemungkinan password dengan masukan karakter dan panjang password tertentu tentunya dengan banyak sekali kombinasi password.

Algoritma *brute force* adalah algoritma yang lempang atau apa adanya. Pengguna hanya tinggal

mendefinisikan karakter set yang diinginkan dan berapa ukuran dari passwordnya. Tiap kemungkinan password akan di generate oleh algoritma ini.

1.2 Definisi Password Cracking

Sebuah password dapat dibongkar dengan menggunakan program yang disebut sebagai password cracker. Program password cracker adalah program yang mencoba membuka sebuah password 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 yang aman dari serangan ini, meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang rumit.

Namun ini tidak berarti bahwa password cracker membutuhkan decrypt. Pada prakteknya, mereka kebanyakan tidak melakukan itu. Umumnya, kita tidak dapat melakukan decrypt password-password yang sudah terenkripsi dengan algoritma yang kuat. Proses-proses enkripsi modern kebanyakan hanya memberikan satu jalan, di mana tidak ada proses pengembalian enkripsi. Namun, anda menggunakan tool-tool simulasi yang mempekerjakan algoritma yang sama yang digunakan untuk mengenkripsi password orisinal. Tool-tool tersebut membentuk analisa komparatif. Program password cracker 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 kalimat yang cocok. Teori ini mungkin tepat mengena pada anda yang terbiasa membuat password asal-asalan. Dan memang pada kenyataannya, password-password yang baik sulit untuk ditembus oleh program password cracker.

1.3 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, penggunaanya 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 password 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 password sembarangan, memakai password yang cuma sepanjang 3 karakter, menggunakan kata kunci yang mudah ditebak, menggunakan password 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 passwordnya.

Brute Force attack tidak serumit dan low-tech seperti algoritma hacking yang berkembang sekarang. Seorang penyerang hanya cukup menebak anama dan kombinasi password 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 diretas tidak dikonfigurasi dengan baik. Beberapa faktor yang menjadi keuntungan seorang hacker, biasanya disebabkan oleh kemalasan manusia itu sendiri,

Hal-hal yang perlu diperhatikan dalam menggunakan

metode *brute force attack* :

a. Asumsikan bahwa *password* diketik dalam huruf kecil (*lower case*).

Pada kasus ini, waktu yang dibutuhkan akan cenderung sama tetapi jika *password* mengandung huruf kapital (*upper case*) cara ini tidak akan berhasil.

b. Coba semua kemungkinan.

Tujuh karakter *lower case* membutuhkan sekitar 4 jam untuk berhasil mendapatkan *password* tetapi jika dicoba semua kemungkinan kombinasi antara karakter *upper case* dan *lower case* akan membutuhkan waktu sekitar 23 hari.

c. Metode ketiga adalah *trade-off*.

Hanya kombinasi-kombinasi yang mungkin yang dimasukkan dalam pencarian, sebagai contoh "password", "PASSWORD" dan "Password".

Kombinasi rumit seperti "pAssWoRd" tidak dimasukkan dalam proses. Dalam kasus ini, lambatnya proses dapat tertangani tetapi ada kemungkinan *password* tidak ditemukan.

II. METODE BRUTE FORCE ATTACK SECARA UMUM

2.1 Metode yang Dipakai Brute Force Attack

Brute Force attack ada 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 Password Cracker mencoba semua kombinasi yang mungkin dari karakter yang telah didefinisikan sebelum atau set karakter yang kustom melawan sebuah password yang telah terenkripsi di brute force dialog.

Kuncinya adalah mencoba semua kemungkinan password dengan formula seperti berikut.

$$KS = L^{(m)} + L^{(m+1)} + L^{(m+2)} + \dots + L^{(M)}$$

L = jumlah karakter yang kita ingin definsikan

m = panjang minimum dari kunci

M = panjang maksimal dari kunci

Contohnya saat kita ingin meretas sebuah LanManager passwords (LM) dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter, maka brute fore cracker harus mencoba $KS = 26^1 + 26^2 + 26^3 + \dots + 26^7 = 8353082582$ kunci yang berbeda. Jika ingin meretas password yang sama denganset karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#\$%^&*()-_+==`[]{}|;\":'<>.,?/", 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 sudah benar sesuai password, maka tinggal hanyalah jadi masalah waktu.

