PENERAPAN ALGORITMA *BRUTE FORCE* PADA SISTEM INFORMASI AKADEMIK UNIVERSITAS BINA DARMA

Dimas Adhi Pratama[1], Deni Erlansyah[2], Febriyanti Panjaitan[3]
Fakultas Teknik Ilmu Komputer, Universitas Bina Darma
Email: 141420183@student.binadarma.ac.id[1], deni@binadarma.ac.id[2],
febriyanti_panjaitan@binadarma.ac.id[3]

ABSTRACT

Bina Darma University has a website where visitors can access various information, but specifically to enter the academic information system, students need to log in first. The log in page is implemented so that the page visitors who obtain the information are truly legitimate and authenticated people. The purpose of this study is to determine the speed performance of the Brute Force Algorithm to find out how well the security of the Bina Darma university's academic information system website from brute force attacks so that researchers are able to understand how the brute force attack works so that the best way to be safe from the attack can be obtained. This research uses C # programming language and Microsot Visual Studio as a text editor. The process of sending 500 - 4000 data produces an average time of 0.17 seconds while for the manual process requires 16 seconds.

Keywords : *Algoritma Brute Force*, Information Systems, *Log* In, Universitas Bina Darma, Brute *Force Attacking*.

ABSTRAK

Universitas Bina Darma memiliki *website* di mana pengunjung dapat mengakses beragam informasi, namun khusus untuk masuk ke sistem informasi akademik, mahasiswa/i perlu melakukan *log in* terlebih dahulu. Halaman *log in* diterapkan agar supaya pengunjung halaman yang memperoleh informasi tersebut benar-benar orang yang sah dan terotentikasi. Tujuan penelitian ini yakni mengetahui performa kecepatan Algoritma *Brute Force* untuk mengetahui seberapa baik keamanan halaman log in *website* sistem informasi akademik universitas Bina Darma dari serangan *brute force* sehingga peneliti mampu memahami cara kerja serangan *brute force* agar dapat diperoleh jalan terbaik untuk dapat aman dari serangan tersebut. Penelitan ini menggunakan bahasa pemograman *C#* dan *Microsot Visual Studio* sebagai text editor. Proses pengiriman 500 – 4000 data menghasilkan waktu rata-rata 0,17 detik sedangkan untuk proses manual memerlukan waktu 16 detik.

Kata Kunci : *Algoritma Brute Force*, Sistem Informasi, *Log* In, Universitas Bina Darma, serangan Brute *Force*.

1. PENDAHULUAN

Banyak sekali layanan yang dibangun dan dapat dinikmati di jaringan internet salah satu contohnya adalah *website*. w*ebsite* dapat menampilkan informasi di internet, baik itu berupa teks, gambar, video & suara maupun interaktif memiliki keuntungan yang menghubungkan (*link*) dari dokumen dengan dokumen lainnya (*hypertext*) yang dapat diakses melalui *browser*. Semua instansi baik pemerintah maupun swasta hampir semuanya memiliki *website* sebagai portal informasi, agar pengunjung dapat mengetahui dengan baik apa yang mereka tawarkan atau sampaikan melalui *website*nya.

Universitas Bina Darma memiliki *website* di mana pengunjung dapat mengakses beragam informasi mulai dari profil, sejarah, berita seputar kegiatan kampus bahkan mahasiswa/i secara khusus dapat mengakses profil akademik mereka di sistem informasi akademik . Namun khusus untuk masuk ke sistem informasi akademik, mahasiswa/i perlu melakukan *log in* terlebih dahulu. Halaman log in diterapkan agar supaya pengunjung halaman yang memperoleh informasi tersebut benar-benar orang yang sah dan terotentikasi.

Meskipun sudah dilengkapi dengan halaman log in sebagai jalan utama untuk otentikasi pengguna, tentu saja tidak ada jaminan akan keamanannya secara penuh. Sebagaimana maraknya *cyber attack (https://kominfo.go.id)* yang sering menghantui situs-situs, mulai dari penyerangan terhadap *server* itu sendiri dengan berbagai macam metode sampai dengan pencurian *password* agar memperoleh otentikasi.

