Jurnal Ilmiah Multidisiplin Ilmu Komputer

Vol.1, No. 1 Agustus 2023, Hal.41-48

EVALUASI RISIKO PADA PENGGUNAAN PASSWORD YANG LEMAH: ANALISIS KASUS PENGGUNAAN PASSWORD UMUM

M.Yamin*[1], Thresia Tifani Malethi[2], Monica[3], Jodhika[4], Silvina Natali[5]
[1,2,3,4,5]Program Studi Teknik Informatika,
STMIK Pelita Nusantara Medan, Jl. Iskandar Muda No.1
E-mail: *[1]muhammadyamin1081@gmail.com, [2]thresiatifani@gmail.com,
[3]ishyavanka18@gmail.com, [4]jodhika26@gmail.com, [5]silvinaanatali@gmail.com

ABSTRAK

Banyak orang cenderung berpikir bahwa serangan siber tidak akan terjadi pada dirinya. Namun, perlu ingat bahwa ketika pelanggaran data dan ancaman siber lainnya terjadi, ada kerugian finansial dan konsekuensi parah lainnya yang bisa dialami. Selama masih menggunakan internet, kita akan selalu menjadi target potensial. Apa yang harus dilakukan? Jangan menganggap password yang kita gunakan aman. Terus evaluasi ulang keamanan kata sandi. Password adalah informasi penting untuk mengakses atau memasuki sebuah sistem. Alfanumerik adalah sistem kata sandi berbasis teks yang umum digunakan. Sayangnya, banyak pengguna membuat kata sandi yang lemah sehingga mudah ditebak dan rentan terhadap berbagai serangan. Untuk membuat kata sandi yang kuat disarankan memiliki banyak variasi dan panjang, tetapi akan sulit diingat oleh pengguna. Kata sandi terbaik tidak selalu rumit, tetapi sulit ditebak. Kata sandi yang memberikan perlindungan tinggi bersifat pribadi bagi Anda dan tidak berisi informasi yang mudah diperoleh, seperti nama dan tanggal lahir.

Kata Kunci: *Keamanan Komputer, Kejahatan Siber, Kata Sandi, Internet*

ABSTRACT

Many people tend to think that cyberattacks won't happen to them. However, keep in mind that when data breaches and other cyberthreats occur, there can be financial loss and other severe consequences. As long as we are still using the internet, we will always be a potential target. What to do? Do not assume the password that we use is safe. Constantly re-evaluate password security. Password is important information to access or enter a system. Alphanumeric is a commonly used text-based password system. Unfortunately, many users create weak passwords that are easy to guess and vulnerable to various attacks. To create a strong password, it is advisable to have many variations and lengths, but which will be difficult for the user to remember. The best passwords aren't always complicated, but hard to guess. Passwords that provide high protection are personal to you and do not contain easily obtainable information, such as your name and date of birth.

Keywords: Computer Security, Cybercrime, Passwords, Internet

Jurnal Ilmiah Multidisiplin Ilmu Komputer

Vol.1, No. 1 Agustus 2023, Hal.41-48

1. PENDAHULUAN

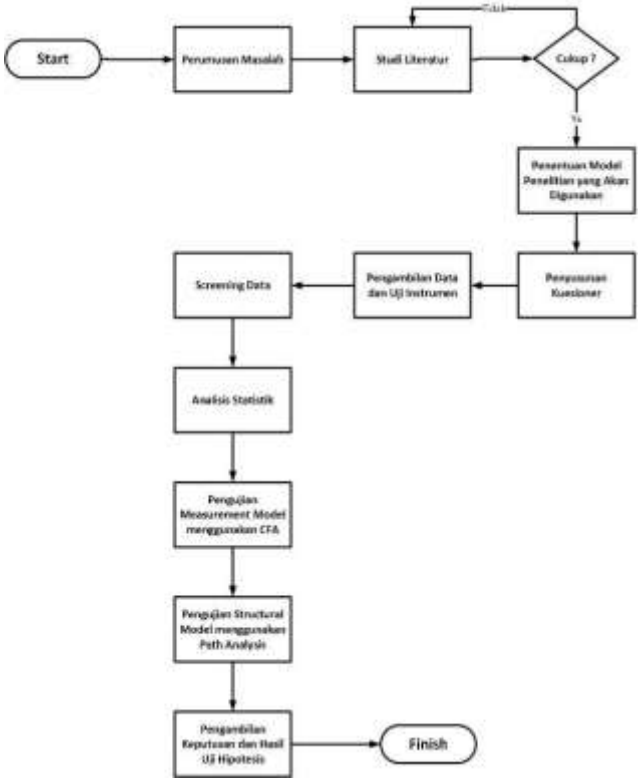
Evaluasi risiko pada penggunaan password yang lemah menjadi isu yang semakin penting dalam era digital ini. Password yang lemah seringkali menjadi pintu masuk bagi para penjahat cyber untuk mengakses data pribadi atau meretas akun online seseorang. Kasus penggunaan password umum secara luas menunjukkan betapa rentannya keamanan data ketika pengguna tidak memperhatikan pentingnya mengamankan akun mereka dengan password yang kuat. Oleh karena itu, evaluasi risiko pada penggunaan password yang lemah menjadi perhatian utama dalam upaya meningkatkan keamanan online.

