CyberStudio Blog

# Manajemen *Password*

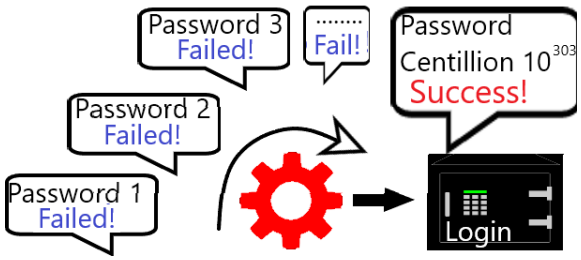
Dengan semakin meningkatnya penggunaan teknologi informasi, maka semakin meningkat pula jumlah user account dan password yang harus kita ingat dan kelola. Password merupakan metode yang nyaman dan mudah untuk melakukan autentikasi user saat masuk ke sistem komputer. Sistem hanya mengharuskan user untuk memberikan informasi yang dapat membuktikan bahwa dia adalah benar orang yang diklaimnya. Pasword biasa digunakan untuk masuk atau login pada akun internet banking, email, sosial media dan lain sebagainya.

Dalam pemilihan password biasanya kita akan mengalami dilemma. Hal ini karena ketika kita menggunakan password yang sama pada beberapa situs maka akan memudahkan hacker ketika terjadi penyusupan pada satu situs untuk mengakses situs-situs lain, namun jika menggunakan password yang berbeda pada masing-masing situs maka user lebih cenderung memilih password yang mudah diingat atau bahkan akan mencatatnya ini juga dapat membahayakan keamanan system yang bersangkutan.

## Beberapa Resiko Berikut Memungkinkan Pengguna Kehilangan Password Mereka

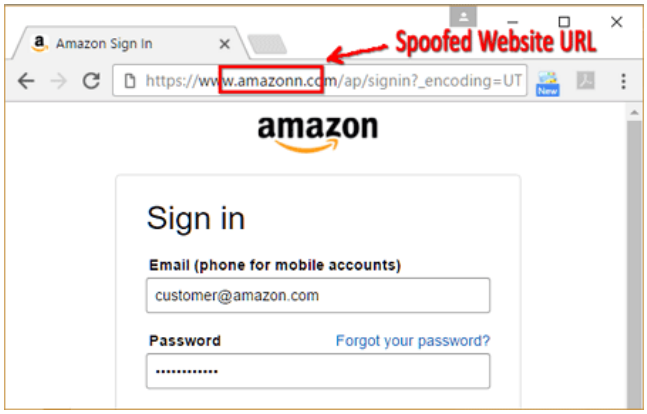
1. Over the Shoulder Attack
   Yaitu sebuah serangan dimana penyerang secara fisik dapat melihat layar perangkat dan keyboard untuk mendapatkan informasi pribadi. Ketika seseorang mengetik passwordnya, orang lain mungkin bisa mengamati apa yang diketiknya dan mencurinya dengan melihat melalui bahu orang tersebut, atau dengan pengawasan secara tidak langsung menggunakan kamera.

2. Brute Force Attack
   Yaitu sebuah serangan dimana penyerang dapat menggunakan program yang secara otomatis dapat menghasilkan password, penyerang akan mencoba semua kemungkinan kombinasi sampai password yang valid ditemukan.




3. Sniffing Attack
   Ketika password dikirim melalui jaringan, password tersebut dapat ditangkap oleh alat sniffing jaringan jika saluran jaringan tidak dienkripsi dengan benar. Alat-alat berbahaya seperti keylogger mungkin bisa menangkap password pengguna ketika diketikkan selama proses autentikasi.

4. Login Spoofing Attack
   Dimana penyerang membuat sebuah halaman login palsu yang mirip dengan halaman asli dengan tujuan untuk mendapatkan informasi peibadi user. Berikut ini merupakan contoh dari login spoffing attack yaitu website spoofing yang mempunyai interface layaknya amazon dengan dibekali area login yang serupa sehingga penyerang dapat mencuri informasu akun.




Tips Agar Password yang Kita Buat Kuat dan Aman :

1. Gunakan kombinasi angka, huruf kecil dan huruf besar. Jika memungkinkan dapat menggunakan beberapa karakter special seperti *,&,%,@,-, dll.
2. Usahakan password yang kita buat memiliki panjang lebih dari 8 karakter karena semakin panjang password maka semakin besar pula kemungkinan password.

3. Hindari penggunaan tanggal lahir, nama orang tua, nama artis idola, urutan nomor serta kata yang ada pada kamus.
4. Gunakan password yang berbeda pada setiap akun, namun jangan menulis atau mengetik password di ponsel, kertas ataupun dokumen file.

---

Contoh password lemah dan kuat:

1. Password lemah :
    - “password” : dianggap lemah karena mudah ditebak
    - “administrator” : dianggap lemah karena merupakan username
    - “ayulestari” : dianggap lemah karena menggunakan nama orang
    - “aaaaaaa” : dianggap lemah karena perulangan huruf yang sama
    - “abcde”/“12345” : dianggap lemah karena merupakan huruf/angka berurutan
    - “computer” : dianggap lemah karena menggunakan kata yang ada pada kamus
2. Password Kuat :
    - t3wahSetyeT4 : tidak ada satu kata di kamus, mengandung karakter abjad dan numerik.
    - 4pRte!ai@3 : tidak ada satu kata di kamus yang mempunyai karakter abjad,numeric, dan tanda baca.
    - Convert_100$toEuros! : ungkapan atau frase yang panjang dan berisi lambang untuk meningkatkan kekuatannya.