Pembobolan Password Menggunakan Teknik Dictionary Attack dengan Menggunakan Bahasa Pemrograman Pyhton dan Cara Mengantisipasinya

**Salma Nur Oktavia1**

1Department of Informatics, UIN Sunan Gunung Djati Bandung, Indonesia

|  |  |  |
| --- | --- | --- |
| **Article Info** |  | ABSTRAK (10 PT) |
| ***Article history:***  Received  Revised  Accepted |  | Perkembangan teknologi yang pesat telat mengubah cara hidup, kerja, dan interaksi antar satu sama lain. Teknologi dapat mengakses berbagai sumber informasi dan berbagai pengetahuan dengan mudah melalui internet. Teknologi diciptakan untuk membantu pekerjaan manusia. Akan tetapi, dengan mengetahui penerapan teknik dictionary attack berorientasi memungkinkan pengguna untuk berhati-hati dalam memilah dan memilih kata sandi serta bijak dalam penggunaan teknologi. Hasil pengujian menunjukkan keberhasilan program dengan memecahkan kode yang ada pada kamus. Artikel ini memberikan panduan praktis bagi pengembangan yang ingin memahami cara mengimplementasikan teknik dictionary attack dengan bahasa pemrograman pyhton.Makalah ini membahas mengenai dictionary attackmengenai penjelasan singkat, prinsip kerja, dan bagaimana pengembangan dari dictionary attack dalam konteks penerapannya untuk membobol password sebuah akun tertentu. Selain itu, pada jurnal laporan ini akan dianalisis kelebihan dan kelemahan dictionary attack dan masing-masing modifikasinya, serta solusi yang dapat dilakukan dalam mengantisipasi dari serangan dictionary attack. |
| ***Kata kunci:***  Bahasa Pemrograman Phyton  Dictionary Attack  Burte force  Password  List of hash  Hacker  Serangan  Cyber Cyber security |
| ***Corresponding Author:***  Salma Nur Oktavia,  Informatics Department, Faculty of Science & Technology, UIN Sunan Gunung Djati Bandung  Jl. A. H. Nasution No. 105, Cibiru, Bandung, Indonesia. 40614  Email: salmanuroktavia2004@gmail.com | | |

# PENDAHULUAN

Perkembangan teknologi yang pesat telah mengubah cara hidup, bekerja, dan berinteraksi antar satu sama lain. Teknologi dapat mengakses berbagai sumber informasi dan berbagi pengetahuan dengan mudah melalui internet.Teknologi meningkatkan efisiensi dan efektivitas pekerjaan dengan menggunakan perangkat keras dan perangkat lunak komputer yang canggih untuk memproses data, membuat produk, dan menyediakan layanan.[1]

Dalam konteks ini, artikel membahas tentang pembobolan password menggunakan teknik dictionary attack dengan menggunakan bahasa pemrograman pyhton dan cara mengantisipasinya. Pemilihan pyhton sebagai implementasi pembobolan password karena terkenal sebagai bahasa pemrograman yang banyak digunakan oleh hacker. [3]

Dictionary attack memanfaatkan psikologi manusia. yaitu kebiasaan bahwa kebanyakan orang akan menggunakan kombinasi kata yang berhubungan dengan kehidupannya sehari-hari dalam membuat password, misalnya tanggal lahir, makanan kesukaan, nama orang tua, dan lain-lain. Kata-kata ini merupakan kata yang terdapat dalam kamus (karena merupakan kata yang digunakan sehari-hari) dan mudah diingat. Psikologi manusia dalam membuat password juga telah dikaji dan dibuktikan dengan penelitian.Pendahuluan ini juga memberikan gambaran umum tentang penjelasan dictionary attack dan cara kerjanya dalam usaha pembobolan password. Serta memberikan solusi, bagaimana mengantisipasi serangan dictionary attack.

# METODE

Untuk melakukan peretasan dengan teknik dictionary attack pada dasarnya ada tiga langkah yaitu, langkah pertama membuat sebuah daftar kata sandi yang berpotensial. Isi daftar biasanya akan mencakup variasi-variasi dari kata-kata seperti kombinasi kata yang berbeda atau penambahan karakter khusus. Langkah kedua, perangkat lunak akan otomatis menggunakan kamus brute force untuk meretas akun online. Menggunakan daftar kata sandi dan alat otomatis secara bersamaan sehingga membuat pemecahan kata sandi lebih cepat dibandingankan secara manual. Langkah ketiga, peretas mencuri dan mengekspos data sensitif yang tersimpan di profil yang berpotensi mendapatkan keuntungan atau niat jahat.

Logo

Description automatically generated

# HASIL DAN PEMBAHASAN

Fungsi crackHash dirancang untuk mencari kata sandi yang sesuai dengan hash yang disediakan sebagai argumen. Dalam kasus ini, hash yang dicari adalah "1a1dc91c907325c69271ddf0c944bc72", dan wordlist.txt berisi beberapa kata sandi yang mungkin sesuai.

