KESADARAN AKAN KEAMANAN PENGGUNAAN USERNAME DAN PASSWORD

Rita Komalasari
Politeknik LP3I Bandung
Email: ritakomalasari@plb.ac.id

Abstrak : Mekanisme kontrol yang paling umum untuk mengotentikasi pengguna sistem informasi terkomputerisasi adalah penggunaan password. Tulisan ini membahas kesenjangan dalam mengevaluasi karakteristik dari password yang digunakan kehidupan dalam nyata dan menyajikan hasil studi empiris pada penggunaan password dan resiko serangan dari hacker menggunakan berbagai metode (key logger, phising, shoulder surfing, dictionary, rainbow table). 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.
.

Kata Kunci : Password, keamanan, manajemen informasi

1. Pendahuluan

Penggunaan username dan password sudah menjadi kebutuhan sehari-hari yang dipergunakan seseorang untuk dapat login ke suatu situs. Otentikasi adalah proses atau protokol yang memperbolehkan suatu entitas untuk memastikan identitas entitas lainnya (Jadhao & Dole, 2013). Organisasi yang berbeda memiliki persyaratan otentikasi yang berbeda dan sehingga mereka menetapkan otentikasi yang berbeda sesuai dengan jenis kebutuhan mereka. Tujuan utama dari otentikasi adalah untuk mengamankan data /sistem dari pihak ketiga. Proses otentikasi digunakan pula dalam instansi militer dan pemerintah, rumah sakit dan pengaturan bisnis lainnya (Jansen, 2015).

Peningkatan serangan cyber dan pelanggaran data akhir-akhir ini menjadikan pemahaman keamanan online juga semakin meningkat. Salah satu informasi yang paling rentan untuk pengguna online adalah penggunaan password. Kesalahan paling umum yang dilakukan seseorang adalah memilih kata sandi yang lemah dan umum. Penulisan password yang paling mudah ditebak adalah '123456', 'password' dan '12345678'. Pembatasan penggunaan password yang berisi konteks informasi spesifik pengguna merupakan satu tantangan tersendiri, misalnya penyertaan nama pengguna, nama situs web, nama organisasi terkait, atau terminologi terkait lainnya kurang aman saat mengotentikasi pengguna di sistem terkait.

Secara teoritis, password apapun dapat diretas menggunakan serangan password, tidak peduli bagaimanapun kompleksitas dari password tersebut. Password kompleks yang setidaknya terdiri dari 8 karakter akan memerlukan bertahun-tahun untuk untuk diretas bahkan dengan perangkat keras modern umumnya. Akan tetapi ketika seseorang memilih password yang kompleks, seringkali membuat kesalahan lain yaitu dengan menggunakan password yang sama di situs yang berbeda. Misalnya jika menggunakan email dan kata

sandi yang sama untuk Gmail, Facebook, Twitter, dan beberapa akun lainnya dan ada pelanggaran data pada Gmail dan sandi terungkap, secara efektif berarti semua akun akan mudah disusupi.
Password alfanumerik, adalah skema otentikasi yang paling umum digunakan (Grawemeyer & Johnson, 2011). Password alfanumerik harus panjang dan kompleks, harus terdiri dari kata umum, nomor dan simbol (Choong & Greene, 2016). Ketika dipaksa untuk menggunakan password alfanumerik asing untuk meningkatkan keamanan, pengguna 18 kali lebih mungkin untuk menuliskannya (Grawemeyer & Johnson, 2011). Sepertiga pengguna melaporkan mereka berbagi kata sandi email dengan orang lain (Kaye, 2011) dan password biasanya digunakan kembali untuk 1,7 untuk 3,4 website (Wash, 2016).

2. Pencegahan *hacking* dengan penanggulangan *password-cracking*

Beberapa penanggulangan umum dapat mencegah hacking password, selalu disarankan untuk menggunakan password yang kuat dan password yang unik untuk situs yang berbeda. Jika sulit diingat, dapat mencoba alat pengelola kata sandi yang baik. Pilih password unik yang kuat menggunakan kombinasi huruf kecil, huruf besar, angka, dan karakter khusus yang panjangnya minimal 8 karakter meskipun situs web memungkinkan untuk password yang lebih sederhana. Satu-satunya kelemahannya adalah bahwa pengguna harus menyimpan beberapa password dan, karena itu, mungkin salah satu cara mengingatnya adalah dengan menuliskannya.