Salah satu bentuk serangan terhadap *password* adalah serangan *brute-force*. Merupakan sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. (Krisnaldi Eka Pramudita:2010) . Istilah *brute-force* sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: "*When in doubt, use brute-force*" (jika ragu, gunakan brute-force). (Renaldi Munir:2009)

Maka dari itu setelah melihat dari kenyataan bahaya keamanan di dunia internet, selanjutnya mencari tahu, menganalisis serta mengukur seberapa amankan *website* yang telah dibangun untuk pengunjung *website* nantinya terhadap serangan *brute force.*

Dari uraian di atas maka penulis mengajukan sebuah judul, yaitu "Penerapan Algoritma Brute Force Pada Sistem Informasi Akademik Universitas Bina Darma" dengan harapan dapat menguji dan menganalisis tingkat keamanan halaman log in situs universitas Bina Darma terhadap serangan *brute force*.

2. METODOLOGI PENELITIAN

2.1 Metode Rekayasa

Penelitian rekayasa adalah penelitian yang menerapkan ilmu pengetahuan menjadi suatu rancangan guna mendapatkan kinerja sesuai dengan persyaratan yang ditentukan. Penelitian berawal dari menentukan spesifikasi rancangan yang memenuhi spesifikasi yang ditentukan, memilih alternatif yang terbaik, dan membuktikan bahwa rancangan yang dipilih dapat memenuhi persyaratan yang ditentukan secara efisiensi, efektif dan dengan biaya yang murah. Penelitian perangkat lunak komputer dapat digolongkan dalam penelitian rekayasa.

2.2 Metode Pengumpulan Data

Dalam penelitian ini metode pengumpulan data yang digunakan pada perancangan aplikasi tersebut adalah studi literatur. Metode ini dilaksanakan dengan melakukan studi kepustakaan yang relevan. Metode ini dilakukan untuk mencari sumber pelengkap yang berhubungan dengan aplikasi yang akan dibangun, yaitu dengan mencari referensi yang berkaitan dengan aplikasi yang akan di buat, sehingga dapat di implementasikan dalam aplikasi tersebut, mulai dari buku-buku, jurnal maupun artikel dan sumber-sumber lain di internet.

2.3 Metode Pengembangan Perangkat lunak

Dalam teori rekayasa perangkat lunak terdapat beberapa macam model pengembangan perangkat lunak. Model pengembangan yang digunakan dalam penelitian ini adalah model SDLC air terjun (*waterfall)* sering juga disebut model sekuensial linier (*sequential linear*) atau alur hidup klasik (*classic life cycle*). Menurut Rosa dan Shalahuddin (2014:28-30) model *waterfall* menyediakan pendekatan alur hidup perangkat lunak secara sekuensial atau terurut dimulai dari analisis, desain, pengodean, pengujian, dan tahap pendukung (*support*).

2.4 Metode Pengujian

Metode pengujian menggunakan *Penetration Testing*. Proses pengujian keamanan jaringan melalui beberapa tahap sebagai berikut (Rathore dkk, 2006)

1. ***Information Gathering***

Pada tahap ini peneliti mencari informasi yang dibutuhkan sebelum melakukan tindakan pengujian. Peneliti akan menelusuri untuk memperoleh informasi berupa nama dari objek *html* yang mengidentifikasikan kotak *input* nama pengguna atau nim dan juga kata sandi.

2. ***Analisis***

Peneliti selanjutnya melakukan analisis untuk menentukan jenis tindakan dan kebutuhan pengujian dengan penetrasi. Peneliti mempelajari akankah ada pemblokiran oleh situs jika terjadi kesalahan kata sandi sebanyak lebih dari beberapa kali , katakanlah 3 kali atau tidak. Dan satu lagi melihat hasil dari respon server jika kata sandi dianggap salah misal tampak ada kata-kata "Kata Sandi Anda Salah".

3. ***Attacking***

Pada tahap ini peneliti akan melakukan serangan terhadap data yang sudah diperoleh dari *information gathering* dengan menciptakan perangkat lunak yang secara langsung mengimplementasikan Algoritma Burte Force dengan bahasa pemrograman pemrograman *C#* .