Perbandingan panjang kunci dengan jumlah permutasi

Key size dalam bits	Permutasi
8	2^8
40	2^{40}
56	2^{56}
64	2^{64}
128	2^{128}
256	2^{256}

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 Intelligence) 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 password 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 password atau passphrase yang dihasilkan dengan metode yang memberikan keamanan 128-bit:

- password 28-huruf acak dengan semua huruf tunggal kasus: "sqrnf oikas ocmpe vflte krbqa jwf"
- 20 karakter acak password 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 password 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 kriptanalisis paling kuat. Solusi lain adalah dengan menggunakan fungsi derivasi kunci (KDF) atau "key stretcher" yang melakukan pekerjaan komputasi yang signifikan dalam mengkonversi password 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 password, 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 password atau PIN.

2.3 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.

2.2 Kelas Serangan

Dalam subbab ini memperlihatkan aprosimasi waktu yang diperlukan sebuah komputer atau sebuah cluster komputer untuk menebak password. Gambar - gambar di bawah adakah aprosimasi dan waktu maksimal untuk menebak sebuah password 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 Passwords/sec Typical for recovery of Microsoft Office passwords on a Pentium 100
- Kelas B. 100,000 Passwords/sec Typical for recovery of Windows Password Cache (.PWL Files) passwords on a Pentium 100
- Kelas C. 1,000,000 Passwords/sec Typical for recovery of ZIP or ARJ passwords on a Pentium 100

- Kelas D. 10,000,000 Passwords/sec Fast PC, Dual Processor PC.
- Kelas E. 100,000,000 Passwords/sec Workstation, or multiple PC's working together.
- Kelas F. 1,000,000,000 Passwords/sec Typical for medium to large scale distributed computing, Supercomputers.

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

- 10 Karakter set

Numerals 0123456789							
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	100	Instant	Instant	Instant	Instant	Instant	Instant
3	1000	Instant	Instant	Instant	Instant	Instant	Instant
4	10,000	Instant	Instant	Instant	Instant	Instant	Instant
5	100,000	10 Secs	Instant	Instant	Instant	Instant	Instant
6	1 Million	1½ Mins	10 Seconds	Instant	Instant	Instant	Instant
7	10 Million	17 Mins	1½ Mins	1½ Mins	Instant	Instant	Instant
8	100 Million	2¾ Hours	17 Mins	1½ Mins	10 Seconds	Instant	Instant
9	1000 Million	28 Hours	2¾ Hours	17 Mins	1½ Mins	10 Seconds	Instant

- 36 karakter set (upper case ATAU lower case dan angka)

Upper Case Alpha ABCDEFGHIJKLMNOPQRSTUVWXYZ							
Lower Case Alpha abcdefghijklmnopqrstuvwxyz							
Numerals 0123456789							
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	1,296	Instant	Instant	Instant	Instant	Instant	Instant
3	46,656	4 Secs	Instant	Instant	Instant	Instant	Instant
4	1.6 million	2½ Mins	16 Seconds	1½ Seconds	Instant	Instant	Instant
5	60.4 million	1½ Hours	10 Mins	1 Min	Instant	Instant	Instant

- 52 karakter set (upper case dan lower case)

Mixed Alpha AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz							
Password		Class of Attack					
Length	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
2	2,704	Instant	Instant	Instant	Instant	Instant	Instant
3	140,608	14 Secs	< 2 Secs	Instant	Instant	Instant	Instant
4	73 Million	12½ Mins	1¼ Mins	8 Secs	Instant	Instant	Instant
5	380 Million	10½ Hours	1 Hour	6 Minutes	38 Secs	4 Secs	Instant
6	19 Billion	23 Days	2¼ Days	5½ Hours	33 Mins	3¼ Mins	19 Secs
7	1 Trillion	3¼ Years	119 Days	12 Days	28½ Hours	3 Hours	17 Mins
8	53 Trillion	169¼ Years	17 Years	1½ Years	62 Days	6 Days	15 Hours
9	2.7 Quadrillion	8,815 Years	881 Years	88 Years	9 Years	322 Days	32 Days