2.1 Penyimpanan password

Jika harus memilih antara penggunaan password yang lemah dimana pengguna dapat mengingatnya dan password yang kuat dimana pengguna harus menuliskan, maka pengguna harus menuliskan dan menyimpan informasi password dengan aman. Pengguna diminta untuk menyimpan kata sandi tertulis di tempat yang aman — bukan pada keyboard atau file komputer yang dilindungi oleh kata sandi yang mudah diretas.

Pengguna harus menyimpan kata sandi tertulis di salah satu lokasi berikut:

a. Sebuah lemari file terkunci atau brankas kantor yang aman
b. Disk enkripsi utuh yang dapat mencegah penyusup untuk mengakses OS dan password yang tersimpan pada sistem.
c. Alat manajemen kata sandi yang aman seperti :
   - LastPass
   - Password Safe, sebuah perangkat lunak open source yang awalnya dikembangkan oleh Counterpane.

2.2 Kebijakan password

Untuk menunjukkan pentingnya mengamankan password. Berikut adalah beberapa cara untuk melakukannya :

a. Mendemonstrasikan cara membuat kata sandi yang aman. Beri rujukan pengguna untuk membuat kalimat sebagai passwors karena sebagian besar pengguna cenderung membuat password yang hanya berupa “kata” secara harfiah, yang bisa menjadikan password menjadi kurang aman.
b. Tunjukkan apa yang bisa terjadi ketika password lemah digunakan atau password dibagikan.

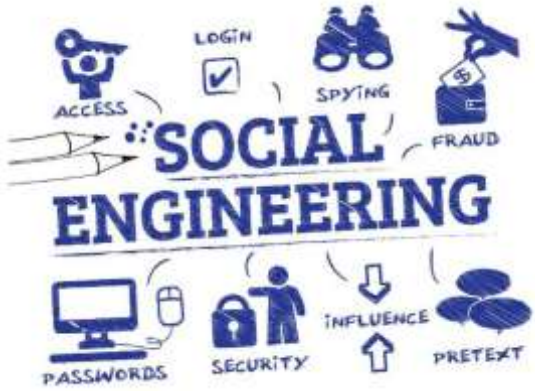
c. Membangun kesadaran pengguna tentang *social engineering attacks*.
d. Menegakkan (atau setidaknya mendorong penggunaan) kebijakan pembuatan sandi yang kuat yang mencakup kriteria berikut:
e. Gunakan huruf besar dan kecil, karakter khusus, dan angka. Jangan gunakan hanya angka. Password tersebut dapat diretas dengan cepat.
f. Salah eja kata atau membuat akronim dari kutipan atau kalimat. Sebagai contoh, ASCII adalah singkatan dari *American Standard Code* untuk *Information Interchange* yang juga dapat digunakan sebagai bagian dari password.
g. Gunakan karakter tanda baca untuk memisahkan kata atau akronim.
h. Ubah password setiap 6 sampai 12 bulan atau segera jika dicurigai password telah diketahui pihak lain.
i. Gunakan sandi yang berbeda untuk setiap sistem. Hal ini sangat penting untuk host infrastruktur jaringan, seperti server, firewall, dan router. Tidak apa-apa untuk menggunakan password sama - hanya buatlah password menjadi sedikit berbeda untuk setiap jenis sistem, seperti *SummerInTheSouth-Win7* untuk sistem Windows dan *Linux+SummerInTheSouth* untuk sistem Linux.
j. Gunakan password dengan variabel panjang. Trik ini dapat membingungkan hacker karena ketidaktahuan panjang minimum atau maksimum password yang diperlukan dan sehingga harus mencoba semua kombinasi password.
k. Jangan gunakan kata slang yang umum atau kata yang ada dalam kamus.
l. Jangan bergantung sepenuhnya pada karakter yang tampak serupa, seperti 3, bukannya E, 5, bukannya S, atau! bukannya 1. Program password cracking dapat memeriksa hal tersebut.
m. Jangan menggunakan kembali password yang sama dalam setidaknya empat sampai lima perubahan password dilakukan.
n. Gunakan screen saver yang dilindungi password. Layar terkunci adalah cara yang bagus untuk sistem untuk diretas bahkan jika hard drive telah dienkripsi.
o. Jangan berbagi sandi. Satu password unik untul satu pengguna.
p. Hindari menyimpan password pengguna di lokasi pusat yang tidak aman, seperti spreadsheet yang tidak terlindungi pada hard disk. Gunakan *Password Safe* atau program serupa untuk menyimpan password pengguna.
q. Aktifkan audit keamanan untuk membantu memantau dan melacak serangan password.
r. Menguji aplikasi untuk memastikan tidak adanya password yang tersimpan dalam jangka waktu tanpa batas dalam memori atau menuliskannya ke disk. Alat yang baik untuk menguji hal ini adalah WinHex.
s. Pastikan sistem di-patched. Password akan disetel ulang selama kelebihan arus buffer atau kondisi penolakan Layanan (DoS) lainnya.
t. Kenali ID pengguna. Jika akun tidak pernah digunakan, Hapus atau Nonaktifkan akun sampai diperlukan. Pengguna dapat menentukan akun yang tidak terpakai dengan inspeksi manual atau dengan menggunakan alat seperti DumpSec, alat yang dapat menghitung sistem operasi Windows dan mengumpulkan ID pengguna dan informasi lainnya.