4. **Evaluasi**

Pada tahap ini hasil yang didapat dari pengujian kemudian dijadikan bahan evaluasi untuk dilaporkan kepada pihak pengelola atau institusi pemilik *Web*.

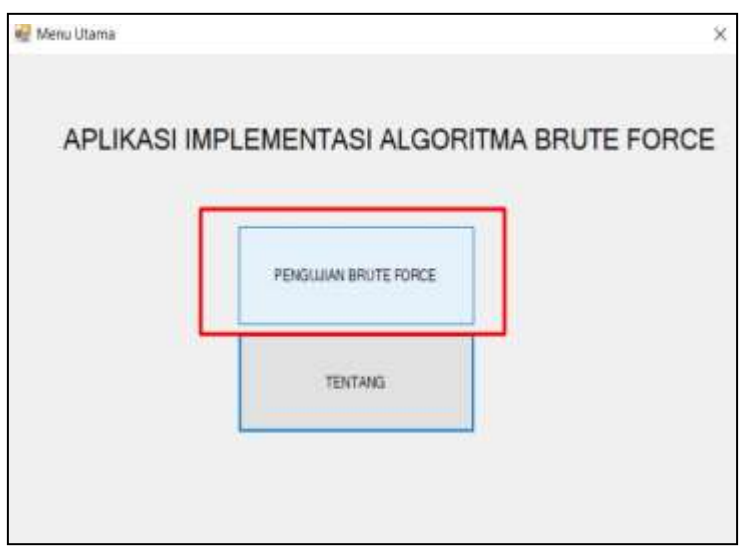
3. HASIL DAN PEMBAHASAN

3.1 Hasil

Hasil yang diperoleh dalam penelitian ini adalah sebuah aplikasi yang telah menerapkan algoritma *brute force* untuk menguji keamanan sistem informasi akademik binadarma

a. Menu Beranda Halaman

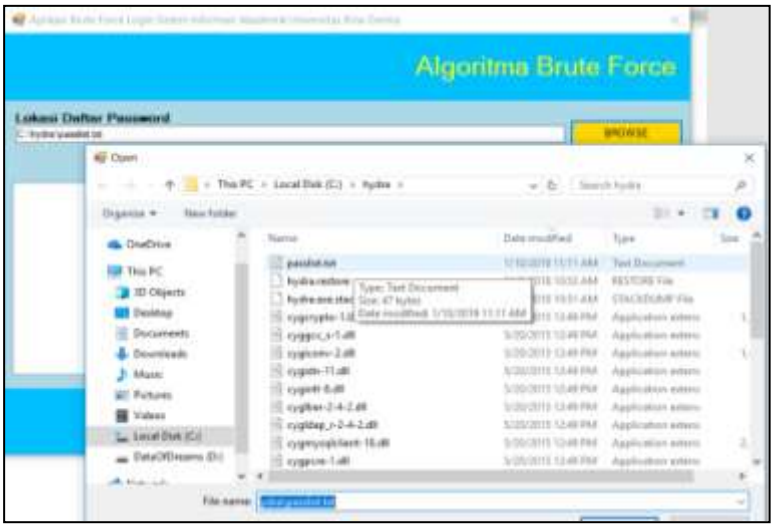
pengguna beranda ini merupakan halaman utama ketika pengguna membuka aplikasi.