Evaluasi risiko pada penggunaan password yang lemah dapat membantu dalam menyadarkan pengguna akan pentingnya praktik keamanan yang baik. Dengan menilai risiko yang terkait dengan password yang lemah, organisasi atau individu dapat memahami dampak potensial dari pelanggaran keamanan dan kehilangan data sensitif. Evaluasi ini juga dapat mengungkapkan kelemahan dalam kebijakan keamanan yang ada dan memberikan pemahaman yang lebih baik tentang tindakan yang perlu diambil untuk meningkatkan keamanan.

Dengan demikian, evaluasi risiko pada penggunaan password yang lemah menjadi kunci dalam menghadapi ancaman keamanan cyber saat ini. Dalam upaya untuk melindungi data pribadi dan memperkuat keamanan online, penting bagi individu dan organisasi untuk memahami risiko yang terkait dengan password yang lemah dan mengambil tindakan pencegahan yang tepat.

2. METODE PENELITIAN

Metode penelitian yang digunakan dalam evaluasi kali ini merujuk pada model waterfall sebagai berikut.



Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Pengertian Password

Password adalah serangkaian karakter yang digunakan untuk mengautentikasi pengguna pada sistem komputer. Contoh sederhananya, ketika kita memiliki akun di komputer, untuk bisa mengaksesnya, perlu memasukkan password yang valid. Password sering juga disebut dengan kata sandi, namun apakah kata sandi memiliki arti yang sama dengan password? Sebagai informasi, kata sandi adalah kode rahasia yang dimasukkan oleh pengguna untuk mendapatkan akses ke sistem, aplikasi, file data, atau server jaringan. Melihat dari penjelasan di atas, dapat disimpulkan bahwa password dan kata sandi merupakan dua hal yang sama dan bermanfaat untuk melindungi data pribadi, file, sistem, jaringan, dan lain sebagainya.

3.2. Fungsi Password

Salah satu fungsi password adalah untuk meningkatkan keamanan dari file, aplikasi, serta jaringan yang ingin dilindungi dari pihak luar. Menurut laman Thycotic, 80% dari semua serangan keamanan cyber disebabkan karena kata sandi yang lemah dan mudah untuk diserang

3.3. Metode Peretasan Password

Menurut Rita Komalasari (dalam Jurnal Teknologi Informasi dan Komunikasi, 2018: 143-148), ada beberapa metode yang digunakan seorang hacker untuk meretas password, antara lain :

a. Social engineering

Metode teknologi rendah yang paling populer untuk mengumpulkan password adalah social engineering.

Social engineering mengambil keuntungan dari sifat mempercayai manusia untuk mendapatkan informasi yang kemudian dapat digunakan untuk kejahatan. Teknik Social engineering yang umum menipu seseorang untuk membocorkan password. Hal ini terjadi sepanjang waktu, sehingga sampai saat ini metode ini masih digunakan.

Untuk mendapatkan password melalui social engineering, hacker hanya memintanya. Misalnya, hacker menelepon pengguna dan mengatakan kepadanya bahwa pengguna memiliki beberapa e-mail yang tampak penting yang terjebak dalam antrian mail, dan hacker perlu password untuk login dan membebaskan email tersebut. Hal ini sering dilakukan hacker mencoba untuk mendapatkan informasi.

Kelemahan umum yang dapat memfasilitasi metode tersebut adalah ketika nama anggota staf, nomor telepon, dan alamat e-mail diposting di situs web perusahaan. Situs media sosial seperti LinkedIn, Facebook, dan Twitter juga dapat digunakan perusahaan karena situs ini dapat mengungkapkan nama karyawan dan informasi kontak

b. Shoulder surfing

Shoulder surfing (tindakan melihat dari bahu seseorang untuk melihat apa yang orang tersebut ketik) adalah metode hack berteknologi rendah yang efektif. Untuk melaksanakan serangan ini, seseorang harus dekat korban dan berusaha untuk tidak terlihat jelas, lalu mendapatkan password dengan melihat baik keyboard atau layar pengguna ketika seseorang log in.