2.3 Metode yang digunakan hacker untuk meretas password

Seorang hacker dapat menggunakan metode berikut untuk meretas password :

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.



Gambar 1. *Social Engineering*

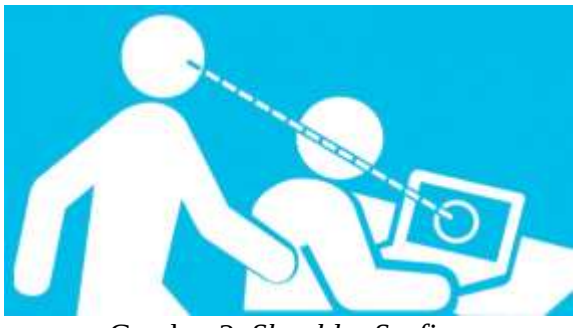
Untuk mendapatkan password melalui *Social engineering*, hacker hanya memintanya. Misalnya, hacker menelepon pengguna dan mengatakan kepadanya bahwa pengguna memiliki beberapa e-mail yang tampak penting yang terjebak dalam antrian mail, dan hacker perlu password untuk login dan membebaskan email tersebut. 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.



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.

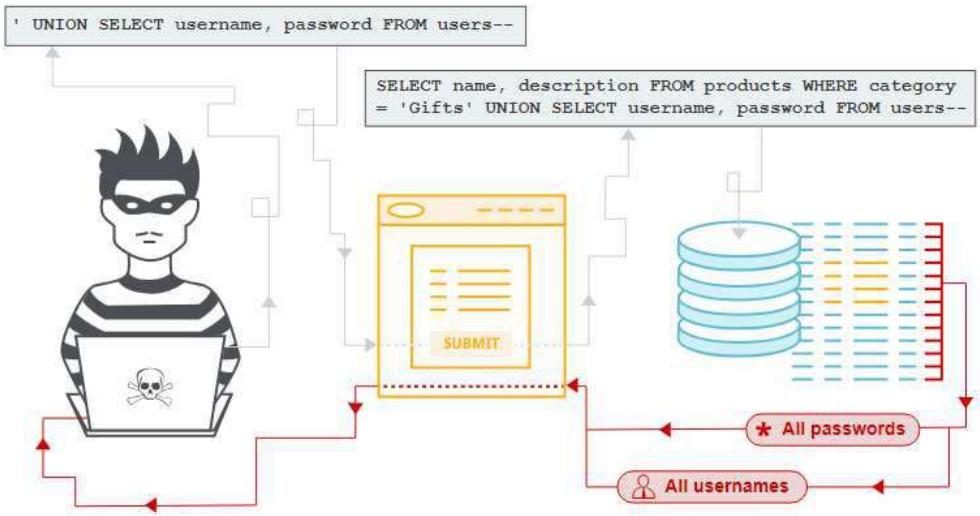
Gambar 3. Keylogger USB Key

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 4. Halaman login palsu yang persis terlihat seperti halaman Facebook sebenarnya.