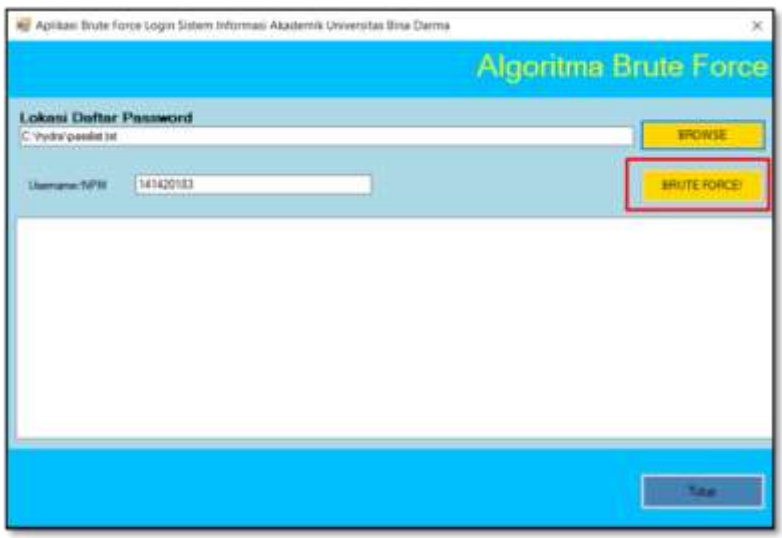
Gambar 1. Menu Beranda

b. **Halaman Pengujian *Brute Force***

Setelah mengklik menu pengujian *brute force* maka akan dihantarkan pada form untuk menjalankan secara langsung algoritma *brute force* dengan mengklik tombol pengujian *brute force* setelah sebelumnya memilih daftar kata sandi yang sudah disiapkan, maka berikutnya adalah cukup menekan tombol *brute force*, maka algoritma *brute force* secara otomatis akan dijalankan.



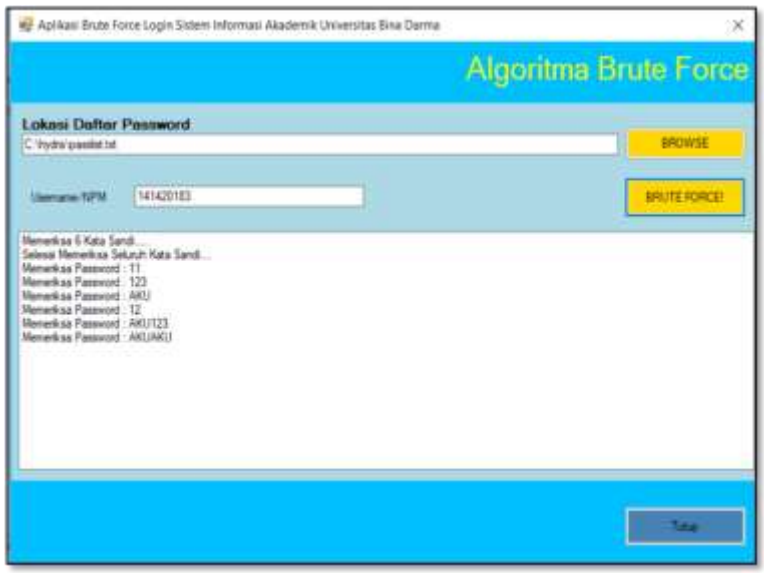
Gambar 2. *Dialog Pemilihan Daftar Kata Sandi*



Gambar 3. Halaman Pengujian

c. Hasil ketika tidak menemukan kata sandi yang benar

Setelah tombol *brute force* diklik, kemungkinan pertama dalah kata sandi tidak dapat ditebak atau ditemukan. Berikut contoh tampilan jika aplikasi yang menjalankan algoritma *brute force* tidak menemukan hasil atau menemukan kata sandi yang tepat.



Gambar 4. Tampilan Hasil ketika kata sandi tidak ditemukan

d. Hasil ketika menemukan kata sandi yang benar

Kemungkinan yang lain adalah ketika kata sandi berhasil ditemukan dalam kamus. Setelah pencarian yang panjang ketika sistem menemukan, langsung menampilkannya ke layar seperti pada gambar di bawah ini.

Gambar 5. Tampilan Hasil ketika kata sandi ditemukan

e. Menu Tentang

Halaman pengguna Tentang merupakan halaman yang berisi informasi umum mengenai pembuat aplikasi.