Vol.1, No. 1 Agustus 2023, Hal.41-48

Gambar 2. Shoulder Surfing

Seorang penyerang bahkan bisa melihat apakah pengguna melirik ke meja untuk melihat salah satu pengingat password atau password itu sendiri. Kamera keamanan atau webcam bahkan dapat digunakan untuk melakukan serangan tersebut. Kedai kopi dan pesawat terbang menyediakan skenario ideal untuk shoulder surfing. Shoulder surfing dapat dengan mudah dipraktekkkan sendiri. Cukup berjalan di kantor dan melakukan Random spot Checks. Buka meja pengguna dan minta untuk masuk ke komputer, jaringan, atau bahkan aplikasi e-mail.

c. Inferensi

Pengguna terkadang memberikan password untuk hal yang disukai, maka kemungkinannya adalah bahwa mungkin ada password diacak berdasarkan minat, hobi, hewan peliharaan, keluarga dan sebagainya. Pada kenyataannya password didasarkan pada hal yang seseorang sering perbincangkan di jaringan sosial dan bahkan disertakan dalam profil, sehingga penyerang dapat melihat dengan seksama informasi ini untuk menebak password daripada menggunakan serangan dictionary atau serangan Brute Force.

Program yang dapat menebak password secara otomatis dan cracker menggunakan beberapa pendekatan yang berbeda. Serangan penebakan password hibrid menganggap bahwa administrator jaringan meminta pengguna untuk membuat password yang setidaknya sedikit berbeda dari kata yang muncul dalam kamus. Aturan penebakan password hibrid bervariasi dari alat ke alat, tetapi sebagian besar merupakan campuran huruf besar dan huruf kecil, terdapat tambahan nomor di akhir sandi, pengejaan password secara mundur atau sedikit kesalahan eja dan termasuk karakter seperti @! #.

d. Otentikasi lemah

Penyerang dapat memperoleh atau menghindari keharusan menggunakan password dengan memanfaatkan sistem operasi yang lebih tua atau tidak aman, yang tidak memerlukan password untuk masuk. Hal yang sama berlaku untuk ponsel atau tablet yang tidak dikonfigurasi untuk menggunakan password. Pada sistem operasi lama yang meminta password, pengguna dapat menekan ESC pada papan ketik untuk langsung masuk. Setelah masuk, pengguna dapat menemukan password lain yang disimpan di tempat tersebut sebagai dial-up, sambungan VPN dan screen saver. Password tersebut

dapat diretas dengan mudah menggunakan alat Elcomsoft's proaktif sistem Password Recovery dan Cain & Abel.

e. Key Logger / Malware

Seorang hacker atau penyerang menggunakan program untuk melacak semua keystroke pengguna sehingga pada akhir hari segala sesuatu yang pengguna ketik termasuk id login dan password telah direkam. Sebuah serangan key logger berbeda dari serangan brute force atau dictionary. Sebuah key logger atau program scraper layar yang merupakan virus malware atau program full blown virus yang dapat diinstal oleh malware yang mencatat semua yang diketik pengguna di layarnya.

Program ini dapat diinstal langsung oleh hacker atau membuat trik untuk proses instal program ini oleh pengguna melalui email dengan mengklik atau men-download link maka program ini harus terlebih dahulu dibuat pada perangkat pengguna. Beberapa virus program akan mencari keberadaan web browser file password klien dan menyalin password yang disimpan dari sejarah browsing pengguna, kecuali telah terenkripsi, akan mudah diakses.

Meskipun password yang lebih kuat tidak memberikan jaminan keamanan yang lebih besar terhadap serangan key logger, maka saat ini banyak organisasi bisnis sudah mulai harus memiliki otentikasi multifaktor (MFA). Dengan otentikasi multi faktor atau otentikasi 2 faktor & Advance, otentikasi pengguna diperlukan untuk memberikan tidak hanya password tetapi juga faktor keamanan lain seperti kode unik yang dihasilkan dari aplikasi mobile yang aman pada ponsel pintar atau perangkat token, sehingga bahkan jika seorang hacker mampu mencapai sistem, tidak akan dapat mengakses password keamanan kedua karena jaringan dilindungi oleh MFA karena jaringan ini hampir tak tertembus untuk serangan luar.