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 5. Serangan SQL Injection

h. Penyetelan ulang password
Penyerang sering merasa lebih mudah untuk mereset password daripada harus menerkanya. Banyak program untukmeretas password sebenarnya adalah password resetters. Dalam kebanyakan kasus, penyerang melakukan boot dari floppy disk atau CD-ROM untuk mendapatkan mengelabui perlindungan Windows.

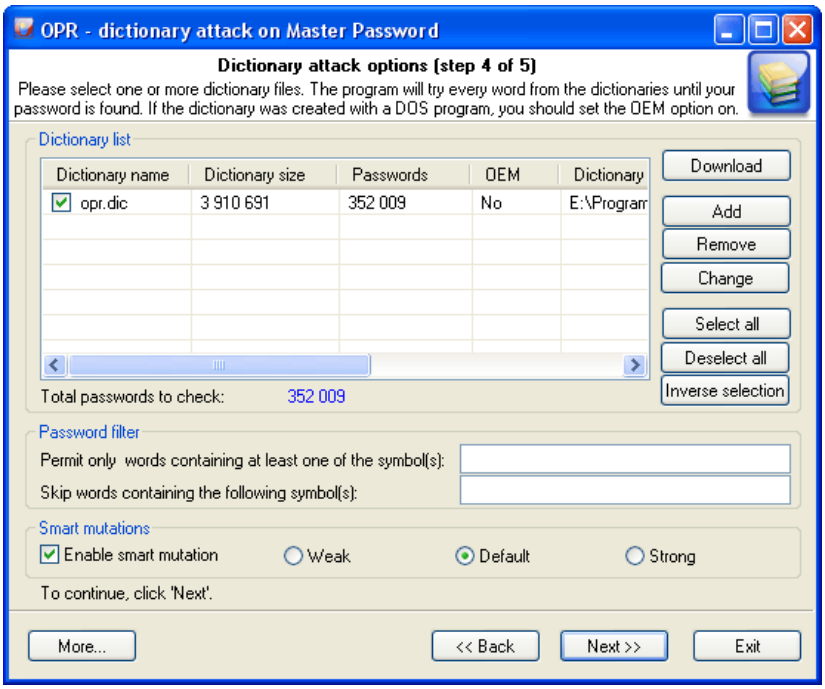
i. Serangan Brute Force
Dalam jenis serangan ini, semua kemungkinan kombinasi password berlaku untuk memecahkan sandi. (Fujita, 2008).
Metode menyerang yang paling dapat diandalkan penyerang atau hacker dan memakan waktu lama adalah serangan Brute Force untuk. Penyerang dapat mencoba dengan setiap kemungkinan 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 dimulai dari termudah. 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 mengambil beberapa dekade.
Reverse Brute Force Attack, dalam serangan brute-force terbalik, satu password diuji terhadap beberapa username atau file terenkripsi. Prosesnya dapat diulang untuk beberapa password tertentu. Dalam strategi tersebut, penyerang umumnya tidak menargetkan pengguna tertentu. Serangan Reverse Brute-Force dapat dikurangi

dengan membangun kebijakan password yang tidak mengizinkan password yang umum.