Gambar 6. Menu Tentang

3.2 Pembahasan

Berdasarkan hasil dari pengujian program dan sistem *login* bina darma, diperoleh analisa sebagai berikut:

1. Kata sandi akan ditemukan selama ada dalam daftar kata sandi pengujian
2. Kata sandi tidak akan ditemukan jika tidak berada dalam daftar kata sandi pengujian
3. Sistem *login* Sistem Informasi Akademik Universitas Bina Darma tidak memiliki pembatasan hak akses untuk melakukan penyerangan secara terus menerus menggunakan Algoritma *Brute Force* hingga kata sandi dapat ditemukan.
4. Waktu proses tergantung berapa banyak percobaan kata sandi dan kestabilan koneksi internet.

4. KESIMPULAN

Setelah dilakukannya analisa terhadap Sistem informasi akademik Universitas Bina Darma dengan menggunakan teknik *brute force*, maka dari itu peneliti dapat meyimpulkan hasil dari penelitian sebagai berikut :

Performa kecepatan algoritma *Brute Force* dalam sistem yang dibangun sangat cepat dibandingkan penyerangan melalui halaman langsung yakni halaman sisfo.binadarma.ac.id. Proses pengiriman data yang berjumlah 500 hingga 4000 *password* menghasilkan lama waktu rata-rata pengiriman satu *username* dan *password* yakni 0,17 detik sedangkan pengiriman data input langsung kehalaman sisfo memerlukan waktu 16 detik per satu proses.

Login Sistem informasi Akademik Universitas Bina Darma Palembang telah memenuhi strandar pembuatan namun masih memiliki celah keamanan dalam proses attacking seperti belum memiliki aturan pembatasan hak akses jika melakukan kesalahan dalam memasukan kata sandi lebih dari 3 kali.

Penyerangan *Brute Force* dilakukan dengan meretas *password* dengan cara mencoba semua kemungkinan kombinasi yang ada pada *wordlist*, proses penyerangan dilakukan dengan mengirim permintaan dan membaca response dari suatu url untuk ditindaklanjutin. Pencegahannya *brute force* dapat dilakukan dengan membatasi akses pengguna seperti aturan blokir tiga kali salah memasukan *login*, mengaktifkan *sensitive case* pada setiap input yang masuk dan sering-sering mengubah *password* pada akun sehingga terhindar dari serangan *brute force*.

DAFTAR PUSTAKA

[1] Agus Eka, Pratama. 2014. *Sistem Informasi dan Implementasinya*. Bandung: Informatika Bandung.

[2] Apdilah, D. 2017. *Analisa Suku Kata Yang Sama Menggunakan Metode Brute Force*. AMIK INTeL Com Global Indo.

[3] Boone, Louis E dan Kurtz, David L. 2002.*Pengantar Bisnis Jilid ke 1*. Singapore:Thompson Learning.Hardjono, D. 2013. *Seri Panduan Lengkap Menguasai Pemograman Web dengan PHP 5.* Yogyakarta:Andi.

[4] Eka Pramudita, Krisnaldi. 2010. *Brute Force Attack dan Penerapannya pada Password Cracking*. Institue Teknologi Bandung.

[5] Hanson, Ward. 2000. *Pemasaran Internet.* Jakarta:Salemba Empat**.**

[6] Setiarso, B., Triono, N. H., & Sugabyo, H. 2009. *Penerapan Knowledge Management Pada Organisasi* (Pertama). Yogyakarta: Graha Ilmu.

[7] Supardi, Yuniar. 2015. *Belajar Coding Android Bagi Pemula*. Jakarta:Flex Media Komputindo

[8] Munawar. 2005. *Pemodelan Visual dengan UML*. Yogyakarta: Graha Ilmu.

[9] Rosa dan Shalahuddin. 2013. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Informatika: Bandung.

[10] Murad. 2013. *Membuat Diagram Dan Gambar Teknik Dengan Menggunakan Microsoft Visio. 2003*. Yogyakarta: Graha Ilmu.

[11] Rathore, B., & Oissg. 2006. *ISSAF-Information Systens Security Assessment Framework 0.2.1B*, 845.

[12] Munir, Rinaldi. 2006. Brute Force Attack dan Penerapanya pada Password Cracking. Jakarta:Salemba Empat.

[13] Raharjo, Suwanto. 2004. *Teori, Analisa, dan Implementasi Jaringan Tanpa Disk Pada GNU/Linuk.* Yogyakarta:Andi.