Katalis Pendidikan: Jurnal Ilmu Pendidikan dan Matematika
Volume 2, Nomor 2, Juni 2025
e-ISSN: 3046-5699; p-ISSN: 3046-6156, Hal. 49-64
DOI: https://doi.org/10.62383/katalis.v2i2.1463
Available Online at: https://journal.lpkd.or.id/index.php/Katalis

Analisis Kombinatorik Dalam Menentukan Keamanan dan Kompleksitas Password dengan Penerapan Teori Kombinatorik

Arnah Ritonga[1*], Bobby Putra Delon Togatorop[2], Herdita Br Ginting[3], Klara Manila Laoli[4], Monica Tri Yuni Sinaga[5], Rina Intan Amelia[6], Widya kartini pangaribuan[7]
[1-7]Universitas Negeri Medan,Indonesia
arnahritonga@unimed.ac.id[1*], togatoropbobby79@gmail.com[2], claralaoli2@gmail.com[3], gintingherdita@gmail.com[4], mtriyunisinaga@gmail.com[5], rinaamel118@gmail.com[6], widyakartini70@gmail.com[7]

Korespondensi Penulis: arnahritonga@unimed.ac.id[*]

Abstract*. Password security is a crucial aspect of digital authentication systems; however, many users still rely on weak and easily guessable passwords, increasing their vulnerability to cyber threats such as brute force and dictionary attacks. This study aims to evaluate password strength based on length and character complexity using a combinatorial theory approach. Through simulations, this research calculates the number of possible character combinations for various password lengths and character types, including lowercase letters, uppercase letters, numbers, and symbols. Additionally, the study estimates the time required to crack different types of passwords using brute force techniques and compares the results with real-world password breach data. The simulation results reveal that passwords composed solely of lowercase letters and fewer than eight characters in length can be cracked within seconds. In contrast, passwords that include a combination of uppercase and lowercase letters, numbers, and symbols with a minimum length of 12 characters would require more than one million years to be deciphered through brute force methods. These findings emphasize that increasing both the length and complexity of passwords significantly enhances security strength. Therefore, users are strongly encouraged to create passwords that are at least 12 characters long and include a diverse mix of character types. Furthermore, implementing Multi-Factor Authentication (MFA) and using password managers are highly recommended strategies to improve account protection. By adopting these practices, the risk of data breaches due to compromised passwords can be substantially reduced, contributing to stronger and more resilient digital security environments.*

Keywords*: Brute force attack; Combinatorial theory; Digital authentication; Password complexity; Password security*

Abstrak. Keamanan kata sandi merupakan aspek krusial dalam sistem autentikasi digital, namun banyak pengguna masih menggunakan kata sandi yang lemah dan mudah ditebak, sehingga meningkatkan kerentanan terhadap ancaman siber seperti serangan brute force dan dictionary attack. Studi ini bertujuan untuk mengevaluasi kekuatan keamanan kata sandi berdasarkan panjang dan kompleksitas karakter dengan pendekatan teori kombinatorik. Dengan menggunakan simulasi, penelitian ini menghitung jumlah kemungkinan kombinasi karakter dari berbagai panjang dan tipe karakter, termasuk huruf kecil, huruf besar, angka, dan simbol. Selain itu, estimasi waktu yang dibutuhkan untuk membobol berbagai jenis kata sandi melalui metode brute force juga dianalisis dan dibandingkan dengan data pelanggaran kata sandi di dunia nyata. Hasil simulasi menunjukkan bahwa kata sandi yang hanya terdiri dari huruf kecil dan memiliki panjang kurang dari delapan karakter dapat dibobol dalam hitungan detik. Sebaliknya, kata sandi yang terdiri dari kombinasi huruf besar, huruf kecil, angka, dan simbol dengan panjang minimal 12 karakter membutuhkan waktu lebih dari satu juta tahun untuk dipecahkan dengan brute force. Temuan ini menegaskan bahwa peningkatan panjang dan kompleksitas karakter kata sandi secara signifikan meningkatkan tingkat keamanannya. Oleh karena itu, pengguna disarankan untuk membuat kata sandi yang memiliki panjang setidaknya 12 karakter dan mencakup berbagai tipe karakter. Di samping itu, penerapan autentikasi multi-faktor (Multi-Factor Authentication) dan penggunaan pengelola kata sandi juga sangat dianjurkan untuk memperkuat perlindungan akun. Strategi ini diyakini dapat secara signifikan mengurangi risiko kebocoran data akibat kompromi kata sandi.