2.4 Pencegahan dari peretasan password

Semua penanggulangan dari semua serangan password yang harus diketahui pengguna untuk melindungi diri. adalah sebagai berikut :

a. Pencegahan untuk Social Engineering Attack
   Untuk melindungi diri dari Social Engineering Attack pengguna harus belajar mempertanyakan kemungkinan adanya penyerang. Jika pengguna mendapatkan panggilan telepon dari seseorang, dan berpikir bahwa mungkin ada kemungkinan bahwa orang tersebut adalah penyerang, tanyakan beberapa pertanyaan yang harus harus dapat dijawab untuk memperoleh kebenaran. Beberapa penyerang profesional mempelajari dahulu perusahaan sebelum menyerang, sehingga kemungkinan tahu semua jawabannya. Itu sebabnya, jika pengguna masih memiliki beberapa keraguan, maka langkah yang dapat dilakukan adalah meminta kepala Departemen mengenai informasi apa pun yang sebenarnya sehubungan penyerang.
b. Pencegahan untuk penebakan (*guessing*) password
   Untuk mencegah serangan ini terjadi, tidak pernah menggunakan password seperti tanggal lahir, nama gadis ibu, nama hewan peliharaan, nama pasangan, atau apa pun yang seseorang mungkin bisa menebak.
c. Pencegahan untuk Serangan Kamus (*Dictionary Attacks*)
   Serangan Kamus sangat sederhana untuk dicegah. Jangan gunakan password yang ada di kamus. Beberapa mungkin berpikir bahwa jika menggunakan kata dari kamus tetapi hanya mengganti sebagian besar huruf dengan angka, maka password akan aman, padahal tidak. Contohnya jika mengubah kata seperti "password" menjadi p455w0rd. Untuk password yang aman, direkomendasikan menggunakan frase seperti "sukabacabuku?88".



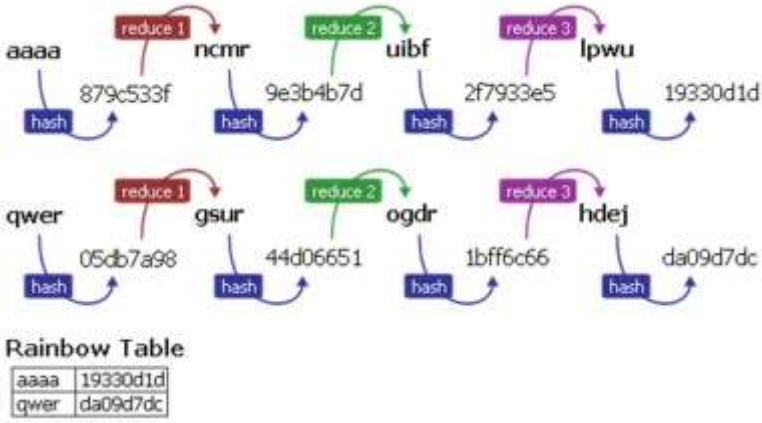
Gambar 6. Serangan Dictionary

d. Pencegahan untuk serangan Brute-Force

Serangan brute-force dapat dicegah dengan membuat password yang sangat panjang, menggunakan banyak angka dan karakter ganjil. Semakin panjang password semakin lama waktu yang dibutuhkan hacker untuk memecahkan password. Jika setelah beberapa hari hacker belum mampu memecahkan password melalui serangan Brute-Force, maka ada kemungkinan hacker menyerah. Seperti disampaikan sebelumnya dalam serangan kamus, membuat frase untuk password adalah pilihan terbaik untuk tetap aman.

Gambar 7.Pencegahan dari serangan Brute Force

e. Pencegahan untuk tabel Rainbow
Peretasan tabel *rainbow* dapat dicegah dengan hanya membuat password yang sangat panjang. Membuat tabel untuk password yang panjang memerlukan waktu yang sangat lama dan sumber daya yang banyak. Itu sebabnya tidak banyak dari tabel ini tersedia.