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

2.3 Contoh Kasus

Gambar di bawah ini mencontohkan 3 buah password dan waktu yang diperlukan tiap kelas komputer untuk menemukan passwordnya :

Sample Passwords		Class of Attack					
Pwd	Combinations	Class A	Class B	Class C	Class D	Class E	Class F
darren	308.9 Million	8½ Hours	5¼ Mins	5 Mins	30 Secs	3 Secs	Instant
Land3rz	3.5 Trillion	11 Years	1 Year	41 Days	4 Days	10 Hours	58 Mins
B33r&Mug	7.2 Quadrillion	22.875 Years	2.287 Years	229 Years	23 Years	2¼ Years	83½ Days

Salah satu kasus yang dapat diteliti dengan algoritma ini adalah kasus untuk sebuah PIN ATM :

PIN ATM kita yang menggunakan seluruhnya angka (C =

10) dengan jumlah karakter 4 (n = 4) atau 6 (n = 6), maka dengan menggunakan algoritma/cara yang sama serangan dengan serangan dengan menggunakan bruteforce attack dapat ditabulasikan sbb:

Pass C=10	Kelas Serangan					
	n	A	B	C	D	E
4	1s	0.1s	0.01s	0.001s	0.0001s	0.00001s
6	2m	10s	1s	0.1s	0.01s	0.001s

III. CONTOH PROGRAM YANG MENERAPKAN BRUTE FORCE ATTACK

3.1 Cain and Abel

Cain & Abel adalah alat recovery password untuk Sistem Operasi Microsoft. Hal ini memungkinkan recovery berbagai jenis password dengan mengendus jaringan, cracking password terenkripsi menggunakan Dictionary-Attack, Brute-Force Attack dan serangan kriptanalisis, merekam percakapan VoIP, decoding password teracak, memulihkan kunci jaringan wireless, mengungkap password cache dan menganalisis routing protokol. Program ini tidak memanfaatkan kerentanan perangkat lunak atau bug yang tidak dapat diperbaiki. Ini mencakup beberapa aspek keamanan / kelemahan yang ada dalam protokol standar, metode otentikasi dan mekanisme caching; tujuan utamanya adalah pemulihan password dan kredensial dari berbagai sumber, namun juga kapal beberapa fungsi "non standard" untuk pengguna Microsoft Windows.

Cain & Abel telah dikembangkan dengan harapan akan berguna bagi administrator jaringan, guru, konsultan keamanan / profesional, staf forensik, vendor keamanan perangkat lunak, tester penetrasi profesional dan semua orang yang berencana untuk menggunakannya untuk alasan yang etis. Pembuat program ini tidak akan membantu atau mendukung setiap aktivitas ilegal dilakukan dengan program ini. Diperingatkan bahwa ada kemungkinan bahwa pemakaian software ini bisa menyebabkan kerusakan dan / atau kehilangan data dan pembuat software tidak bertanggung jawab atas kerusakan atau kehilangan data.

Versi Cain and Abel terbaru lebih cepat dan berisi banyak fitur baru seperti APR (Arp Poison Routing) yang memungkinkan sniffing di switched LAN. Sniffer dalam versi ini juga dapat menganalisa protokol terenkripsi seperti SSH-1 dan HTTPS, dan berisi filter untuk menangkap berbagai mekanisme otentikasi. Versi baru ini juga memonitor otentikasi routing protokol dan kamus dan brute-force cracker untuk semua algoritma hashing umum dan untuk otentikasi spesifik, kalkulator password/hash, serangan kriptanalisis, dekoder password

dan beberapa utilitas tidak begitu umum yang terkait dengan jaringan dan sistem keamanan.

3.2 Brutus

Ada puluhan cracker password offline untuk resource yang dilindungi sandi. Cracker tersebut dirancang untuk mencari password yang lemah dan memberitahu administrator bagaimana seaman apa sumber daya itu sebenarnya.