Kata kunci: Autentikasi digital; *Brute force attack*; Keamanan password; Kompleksitas password; Teori kombinatorik

Received: Maret 17, 2025; Revised: Maret 31, 2025; Accepted: April 12, 2025; Online Available: April 14, 2025

1. LATAR BELAKANG

Matematika berperan penting dalam berbagai aspek kehidupan, termasuk teknologi dan keamanan informasi. Kombinatorika, sebagai cabang matematika, digunakan untuk menyelesaikan masalah melalui teknik komputasi dan perhitungan sistematis. Selain dalam bidang akademik, kombinatorika juga diterapkan dalam keamanan digital, khususnya dalam menganalisis kompleksitas dan kekuatan kata sandi. Dalam keamanan digital, kombinatorika membantu menentukan jumlah kemungkinan kombinasi kata sandi berdasarkan jumlah karakter, variasi simbol, dan pola yang tersedia. Proses berpikir kombinatorik meliputi pengenalan masalah, pemahaman informasi, penyusunan solusi sistematis, serta transformasi ke bentuk kombinatorik yang lebih sederhana. Pendekatan ini dapat digunakan untuk menilai tingkat keamanan kata sandi dengan mempertimbangkan kompleksitas karakter dan tingkat kesulitannya. Perkembangan informasi teknologi tidak terlepas dari komputer, yang dapat meningkatkan proses pengerjaan setiap laporan yang diperlukan dalam sistem pengelolaan data dan keamanan. Teknologi informasi saat ini diterapkan oleh hampir seluruh organisasi untuk mencapai tujuan tertentu. Dalam konteks ini, teori kombinatorik memiliki peran penting dalam menganalisis keamanan dan kompleksitas kata sandi. Teknologi memberikan efek kombinatorial yang mempercepat kemajuan dalam berbagai aspek, termasuk dalam menentukan tingkat kekuatan kata sandi berdasarkan jumlah karakter, variasi simbol, dan kemungkinan kombinasi yang tersedia.

Kata sandi berbasis teks sering kali dianggap kurang aman karena mudah diprediksi dan dapat ditebak oleh pihak yang tidak bertanggung jawab. Hal ini memungkinkan mereka untuk meniru pengguna yang sah dan menyalahgunakan akses yang dimiliki. Banyak pengguna juga cenderung membuat kata sandi yang lemah, sering kali berdasarkan kata-kata yang terdapat dalam kamus. Untuk mengatasi masalah ini, organisasi berinisiatif untuk menetapkan kebijakan baru dalam pembuatan kata sandi. Dalam kebijakan tersebut, ditetapkan bahwa kata sandi harus memenuhi jumlah karakter minimum, harus mencakup huruf besar dan angka, serta tidak boleh terdiri dari kata-kata yang ada dalam kamus. Tujuan dari kebijakan kata sandi ini adalah untuk mengurangi kemungkinan pengguna membuat kata sandi yang mudah ditebak oleh hacker, baik melalui teknik tebakan langsung maupun serangan brute-force. Dengan menetapkan kebijakan kata sandi yang efektif, keamanan layanan informasi dapat ditingkatkan secara signifikan.(Sari, dkk 2018)

Di era digital saat ini, keamanan siber menjadi tantangan utama dalam melindungi data dan informasi pengguna. Password masih menjadi metode autentikasi yang paling umum

digunakan untuk mengamankan akun digital. Namun, banyak pengguna masih menggunakan password yang lemah dan mudah ditebak, yang meningkatkan risiko serangan siber, seperti brute force attack dan dictionary attack (Bonneau, 2012). Menurut Verizon Data Breach Investigations Report (2022), sekitar 81% insiden kebocoran data terjadi akibat penggunaan password yang tidak aman atau berhasil diretas. Fakta ini menunjukkan bahwa banyak sistem masih bergantung pada metode autentikasi yang rentan terhadap eksploitasi. Salah satu pendekatan yang dapat digunakan untuk mengukur tingkat keamanan password adalah dengan menerapkan teori kombinatorik, yang menghitung jumlah kemungkinan kombinasi karakter dalam sebuah password.

Dalam kajian Menezes, van Oorschot, dan Vanstone (1996) yang tertuang dalam Handbook of Applied Cryptography, dijelaskan bahwa semakin besar ruang kemungkinan kombinasi karakter dalam sistem autentikasi, semakin sulit bagi penyerang untuk menebak password melalui serangan brute force. Oleh karena itu, penerapan analisis kombinatorik dapat membantu dalam menentukan seberapa kuat suatu password berdasarkan panjang dan variasi karakter yang digunakannya. Seiring perkembangan teknologi, metode peretasan password juga semakin canggih. Beberapa sistem keamanan modern telah mengadopsi multi-factor authentication (MFA) dan enkripsi berbasis hash sebagai lapisan perlindungan tambahan (Stallings, 2018). Namun, password tetap menjadi komponen utama dalam sistem keamanan digital. Oleh karena itu, memahami bagaimana kombinasi karakter memengaruhi tingkat keamanan password dapat membantu pengguna dalam memilih kata sandi yang lebih aman dan tahan terhadap serangan.