Gambar 8. Serangan Rainbow table

f. Pencegahan untuk phishing
Serangan phishing sangat mudah dihindari. Ketika diminta untuk memasukkan informasi pribadi ke dalam sebuah situs web, carilah informasi ke *URL Bar*. Jika misalnya seharusnya berada di Gmail.com dan di URL Bar itu menyatakan sesuatu yang sama sekali berbeda seperti gmail.randomsite.com, atau gamilmail.com, maka harus diketahui ini adalah alamat palsu. Ketika berada di situs web Gmail yang sebenarnya, URL harus dimulai dengan www.google.com, selain alamat tersebut maka palsu.

g. Pencegahan untuk serangan key logger kunci

Serangan key logger dapat dihindari dengan menggunakan keyboard virtual di mana posisi karakter akan berubah secara acak. OTP (satu kali sandi) dapat digunakan untuk menghindari serangan key logger. Sebagai contoh, ketika akun Gmail dikonfigurasi dengan autentikasi dua langkah, OTP yang dikirim ke ponsel diperlukan untuk login. OTP dapat diperoleh di perangkat khusus seperti SafeNet eToken NG-OTP, RSA SecurID tokens. AntiLogger seperti asZemana, Sandboxie, key scrambler dapat digunakan untuk menghindari serangan key logger.

h. Pencegahan untuk serangan SQL Injection
   Patch untuk sistem operasi, Softwares, dan antivirus harus diperbarui secara teratur. Validasi yang tepat dari input data dapat mengurangi serangan SQL Injection. Izin kontrol akses pada database harus didefinisikan secara ketat.
i. Pengaturan ulang kata sandi otomatis:
   Fungsi ini memungkinkan pengguna mengelola sebagian besar masalah sandi mereka tanpa melibatkan orang lain. Jika tidak, dukungan ini menjadi mahal, terutama untuk organisasi yang lebih besar

2.5 Metode Otentifikasi berdasarkan password

Ketika menjalankan metode otentikasi pada jaringan dan tingkat kebijakan keamanan, mayoritas pengguna terbukti tidak dapat diandalkan dalam menyimpan dan menciptakan password yang kuat.

a. Passfrase
   Pass frase biasanya suatu kalimat yang selalu mudah diingat baik kutipan, kalimat favorit atau kombinasi dari kedua angka dan karakter khusus. Mayoritas perangkat lunak enkripsi harus menggunakan frasa Pass untuk private key, bukan password.
   Keuntungan : passfrase berupa sebuah ide untuk password menjadi lebih mudah untuk diingat, tapi hampir mustahil untuk diretas. Meskipun hampir mustahil untuk diretas karena panjangnya passfrase.
   Kekurangan: baik password dan passfrase dapat digunakan untuk login melalui penggunaan key logger, atau diketahui jika ditransmisikan melalui saluran komunikasi teks biasa.
b. Metode password konvensional:
   Otentikasi tradisional atau konvensional password sudah terlalu ketinggalan jaman dan merupakan metode yang paling banyak digunakan. Dalam skema ini pengguna masuk ke login menggunakan username dan password. Sistem pertama kali mengotentikasi pengguna dari database pengguna dan atas dasar otentikasi pengguna kemudian diberikan akses ke sistem yang diberikan.
   Keuntungan: merupakan hal yang sederhana, mudah diingat, mudah digunakan, tidak diperlukan perangkat keras atau perangkat lunak atau personil khusus tambahan.
   Kerugian: metodenya rentan terhadap berbagai serangan seperti serangan shoulder surfing, key logger, dan spoofed login dan phishing.
c. Infrastruktur kunci publik (PKI)/Public key cryptography
   Password dapat dienkripsi untuk menghindari serangan. Kriptografi kunci publik juga dikenal sebagai kriptografi asimetris. Fungsi infrastruktur kunci publik (PKI) adalah memberikan entitas, yaitu karyawan atau server kemampuan untuk mengkomunikasikan, mengotentikasi, menandatangani dan memverifikasi identitas dengan membuat sertifikat digital, lalu menghasilkan dua kunci matematis terkait, kunci publik dan kunci pribadi. Kunci publik tersedia bagi siapa saja yang ingin

bertukar data dengan entitas dan kunci privat adalah satu-satunya cara untuk entitas dapat mendekripsi, atau mengidentifikasi password sendiri dengan benar. Pesan mungkin dienkripsi menggunakan kunci publik atau kunci privat dan didekripsi menggunakan kunci pribadi atau kunci publik yang sesuai.