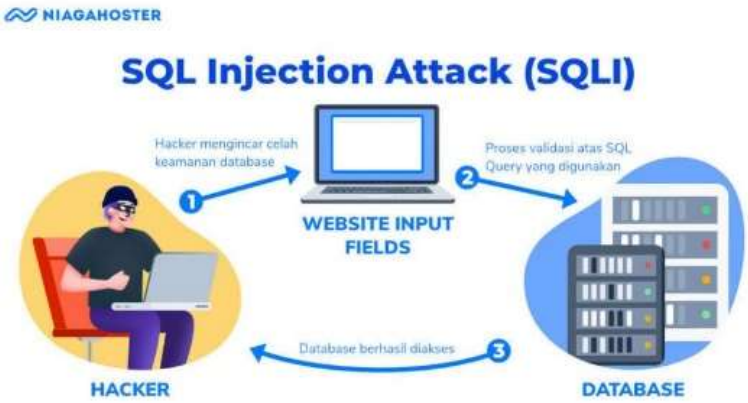
f. Phising

Phising adalah cara mudah untuk memperoleh password pengguna. Jika pengguna akan memberikan password dengan cara yang mudah maka tidak diperlukan cara meretas yang lebih keras yang perlu untuk memecahkan password. Hal ini berlaku dengan adanya serangan phishing ini. Dalam serangan ini penyerang mengirim email palsu yang mengaku berasal dari organisasi yang sah. Hal ini biasanya dikombinasikan dengan ancaman atau permintaan informasi seperti akun akan ditutup, saldo jatuh tempo, informasi akan hilang dari akun pengguna. Email akan meminta pengguna memberikan informasi rahasia seperti rincian rekening bank, nomor rekening, PIN ATM, nomor VPN, password. Rincian ini kemudian digunakan oleh pemilik situs web untuk melakukan penipuan. Oleh karena itu pengguna dengan mudah memberikan sendiri informasi rahasia kepada hacker.

Gambar 3. Kode OTP Palsu Melalui Email

g. Serangan SQL Injection

Situs web yang dirancang dengan buruk merupakan korban yang rentan dari jenis serangan ini. Dalam serangan ini penyerang dapat menyuntikkan perintah SQL dan mendapatkan akses untuk mendapatkan data dari database. Ini adalah teknik kode injeksi yang digunakan untuk menyerang website dan login dengan hak administrator.



Gambar 4. SQL Injection Attack

h. Penyetelan ulang password

Penyerang sering merasa lebih mudah untuk mereset password daripada harus menebaknya. Banyak program untuk meretas password sebenarnya adalah password resetters. Dalam kebanyakan kasus, penyerang melakukan boot dari flashdrive atau CD-ROM untuk mendapatkan mengelabui perlindungan Windows.

i. Serangan Brute Force

Dalam jenis serangan ini, semua kemungkinan kombinasi password berlaku untuk memecahkan sandi. (Fujita, 2008). Metode menyerang yang paling dapat diandalkan penyerang atau hacker dan memakan waktu lama adalah serangan Brute Force. Penyerang dapat mencoba dengan setiap kemungkinan kombinasi karakter, angka, karakter khusus seperti mulai dari abcd11..... ABCD999..... zzzz123. ZZZZ10 dan sebagainya. Seorang hacker dapat menggunakan program komputer atau kode program untuk menebak kombinasi karakter yang paling mungkin untuk menebak password.

Untuk menebak password, hacker dapat memulainya dari password yang termudah terlebih dahulu. Serangan brute force bekerja dengan menghitung setiap kemungkinan kombinasi yang bisa membuat password dan pengujian untuk melihat apakah itu adalah password yang benar. Seiring dengan bertambahnya panjang password, jumlah waktu, rerata, untuk menemukan kata sandi yang benar akan meningkat secara eksponensial. Ini berarti password pendek biasanya dapat ditemukan cukup cepat, tapi password yang lebih panjang mungkin dapat ditebak dalam rentang waktu yang lebih lama bahkan sampai dengan beberapa dekade.

3.4. Pencegahan Peretasan Password

Beberapa hal yang dapat dilakukan untuk mencegah terjadinya peretasan password adalah sebagai berikut:

1. Buat kata sandi yang kompleks.

   Kata sandi yang digunakan untuk mengakses akun pada aplikasi atau situs web harus memuat kombinasi angka, huruf besar dan kecil, dan karakter spesial yang sulit ditebak. Jangan gunakan entri kata sandi yang sama untuk situs web atau akun lain. Langkah ini bertujuan mengurangi risiko jika sewaktu-waktu seseorang berhasil meretas salah satu kata sandi.
2. Gunakan program pengelola kata sandi (password manager).