Dalam era digital yang terus berkembang, keamanan kata sandi menjadi aspek fundamental dalam melindungi data sensitif dari ancaman siber yang semakin kompleks. Kata sandi merupakan lapisan pertama pertahanan dalam sistem keamanan digital, baik pada aplikasi berbasis web, desktop, maupun perangkat seluler. Penggunaan kata sandi yang lemah, seperti pola sederhana atau informasi yang mudah ditebak, sering kali menjadi penyebab utama terjadinya pelanggaran data dan akses tidak sah. Akibatnya, individu dan organisasi berpotensi menghadapi risiko kerugian finansial, kerusakan reputasi, dan eksploitasi data pribadi (Yamin et al., 2023). Di sisi lain, perkembangan teknologi memunculkan kebutuhan untuk meningkatkan keamanan kata sandi melalui pendekatan yang lebih sistematis dan berbasis sains. Salah satu pendekatan yang relevan adalah analisis kombinatorik, yang memungkinkan penghitungan jumlah kemungkinan kombinasi karakter dalam suatu kata sandi. Dengan penerapan teori kombinatorik, kelemahan dalam struktur kata sandi dapat diidentifikasi, dan rekomendasi untuk meningkatkan kekuatan kata sandi dapat diberikan. Pendekatan ini juga

bermanfaat untuk memahami tingkat kesulitan serangan terhadap kata sandi menggunakan metode brute force atau algoritma lainnya (Aditama et al., 2023). Selain itu, teknologi pengelola kata sandi semakin banyak digunakan untuk membantu pengguna mengelola kata sandi yang kompleks. Aplikasi seperti LastPass, 1Password, dan Keeper menawarkan berbagai fitur untuk meningkatkan keamanan, termasuk autentikasi multifaktor dan penyimpanan data yang terenkripsi. Namun, efektivitas aplikasi-aplikasi ini perlu dievaluasi berdasarkan standar keamanan, seperti ISO/IEC 25010, untuk memastikan bahwa mereka mampu menghadapi tantangan keamanan modern (Aditama et al., 2023).

Dalam analisis terbaru, penggunaan teknik data mining juga mulai diterapkan untuk memahami pola dalam kata sandi dan memprediksi tingkat kompleksitasnya. Dengan algoritma seperti K-Nearest Neighbor (KNN), Naïve Bayes, Decision Tree, Ensemble Methods, dan Linear Regression, penelitian dapat memberikan gambaran yang lebih mendalam tentang hubungan antara pola kata sandi dan tingkat keamanannya. Hal ini tidak hanya membantu meningkatkan kebijakan keamanan tetapi juga memberikan solusi praktis bagi pengguna dalam menciptakan kata sandi yang kuat dan mudah dikelola (Mardiani et al., 2023). Secara keseluruhan, pendekatan teoritis seperti kombinatorik, analisis standar keamanan, dan teknik data mining memberikan kontribusi penting dalam memitigasi risiko terkait kata sandi. Melalui penelitian ini, diharapkan pengembangan metode untuk meningkatkan keamanan kata sandi dapat terus dilakukan, sehingga individu maupun organisasi dapat lebih terlindungi dari ancaman siber.

2. KAJIAN TEORITIS

Penerapan Teori Kombinatorik dalam Keamanan Password

Teori kombinatorik adalah salah satu cabang matematika yang berfokus pada cara menghitung kemungkinan susunan elemen dalam suatu himpunan. Dalam dunia keamanan digital, teori ini dimanfaatkan untuk menentukan jumlah kemungkinan kombinasi karakter dalam sebuah password, yang berperan penting dalam meningkatkan ketahanan terhadap serangan siber. Menurut Menezes, van Oorschot, dan Vanstone (1996) dalam Handbook of Applied Cryptography, semakin besar jumlah kemungkinan kombinasi suatu password, semakin sulit bagi penyerang untuk menebaknya menggunakan teknik brute force. Jumlah kombinasi password dapat dihitung dengan rumus berikut:

$$C = n^k$$

Dimana:

a. C adalah jumlah kemungkinan kombinasi password
b. n adalah jumlah karakter yang tersedia
c. k adalah panjang password