Brutus adalah jenis cracker password yang berbeda. Ia bekerja online, mencoba membobol telnet, POP3, FTP, HTTP, RAS atau IMAP dengan hanya mencoba untuk login sebagai pengguna yang sah. Brutus meniru serangan dari luar seperti pada kenyataannya (tidak seperti cracking password aplikasi lain yang mensimulasikan serangan internal) dan dengan demikian berfungsi sebagai alat keamanan audit berharga.

Brutus dapat berjalan dalam modus single user (mencoba masuk ke akun pengguna tunggal dengan mencoba kombinasi password yang berbeda) atau dengan mencoba daftar kombinasi user / password dari file word. Aplikasi akan memindai host untuk layanan yang dikenal dan dapat dengan mudah dimodifikasi untuk break-in layanan kustom lain yang membutuhkan logon interaktif dari sebuah username dan password.

Menggunakan Brutus akan mengajarkan Anda banyak tentang sistem, karena mensimulasikan serangan nyata. Untuk membuat baik penggunaan simulasi serangan Brutus, seorang administrator harus yang perhatikan apakah usaha break-in akan dicatat, dan apakah timeout dikeluarkan setelah beberapa kali gagal login - ini dapat dengan mudah dilihat pada kemajuan yang dibuat Brutus.

3.3 Hydra

Hydra adalah sebuah proyek software yang dikembangkan oleh sebuah organisasi bernama "The Hacker's Choice" (THC) yang menggunakan brute force dan dictionary attack untuk menguji untuk password yang lemah atau password sederhana pada satu atau banyak host remote menjalankan berbagai layanan yang berbeda. Ia dirancang sebagai bukti untuk menunjukkan kemudahan cracking password karena password yang dipilih buruk.

Proyek ini mendukung berbagai layanan dan protokol: AFP, TELNET, FTP, Firebird, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MySQL, REXEC, RSH, rlogin, CVS, Subversion, SNMP, SMTP - AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, NCP, PCNFS, ICQ, SAP/R3, LDAP, PostgreSQL, TeamSpeak, Cisco auth, Cisco memungkinkan, dan Cisco AAA.

3.4 LastBit

LastBit Software adalah sebuah perusahaan pengembangan perangkat lunak Rusia berfokus pada solusi password recovery dan security tools. LastBit Software adalah perusahaan pertama yang mengembangkan tool recovery password untuk Microsoft

Office Word dan Excel dan memberikan recovery password dengan metode unik yang menjamin pemulihan password berhasil terlepas dari panjang password.

Aplikasi password recovery pertama diluncurkan pada tahun 1997. Sejak itu LastBit mengembangkan yang dikembangkan banyak solusi password recovery untuk aplikasi paling populer.

Smart Force Attack adalah penyempurnaan varian serangan Brute force, dikembangkan oleh LastBit Corp Metode. Recovery password didasarkan pada anggapan bahwa password yang terdiri dari huruf dan masuk akal. Smart Force Attack didasarkan pada tabel statistik yang dibangun dengan cara menganalisis sejumlah besar teks. Dengan cara ini, lebih efektif karena karena tidak memeriksa berarti kombinasi huruf.

Efektivitas metode ini dapat dibandingkan dengan Dictionary attack dengan sebuah kamus yang panjang. Jika password dihasilkan secara otomatis (secara acak), Smart Force Attack metode tidak dapat digunakan. Hal ini juga tidak akan memulihkan password dengan angka dan karakter non-alpha. Last memungkinkan untuk memeriksa sampai dengan 11 karakter dalam jumlah waktu yang wajar dengan Smart metode Attack Force.

3.5 John The Ripper

John the Ripper merupakan password cracking perangkat lunak gratis. Awalnya dikembangkan untuk sistem operasi UNIX, yang saat ini berjalan pada 15 platform yang berbeda (11 arsitektur spesifik Unix, DOS, Win32, BeOS, dan OpenVMS). Ini adalah salah satu program pengujian password yang paling populer dengan mengombinasikan sejumlah password cracker ke dalam satu paket, autodetects jenis hash password, dan memasukkan cracker yang dapat dimodifikasi.