   Program ini menyimpan entri-entri kata sandi dan mengisi formulir informasi pribadi pada beragam situs secara otomatis. Dengan demikian, kita bisa membuat kata sandi yang kompleks dan unik untuk setiap situs, tanpa harus memasukkan sendiri kata sandi tersebut secara berulang. Kita memang harus tetap mengingat entri-entri kata sandi yang dibuat. Namun, program pengelola kata sandi membuat meningkatkan keamanan perangkat yang digunakan.

   Beberapa program pengelola kata sandi pihak ketiga yang sangat bereputasi mencakup "Dashlane 4", "LastPass 4.0 Premium", "1Password", "Sticky Password Premium", dan "LogMeOnce Ultimate". Sebagian besar peramban memiliki fitur pengelola kata sandi bawaan yang menyimpan entri-entri kata sandi (meskipun biasanya fitur ini tidak mengenkripsi entri-entri tersimpan).
3. Jangan sebarkan kata sandi

   Meskipun sudah jelas, langkah ini perlu diingat dengan baik. Jangan pernah memberikan kata sandi kepada administrator situs agar ia bisa mengakses akun, kecuali untuk beberapa layanan sekolah. Selain itu, jangan sebarkan kombinasi PIN atau koda sendi ponsel dan tablet kepada orang lain. Teman kita bisa saja tidak sengaja membocorkan kode sendi Anda kepada orang lain
4. Ganti kata sandi secara berkala

   Jangan gunakan kata sandi yang sama dua kali (mis. kata sandi akun Facebook harus berbeda dari kata sandi akun rekening bank, dan lain-lain) dan Saat mengganti kata sandi, lakukan perubahan secara menyeluruh. Jangan sekadar mengganti satu huruf dengan angka.
5. Aktifkan autentikasi dua faktor

   Sistem autentikasi ini mengharuskan kita untuk memasukkan kode yang dikirimkan melalui pesan singkat atau layanan lain agar akun dapat diakses setelah Anda memasukkan nama pengguna dan kata sandi. Meskipun peretas berhasil mengetahui kata sandi, sistem autentikasi ini menyulitkannya untuk mengakses informasi akun.

4. KESIMPULAN

Kesimpulan yang dapat diambil adalah penelitian ini memberikan manfaat bagi masyarakat mengenai tentang bagaimana seorang hacker dapat dengan mudah memprediksi dan mungkin meretas password. Studi ini memungkinkan pengguna untuk menjadi lebih waspada pada saat menggunakan web online dan layanan cloud yang melakukan berdasarkan password dan username. Dengan mempelajari dan menganalisis hal ini, penulis percaya bahwa analisis mendalam akan memberikan informasi yang cukup untuk penggunaan username dan password dan dengan demikian merubah perilaku individu dalam penggunaan sistem berbasis password baik online maupun offline.

Saran yang dapat kami sampaikan adalah untuk orang-orang yang mempunyai password dalam jumlah yang banyak, lebih baik memakai password manajemen daripada di tulis di suatu

tempat. Pemilihan password sebaiknya yang mudah di ingat tetapi mempunyai suatu algoritma tertentu atau sesuatu yang terinspirasi menurut kita.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada STMIK Pelita Nusantara Medan dan Dosen Pengampu Mata Kuliah Keamanan Komputer yang telah memberi dukungan terhadap penelitian ini.

DAFTAR PUSTAKA

[1] Komalasari, R. (2018). Kesadaran Akan Keamanan Penggunaan Username Dan Password. Tematik: Jurnal Teknologi Informasi Komunikasi (e-Journal), 5(2), 141-152.

[2] Sari, Y. A. L., Kusyanti, A., & Rokhmawati, R. I. (2017). 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 e-ISSN, 2548, 964X.

[3] Santoso, K. I. (2013). Dua Faktor Pengamanan Login Web Menggunakan Otentikasi One Time Password Dengan Hash SHA. Semantik, 3(1).

[4] Ustadztama, M. G. (2017). METODE CHECKSUM SEBAGAI LANGKAH MEYAKINI DOKUMEN ELEKTRONIK DALAM PEMERIKSAAN PAJAK. In *Forum Ilmiah Keuangan Negara* (Vol. 3, No. 1, pp. 14-14).

[5] DM, M. Y., Addermi, A., & Lim, J. (2022). Kejahatan Phising dalam Dunia Cyber Crime dan Sistem Hukum di Indonesia. Jurnal Pendidikan dan Konseling (JPDK), 4(5), 8018-8023.

[6] Santoso, S., 2015. AMOS 22 untuk Structural Equation Modeling Konsep Dasar dan Aplikasi. Elex Media Komputindo. Jakarta

[7] Tsai, S.H. et al. 2016. Understanding online safety behaviors: A protection motivation theory perspective.