Sebagai ilustrasi, jika sebuah assword hanya menggunakan huruf kecil (26 karakter) dengan panjang 6 karakter, jumlah kemungkinannya adalah:

$$C = 26^6 = 308.915.776$$

$$C = 94^8 = 6{,}09\times 10^{15}$$

Studi Kasus: Kebocoran Password dan Keamanan Sistem

Sejumlah studi telah menganalisis bagaimana lemahnya keamanan password dapat meningkatkan risiko kebocoran data. Dalam penelitian Bonneau (2012), ditemukan bahwa lebih dari 20% pengguna memilih password yang dapat ditebak dengan mudah karena menggunakan kata-kata umum. Beberapa password yang sering digunakan meliputi:

a. 123456
b. password
c. qwerty
d. abc123

Sementara itu, dalam peristiwa RockYou Data Breach (2009), sebanyak 32 juta password yang bocor dianalisis, dan ditemukan bahwa hampir 50% pengguna menggunakan password dengan panjang kurang dari 8 karakter. Hal ini menunjukkan bahwa sebagian besar pengguna masih menggunakan password yang lemah, sehingga meningkatkan kerentanan terhadap serangan siber.

Perbandingan Metode Analisis Keamanan Password

Selain pendekatan kombinatorik, ada metode lain yang digunakan dalam menilai kekuatan password, salah satunya adalah password entropy.

1. Analisis Kombinatorik

Digunakan untuk menghitung jumlah kemungkinan kombinasi password berdasarkan panjang dan karakter yang digunakan. Memungkinkan penilaian seberapa besar ruang kemungkinan kombinasi dalam sistem autentikasi.

2. Entropy Password

Mengukur tingkat ketidakpastian dalam password menggunakan rumus :

$$H = k \times log_2 (n)$$

Contoh:

a. Password “abc123” memiliki entropy rendah karena mudah ditebak.
b. Password “Tr&9sX!h2” memiliki entropy lebih tinggi karena lebih acak.

Analisis kombinatorik dan entropy saling melengkapi dalam menilai kekuatan password. Kombinatorik menunjukkan jumlah kemungkinan kombinasi, sementara entropy mengukur tingkat kerandoman password.

3 Jenis Serangan terhadap Password

Sistem keamanan berbasis password menghadapi berbagai ancaman siber. Berikut adalah beberapa metode serangan yang umum digunakan oleh peretas:

a. Brute Force Attack

Teknik ini mencoba setiap kemungkinan kombinasi karakter hingga menemukan password yang benar. Semakin kecil ruang kemungkinan kombinasi, semakin cepat password dapat ditebak.

b. Dictionary Attack

Metode ini menggunakan daftar kata-kata umum yang sering dipakai sebagai password. Misalnya, password seperti *admin*, *qwerty*, dan *iloveyou* mudah ditebak karena sering digunakan oleh banyak orang.

c. Hybrid Attack

Kombinasi antara *dictionary attack* dan *brute force attack*. Contohnya, mencoba variasi kata umum dengan tambahan angka atau simbol, seperti *password123* atau *admin2023*.

d. Credential Stuffing

Teknik ini menggunakan kombinasi username dan password yang telah bocor dari insiden keamanan sebelumnya untuk mencoba mengakses berbagai akun lain yang menggunakan kredensial serupa.

e. Implementasi Keamanan Password dalam Sistem Nyata

Beberapa perusahaan teknologi telah menerapkan kebijakan keamanan password berbasis kombinatorik untuk meningkatkan perlindungan data pengguna:

→ Google

Mengimbau pengguna untuk menggunakan password yang panjang dan acak. Menyediakan layanan *Google Password Manager* untuk membantu pengguna mengelola password mereka dengan lebih aman.

→ Microsoft

Menerapkan kebijakan password expiration, di mana pengguna harus memperbarui password mereka secara berkala untuk meningkatkan keamanan.Menggunakan sistem deteksi aktivitas mencurigakan yang memperingatkan pengguna jika ada upaya login yang tidak biasa.

→ NIST (National Institute of Standards and Technology)

Merekomendasikan panjang password minimal 12-16 karakter untuk meningkatkan keamanan. Menyarankan untuk tidak menggunakan password hints, karena dapat memperburuk keamanan akun.

4. Strategi Pembuatan Password yang Aman

Berdasarkan analisis kombinatorik dan berbagai teknik serangan terhadap password, ada beberapa strategi yang direkomendasikan untuk meningkatkan keamanan:

a.Gunakan kombinasi karakter yang beragam:

Kombinasikan huruf besar, huruf kecil, angka, dan simbol untuk memperbanyak kemungkinan kombinasi password.

b. Gunakan panjang password minimal 12 karakter:

Menurut NIST (2020), panjang password minimal yang disarankan adalah 12-16 karakter untuk perlindungan optimal.

c. Hindari penggunaan kata-kata umum

Jangan gunakan nama, tanggal lahir, atau kata-kata yang mudah ditebak.