## 3.1. Hasil

1. Source Code Python

import hashlib

def crackHash(*inputPass*):

    try:

        passFile = open("worldlist.txt", "r")

    except:

        print("Cloud not find file.")

    for password in passFile:

        encPass = password.encode("utf-8")

        digest = hashlib.md5(encPass.strip()).hexdigest()

        if digest == *inputPass*:

            print("Password Found: " + password)

if \_\_name\_\_ == '\_\_main\_\_' :

    crackHash("1a1dc91c907325c69271ddf0c944bc72")

Jika menggunakan wordlist.txt dengan konten sebagai berikut:

123124

admin

pass

password

Dan jika hash yang dicari adalah "1a1dc91c907325c69271ddf0c944bc72", berikut adalah contoh output yang mungkin dihasilkan:

1. Output



kata sandi yang cocok dengan hash yang dicari adalah "password". Harap dicatat bahwa hasilnya akan bergantung pada kata sandi yang ada dalam wordlist.txt dan hash yang dicari.

## 3.2. Pembahasan

Di era globalisasi ini, manusia di seluruh dunia semakin memanfaatkan teknologi informasi dalam kehidupannya sehari-hari. Saat ini internet sudah bukan barang baru bagi masyarakat. Sudah banyak kegiatan bisnis, transaksi keuangan, komunikasi, bahkan blogging dan jejaring sosial yang menggunakan internet. Informasi pribadi seseorang sudah semakin mudah dicari melalui search engine dan jejaring sosial.[5]

Sebuah akun, baik akun email, administrator situs web, akun transaksi jual beli, dan lain-lain merupakan hal yang bersifat pribadi karena bisa mengandung informasi sensitif. Oleh karena itu, saat ini kriptografi dan sistem keamanan komputer terhadap akun sangat dibutuhkan. Akan tetapi, ironisnya ketika ilmu kriptografi untuk mengenkripsi sebuah informasi semakin berkembang, semakin berkembang pula cara untuk melawannya. Dictionary attack merupakan salah satu bentuk serangan terhadap kriptografi yang hingga saat ini masih dianggap efektif untuk memecahkan kode password sebuah akun. [4]

Dictionary attack memanfaatkan psikologi manusia. yaitu kebiasaan bahwa kebanyakan orang akan menggunakan kombinasi kata yang berhubungan dengan kehidupannya sehari-hari dalam membuat password, misalnya tanggal lahir, makanan kesukaan, nama orang tua, dan lain-lain. Kata-kata ini merupakan kata yang terdapat dalam kamus (karena merupakan kata yang digunakan sehari-hari) dan mudah diingat. Psikologi manusia dalam membuat password juga telah dikaji dan dibuktikan dengan penelitian [2].

1. **KESIMPULAN**

Dalam era globalisasi ini, pemanfaatan teknologi informasi telah menjadi bagian integral dari kehidupan sehari-hari manusia di seluruh dunia. Internet telah menjadi sarana yang umum digunakan dalam berbagai aktivitas, termasuk bisnis, transaksi keuangan, komunikasi, blogging, dan jejaring sosial. Namun, semakin berkembangnya teknologi juga menimbulkan tantangan baru terkait keamanan, terutama dalam melindungi informasi pribadi yang dapat dengan mudah diakses melalui mesin pencari dan jejaring sosial.

Akun-akun seperti email, administrator situs web, dan akun transaksi jual beli menjadi aspek yang sangat pribadi karena mengandung informasi sensitif. Oleh karena itu, perlindungan terhadap akun menggunakan kriptografi dan sistem keamanan komputer menjadi sangat penting. Meskipun demikian, paradoksnya adalah seiring dengan kemajuan ilmu kriptografi untuk mengamankan informasi, juga muncul metode baru untuk melawannya. Salah satu bentuk serangan yang tetap dianggap efektif adalah Dictionary Attack, yang memanfaatkan psikologi manusia dalam pemilihan kata sandi.

Penelitian menunjukkan bahwa kebanyakan orang cenderung menggunakan kombinasi kata yang terkait dengan kehidupan sehari-hari mereka dalam membuat kata sandi, seperti tanggal lahir, makanan kesukaan, atau nama orang tua. Kata-kata ini, karena sering digunakan dalam kamus dan mudah diingat, menjadi target utama dalam serangan Dictionary Attack. Psikologi manusia dalam pembuatan kata sandi telah dikaji dan terbukti, menciptakan tantangan baru dalam upaya memastikan keamanan akun.

Dengan demikian, perlindungan akun melalui kriptografi dan sistem keamanan komputer tidak hanya mengandalkan pada perkembangan teknologi, tetapi juga memerlukan kesadaran akan praktik keamanan yang baik dari pengguna. Kombinasi pendekatan teknis dan pemahaman psikologis dapat membantu meningkatkan keamanan informasi pribadi dalam era digital ini.

# REFERENSI

[1] Analisis Dictionary Attack dan Modifikasinya Dalam Membobol Password Serta Solusi Melawannya - Informatika.

[2] The Imperva Application Defense Center (ADC). (2010). http://www.imperva.com/docs/WP\_Consumer\_Password\_Worst\_Practices.pdf.

[3] Kriptografi Dengan Python - OSF.

[4] Exabytes: "Brute Force: Pengertian, Metode, dan Cara Mencegahnya".

[5] Academia.edu: "Brute Force Attack dan Penerapannya pada Password Cracking".