Hal ini dapat dijalankan terhadap berbagai format password terenkripsi termasuk beberapa jenis hash password crypt paling sering ditemukan pada berbagai Unix (berdasarkan DES, MD5, atau Blowfish), Kerberos AFS, dan Windows NT/2000/XP/2003 LM hash. Beberapa modul tambahan telah memperluas kemampuannya untuk memasukkan password hash MD4 berbasis dan password disimpan di LDAP, MySQL dan lain-lain.

Salah satu mode yang John dapat gunakan adalah dictionary attack. Dibutuhkan sampel text string (biasanya dari file, yang disebut sebuah wordlist, berisi kata-kata ditemukan dalam kamus), menyandikannya dalam format yang sama sebagai password yang diuji (termasuk algoritma enkripsi dan kunci), dan membandingkan output ke dienkripsi string. Hal ini juga dapat melakukan berbagai perubahan ke dalam kamus kata-kata yang dicoba ini. Banyak perubahan ini yang juga digunakan dalam modus serangan tunggal John, yang memodifikasi sebuah plaintext yang terkait (seperti username dengan password terenkripsi) dan memeriksa variasi terhadap hash dienkripsi.

John juga menawarkan modus brute force attack. Dalam jenis serangan ini, program ini berjalan melalui semua plaintexts mungkin, hashing masing-masing dan membandingkannya dengan hash input. John

menggunakan tabel frekuensi karakter untuk mencoba plaintexts mengandung lebih karakter yang sering digunakan pertama. Metode ini berguna untuk cracking password yang tidak muncul dalam kamus daftar kata, tetapi tidak butuh waktu lama untuk dijalankan

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 Web kecuali mempunyai mekanisme defense tersendiri.

Cara efektif untuk mengalahkan brute force attack adalah mengharuskan semua user memilih password yang kuat. Password juga disarankan mempunyai sedikitnya 7 karakter, dengan campuran huruf besar dan kecil, angka, dan tanda baca. Selain itu, buat pesan yang ditampilkan oleh login failure seambigu mungkin, seperti "invalid username or password". Pesan seperti ini tidak akan memberikan informasi yang ekstra tentang sistem sehingga hacker yang menggunakan brute force atau dictionary attack tidak dapat mengambil untung dan meringankan pekerjaannya.

Cracking dengan Brute Force akan sangat lamban jika dihadapkan pada enkripsi yang kuat, (misalnya dengan ukuran password yang lebih panjang) dan algoritma yang lebih pelan. Enkripsi kuat modern juga dapat menahan brute force attack dengan memberikan mereka banyak waktu pengerjaan. Enkripsi data membuat sebuah akses data menjadi sulit sehingga malicious cracker bisa mengganti target mereka daripada membuang sumber daya untuk menghadapi enkripsi yang kuat.

REFERENSI

- [1] *Algoritma Brute Force Bagian 2 - Algoritma Brute Force (lanjutan).ppt*. Munir, Rinaldi.
- [2] www.computerhope.com/jargon/b/brutforc.htm tanggal akses 4 Desember 2010
- [3] *Pattern Matcing.ppt* Munir, Rinaldi
- [4] Munir, Rinaldi, "IF2251 STRATEGI ALGRORITMIK Diktat Kuliah Strategi Algoritmik", Departemen Teknik Informatika, 2006.
- [5] Penggunaan *Brute Force* untuk Meretas *Password File Rar*, Fajar Zaki Al Faris 2006
- [6] <http://www.hoobie.net/brutus/> tanggal akses 4 Desember 09.30
- [7] www.tech-faq.com/brute-force-attack.html. tanggal akses 4 Desember 2010
- [8] <http://www.securiteam.com/tools/2QUQ2PPRPG.html> , 4 Desember 2010 pukul 09.30
- [9] http://www.hackingspirits.com/eth-hac/tools/brute_force.html, tanggal akses 4 Desember 2010 09.17.
- [10] <http://www.lockdown.co.uk/?pg=combi&s=articles> , tanggal akses 7 Desember 2010 pukul 07.28
- [11] www.mandylionlabs.com/PRCCalc/BruteForceCalc.htm tanggal akses 5 Desember 2010

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 8 Desember 2010



Krisnaldi Eka Pramudita