5. Gunakan Multi-Factor Authentication (MFA)

Selain password, tambahkan lapisan keamanan ekstra seperti kode OTP atau autentikasi biometrik.

Teori kombinatorik dapat digunakan untuk mengevaluasi keamanan password dengan menghitung jumlah kemungkinan kombinasi karakter yang tersedia. Semakin panjang dan kompleks sebuah password, semakin sulit bagi peretas untuk menebaknya dengan metode brute force attack. Berbagai metode serangan terhadap password seperti brute force attack, dictionary

attack, dan credential stuffing menunjukkan pentingnya strategi pembuatan password yang lebih aman. Menggunakan variasi karakter, memperpanjang password, serta menerapkan MFA adalah langkah-langkah efektif untuk meningkatkan keamanan password. Metode kombinatorik dan entropy password dapat digunakan secara bersamaan untuk menganalisis dan meningkatkan kekuatan password dengan lebih akurat.

3. METODE PENELITIAN

Pendekatan Penelitian

Penelitian ini menerapkan metode kuantitatif dengan pendekatan analisis kombinatorik untuk mengevaluasi tingkat keamanan password berdasarkan jumlah kemungkinan kombinasi karakter yang dapat terbentuk. Pendekatan ini dipilih karena memungkinkan perhitungan matematis terhadap ketahanan password dalam menghadapi serangan brute force dan teknik peretasan lainnya.

Sumber Data

Penelitian ini menggunakan dua jenis data utama, yaitu data sekunder dan simulasi perhitungan kombinatorik

Data Sekunder

Data dari laporan keamanan siber, seperti Verizon Data Breach Investigations Report (2022) dan RockYou Data Breach (2009), yang berisi analisis mengenai kebiasaan pengguna dalam memilih password. Studi dari Bonneau (2012) yang mengevaluasi pola penggunaan password dari 70 juta data autentikasi yang dikumpulkan secara anonim. Pedoman keamanan password dari National Institute of Standards and Technology (NIST, 2020) yang merekomendasikan kebijakan terkait panjang dan kompleksitas password

Simulasi Perhitungan Kombinatorik

Simulasi dilakukan untuk menghitung jumlah kemungkinan password berdasarkan variasi panjang dan karakter yang digunakan. Proses simulasi dilakukan menggunakan bahasa pemrograman Python guna menganalisis tingkat ketahanan password terhadap serangan brute force.

Teknik Analisis Data

Analisis dalam penelitian ini dilakukan menggunakan tiga metode utama:

Perhitungan Kombinatorik

Menggunakan rumus kombinatorik untuk menghitung jumlah kemungkinan kombinasi password:

$$C = n^k$$

Simulasi dilakukan untuk membandingkan jumlah kombinasi berdasarkan berbagai skenario panjang password dan jenis karakter yang digunakan.

Estimasi Waktu Serangan Brute Force

Menghitung perkiraan waktu yang dibutuhkan untuk menebak password menggunakan teknik brute force dengan asumsi komputer dapat memproses 1 miliar tebakan per detik.

Rumus yang digunakan: $T = \frac{C}{R}$,

dimana: T adalah waktu yang dibutuhkan untuk menebak password

C adalah jumlah kemungkinan kombinasi password

R adalah kecepatan serangan (misalnya, 1 milliar tebakan per detik).

Perbandingan dengan Data Kebocoran Password

a. Melakukan analisis terhadap kumpulan password yang telah bocor dalam berbagai insiden keamanan.
b. Menilai seberapa mudah password dalam dataset tersebut dapat ditebak dibandingkan dengan password yang lebih kompleks.

Perangkat dan Alat yang Digunakan

Dalam penelitian ini, beberapa perangkat dan alat bantu digunakan untuk mendukung proses analisis, antara lain:

1. **Python**: Digunakan untuk melakukan simulasi perhitungan kombinatorik dan estimasi waktu serangan brute force.
2. **Jupyter Notebook**: Platform yang digunakan untuk menjalankan kode Python dan melakukan analisis hasil simulasi.
3. **Dataset Password**: Menggunakan kumpulan data password yang dikumpulkan dari berbagai laporan keamanan.

Tahapan Penelitian

Penelitian ini dilakukan melalui beberapa tahapan sistematis sebagai berikut:

1. Pengumpulan Data
    a. Mengumpulkan data sekunder dari laporan keamanan siber dan studi terkait password.
    b. Menentukan skenario panjang dan kompleksitas password untuk simulasi.
2. Perhitungan Kombinatorik
    a. Melakukan perhitungan jumlah kemungkinan kombinasi password berdasarkan panjang dan jenis karakter yang digunakan.
    b. Menyusun tabel hasil perhitungan sebagai dasar analisis.
3. Estimasi Waktu Serangan Brute Force
    a. Menggunakan kecepatan pemrosesan 1 miliar tebakan per detik untuk memperkirakan waktu yang dibutuhkan untuk menebak berbagai jenis password.
4. Analisis dan Interpretasi Hasil
    a. Membandingkan hasil simulasi dengan laporan kebocoran password yang telah terjadi.
    b. Menyusun rekomendasi terkait panjang dan kompleksitas password yang optimal untuk keamanan digital.