Keuntungan: metode ini memberikan kerahasiaan untuk pesan, digunakan untuk membuat tanda tangan digital dan berguna ketika berkomunikasi melalui jaringan yang tidak aman seperti internet dan server internal.

d. Keystroke dinamics

Keystroke Dinamics adalah solusi biometrik di mana pengguna mengetik secara berirama pada keyboard dan waktu antara tombol ditekan digunakan sebagai teknik otentikasi.

Keuntungan: tidak memerlukan hardware tambahan hanya keterampilan pemrograman saja cukup. Ini mencegah dari shoulder surfing, key logger dan phishing. Bahkan walaupun mempunyai password penyerang tidak dapat mengakses sistem.

Kekurangan: penolakan akan terjadi apabila terjadi kecepatan mengetik yang berbeda dari pengguna. Akan sulit untuk mengidentifikasi bahkan bila yang login adalah pengguna yang sah.

a. Password grafis

Password grafis adalah alternatif untuk password berbasis teks. Objek grafis ditampilkan dan pengguna memilihnya. Objek yang dipilih kemudian digambar oleh pengguna menggunakan mouse, touchpad atau layar sentuh. Sistem berjalan pra-pengolahan pada objek dan mengubahnya menjadi bentuk hierarkis. Akhirnya, pencocokan hierarkis dilakukan untuk otentikasi pengguna.

Keuntungan: ini mencegah dari serangan shoulder surfing.

Kekurangan: sistem mengotentikasi pengguna hanya jika sketsa yang tepat ditarik oleh pengguna pada layar sentuh.

Waktu pemrosesan tergantung pada seberapa baik pengguna menggambar sketsa. Biasanya dibutuhkan waktu lebih lama untuk proses dibandingkan dengan skema lainnya. Juga tergantung pada kemampuan pengguna untuk menggambar sketsa dan waktu proses yang lebih lama daripada skema lain.

b. One-Time Password:

One-time password (OTP) adalah password yang berlaku untuk jangka waktu yang singkat dan hanya dapat digunakan sekali. Sebuah OTP juga dapat dihasilkan dari daftar password. Perbankan dan perusahaan keuangan adalah perusahaan yang selalu menggunakan metode ini.

Keuntungan: OTP digunakan untuk menghindari pencurian identitas, melindungi transaksi online dari serangan replay, key logger dan serangan shoulder surfing.

Kerugian: hal ini membutuhkan beberapa teknologi tambahan seperti SMS ke ponsel, atau panggilan ke mobile untuk OTP.

c. Biometrik:

Biometrik adalah sistem otentikasi berbasis gambar dimana sistem sidik jari, sistem pembacaan wajah, sistem pemindai iris/retina, sistem pengenalan ucapan, sistem verifikasi tanda tangan, sistem geometri tangan, sistem tulisan tangan, digunakan untuk verifikasi spesimen asli. Gambar diproses terlebih dahulu dan kemudian klasifikasi gambar dilakukan.

Keuntungan: Biometrik adalah tanda tangan asli dan unik sehingga tidak dapat dicuri, tidak bisa dilupakan; tidak juga dapat diberikan kepada orang lain. Biometrik akan mengubah cara mengotentikasi diri, dengan 99% akurasi.
Kekurangan: Biometrik mahal dan sulit untuk diimplementasikan.

3. Kesimpulan

Makalah 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.

Daftar Pustaka

[1] Jadhao, P., & Dole, L. (2013). Survey on Authentication Password Techniques. *International Journal of Soft Computing and Engineering (IJSCE)*, 67-68

[2] Jansen, W. (2015). Authenticating Users on Handheld Devices. *Canadian Information Technology Security Symposium*, (pp. 1-12).

[3] Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers*, *23*(3), 256–267. Retrieved from https://doi.org/10.1016/j.intcom.2011.03.007

[4] Choong, Y., & Greene, K. (2016). What's a special character anyway? Effects of ambiguous. *Proceedings of the Human Factors and Ergonomics*, (pp. 760-764).

[5] Kaye, J. (2011). Self-reported password sharing strategies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, (pp. 2619–2622). New York.

[6] Wash, R. R. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. *Proceeding of the 12th Symposium on Usable Privacy and Security*, (pp. 175–188).