Penelitian ini menggunakan pendekatan kombinatorik untuk mengevaluasi keamanan password berdasarkan jumlah kemungkinan kombinasi karakter yang dapat terbentuk. Simulasi dilakukan dengan menggunakan Python guna memperkirakan waktu yang dibutuhkan untuk menebak password dengan teknik brute force. Analisis dilakukan dengan membandingkan hasil simulasi dengan data kebocoran password dari berbagai studi dan laporan keamanan siber. Hasil penelitian akan memberikan rekomendasi terkait panjang dan kompleksitas password yang optimal untuk meningkatkan keamanan pengguna dalam sistem autentikasi digital.

4. HASIL DAN PEMBAHASAN

Analisis Jumlah Kombinasi Password

Hasil perhitungan jumlah kemungkinan kombinasi password berdasarkan panjang dan karakter yang digunakan ditampilkan dalam tabel 4.1.

Tabel 1. Jumlah Kombinasi Password Berdasarkan Panjang Dan Jenis Karakter

Karakter Digunakan	Panjang Password	Jumlah Kombinasi $C = n^k$
Huruf kecil (26)	6	26^6 = 308.915.776
Huruf kecil (26)	8	26^8 = 208.827.064.576
Huruf kecil + huruf besar (52)	8	52^8 = 53.459.728.531.456
Huruf + angka (62)	10	$62^{10} = 8{,}391 \times 10^{17}$
Huruf + angka + simbol (94)	12	$94^{12} = 4{,}57 \times 10^{23}$

Interpretasi:

1. Semakin Panjang dan kompleks sebuah password, semakin besar jumlah kemungkinan kombinasi dapat terbentuk
2. Password yang hanya terdiri dari huruf kecil memiliki kemungkinan kombinasi yang jauh lebih kecil dibandingkan password yang menggunakan kombinasi huruf, angka, dan simbol.

Estimasi Waktu Serangan Brute Force

Untuk memahami seberapa cepat password dapat ditebak oleh serangan brute force, dilakukan simulasi dengan asumsi kecepatan serangan sebesar 1 milliar tebakan per detik. Hasil estimasi waktu yang dibutuhkan ditampilkan dalam tabel 4.2.

Tabel 2. Estimasi Waktu Serangan Brute Force

Karakter Digunakan	Panjang Password	Jumlah Kombinasi	Waktu Perkiraan (1 Milliar Tebakan/detik)
Huruf kecil (26)	6	308 juta	0,3 detik
Huruf kecil + huruf besar (52)	8	53 triliun	53 detik
Huruf + angka (62)	10	8,39 kuadriliun	266 tahun
Huruf + angka + simbol (94)	12	4,57 sekstiliun	1,45 juta tahun

Interpretasi:

a. Password pendek dengan karakter terbatas dapat ditebak dalam hitungan detik atau menit.

b. Password yang memiliki kombinasi huruf, angka, dan simbol dengan panjang lebih dari 10 karakter memiliki tingkat keamanan yang jauh lebih tinggi.

c. Password 12 karakter dengan kombinasi lengkap memerlukan lebih dari 1 juta tahun untuk ditebak oleh serangan brute force, menjadikannya sangat aman.

Perbandingan dengan Data Kebocoran Password

Untuk mengevaluasi apakah kebiasaan pengguna dalam membuat password sudah cukup aman, penelitian ini membandingkan hasil perhitungan kombinatorik dengan data dari kebocoran password yang pernah terjadi. Berdasarkan penelitian Bonneau (2012) dan laporan RockYou Data Breach (2009), ditemukan bahwa sebagian besar pengguna masih menggunakan password dengan pola yang mudah ditebak. Contoh password yang paling sering digunakan:

1. 123456
2. password
3. qwerty
4. abc123
5. iloveyou

Temuan:

Password yang sering digunakan dalam data kebocoran memiliki panjang kurang dari 8 karakter dan hanya terdiri dari huruf kecil atau angka, yang membuatnya sangat mudah ditebak.Sebagian besar password dalam dataset kebocoran dapat ditebak dalam waktu kurang dari 1 detik menggunakan serangan brute force. Pengguna masih cenderung memilih password berdasarkan kemudahan mengingat, bukan berdasarkan keamanan.

Rekomendasi Keamanan Password

Berdasarkan hasil penelitian ini, berikut beberapa rekomendasi untuk meningkatkan keamanan password:

1. Gunakan password dengan minimal 12 karakter: Panjang password yang lebih pendek dari ini dapat ditebak dalam waktu yang relatif singkat.
2. Gunakan kombinasi karakter yang beragam: Gunakan huruf besar, huruf kecil, angka, dan simbol untuk meningkatkan jumlah kemungkinan kombinasi.
3. Hindari penggunaan kata-kata umum atau pola berulang: Hindari password yang mudah ditebak seperti 123456, password, atau qwerty.
4. Gunakan password manager: Alat ini dapat membantu menyimpan password yang panjang dan unik untuk setiap akun.

5. Gunakan Multi-Factor Authentication (MFA): Menambahkan lapisan keamanan tambahan seperti OTP atau autentikasi biometrik dapat melindungi akun dari akses tidak sah.

Semakin panjang dan kompleks password, semakin besar jumlah kemungkinan kombinasi, sehingga semakin sulit untuk ditebak oleh serangan brute force. Password yang hanya menggunakan huruf kecil atau angka dapat ditebak dalam waktu yang sangat singkat, bahkan kurang dari 1 detik. Password dengan panjang minimal 12 karakter dan kombinasi huruf, angka, serta simbol memiliki tingkat keamanan yang jauh lebih baik karena membutuhkan waktu lebih dari 1 juta tahun untuk ditebak. Banyak pengguna masih memilih password yang lemah, seperti yang terlihat dari dataset kebocoran password, sehingga meningkatkan risiko keamanan. Pengguna disarankan untuk menggunakan password yang lebih kuat, menerapkan password manager, dan mengaktifkan multi-factor authentication untuk perlindungan yang lebih baik.

KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa teori kombinatorik dapat digunakan untuk menganalisis tingkat keamanan password dengan menghitung jumlah kemungkinan kombinasi karakter yang tersedia. Semakin panjang dan kompleks sebuah password, semakin besar jumlah kombinasi yang dapat terbentuk, sehingga meningkatkan ketahanannya terhadap serangan siber, terutama brute force attack. Hasil analisis menunjukkan bahwa password yang hanya terdiri dari huruf kecil memiliki jumlah kemungkinan kombinasi yang lebih sedikit dibandingkan dengan password yang menggunakan kombinasi huruf besar, huruf kecil, angka, dan simbol. Oleh karena itu, password dengan variasi karakter yang lebih banyak akan lebih sulit untuk ditebak oleh sistem peretasan otomatis. Selain itu, penelitian ini juga mengungkapkan bahwa panjang password memiliki peran penting dalam menentukan tingkat keamanannya. Simulasi perhitungan menunjukkan bahwa password dengan panjang kurang dari 8 karakter dapat ditebak dalam hitungan detik, terutama jika hanya menggunakan kombinasi karakter yang terbatas. Sebaliknya, password dengan panjang 12 karakter atau lebih, yang terdiri dari kombinasi lengkap antara huruf besar, huruf kecil, angka, dan simbol, dapat bertahan dari serangan brute force hingga lebih dari satu juta tahun, sehingga menjadikannya jauh lebih aman. Fakta ini menegaskan bahwa pemilihan password yang kuat sangat diperlukan untuk melindungi akun pengguna dari ancaman peretasan.

Berdasarkan hasil analisis ini, terdapat beberapa rekomendasi yang dapat diterapkan dalam pembuatan password yang lebih aman. Pengguna disarankan untuk menggunakan password dengan panjang minimal 12 karakter, serta memastikan adanya kombinasi berbagai jenis karakter untuk meningkatkan kompleksitasnya. Selain itu, penggunaan password yang mudah ditebak, seperti nama, tanggal lahir, atau kata-kata umum, harus dihindari karena lebih rentan terhadap serangan. Penggunaan password manager juga dapat menjadi solusi untuk menyimpan dan mengelola password yang kompleks agar tetap aman dan mudah diakses. Selain itu, penerapan Multi-Factor Authentication (MFA) sangat dianjurkan sebagai langkah perlindungan tambahan dalam sistem keamanan digital. Dengan menerapkan praktik ini, risiko kebocoran data akibat peretasan password dapat dikurangi secara signifikan.

Saran

Untuk meningkatkan kesadaran dan perlindungan terhadap keamanan password, terdapat beberapa saran yang dapat diterapkan oleh berbagai pihak. Bagi pengguna internet, disarankan untuk selalu menggunakan password yang panjang, kompleks, dan unik untuk setiap akun yang dimiliki. Selain itu, pengguna harus mengaktifkan autentikasi dua faktor (2FA/MFA) guna memberikan lapisan keamanan tambahan dalam proses login. Penggunaan password yang sama di beberapa akun juga perlu dihindari, karena hal ini dapat meningkatkan risiko peretasan apabila salah satu akun mengalami kebocoran data.

Bagi pengembang sistem keamanan, perlu diterapkan kebijakan yang mewajibkan pengguna untuk membuat password dengan panjang minimal 12 hingga 16 karakter, serta mendorong penggunaan kombinasi karakter yang lebih kuat. Selain itu, penyimpanan password dalam database harus dilakukan dengan metode enkripsi dan hashing yang aman untuk mencegah pencurian data akibat kebocoran sistem. Pengembang juga dianjurkan untuk menerapkan sistem rate-limiting yang membatasi jumlah percobaan login dalam waktu tertentu, sehingga dapat mengurangi efektivitas serangan brute force.

Sementara itu, bagi peneliti di bidang keamanan siber, studi lebih lanjut dapat dilakukan untuk mengeksplorasi efektivitas metode kombinatorik dalam menghadapi serangan yang lebih canggih, seperti rainbow table attack atau serangan berbasis kecerdasan buatan. Penelitian lanjutan juga dapat mengkaji bagaimana kombinasi teori kombinatorik dan entropy password dapat digunakan secara bersamaan untuk menciptakan model evaluasi keamanan password yang lebih akurat dan komprehensif. Dengan semakin berkembangnya teknologi dan metode

peretasan, diperlukan inovasi dalam strategi perlindungan password agar keamanan data tetap terjaga

DAFTAR REFERENSI

Aditama, W. Y., Hikmah, I. R., & Priambodo, D. F. (2023). Analisis komparatif keamanan aplikasi pengelola kata sandi berbayar berdasarkan ISO/IEC 25010. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 10, 857–864.

Afifah, R. N., Hidayat, R., Setiyadi, E. B., & Ihsanuddin, I. (2023). Proses berpikir kombinatorik siswa dalam menyelesaikan soal matematika ditinjau dari self efficacy. Jurnal Prodi Pendidikan Matematika (JPPM), 5(2), 699–711.

Bonneau, J. (2012). Ilmu menebak: Analisis terhadap 70 juta password yang dianonimkan. IEEE Symposium on Security & Privacy, 538–552.

Institut Nasional Standar dan Teknologi (NIST). (2020). Panduan identitas digital: Manajemen autentikasi dan siklus hidup. Departemen Perdagangan Amerika Serikat.

Laitinen, A., & Eronen, J. (2020). Serangan brute force dan keamanan password: Analisis empiris. Jurnal Penelitian Keamanan Siber, 8(2), 112–125.

Mahayasa, I. M. P., Nugraha, I. N. B. S., & Ambaradewi, N. L. G. (2024). Implementasi System Loyalti Manajemen (Renata) menggunakan framework Laravel 9 studi kasus Agung Toyota Kuta. Jurnal Manajemen dan Teknologi Informasi, 14(2), 35–42.

Mardiani, E., Rahmansyah, N., Wijaya, Y. F., et al. (2023). Analisis kompleksitas password dengan metode KNN, Naïve Bayes, Decision Tree, Ensemble Methods dan Linear Regression. Digital Transformation Technology (Digitech), 3, 955–963.

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Panduan kriptografi terapan. CRC Press.

Muhammad Akfal, T. (2024). Matematika olimpiade materi kombinatorika pada siswa tingkat SMP. Jurnal Pengabdian Kepada Masyarakat, 2(2), 186–190.

RockYou Data Breach. (2009). Analisis terhadap 32 juta password yang bocor. Laporan Penelitian Keamanan Siber.

Sari, Y. A. L., Kusyanti, A., & Rokhmawati, R. I. (2018). Analisis faktor-faktor yang memengaruhi perilaku pengguna sistem informasi akademik mahasiswa dalam penciptaan kata sandi kuat dengan menggunakan Protection Motivation Theory (Studi pada XYZ). Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2(4), 1348–1357.

Stallings, W. (2018). Kriptografi dan keamanan jaringan: Prinsip dan praktik (Edisi ke-7). Pearson.

Verizon. (2022). Laporan investigasi kebocoran data. Verizon Enterprise Solutions.

Wang, D., Wang, P., & Wang, C. (2016). Memahami keamanan password dalam skenario percobaan terbatas. Keamanan & Komputer, 63, 168–182.

Yamin, M., Malethi, T. T., Ishyavanka, M., Jodhika, S., & Natali, S. (2023). Evaluasi risiko pada penggunaan password yang lemah: Analisis kasus penggunaan password umum. Jurnal Ilmiah Multidisiplin Ilmu Komputer, 1, 41–48.