KEAMANAN DAN MANAJEMEN PASSWORD

Ahmad Ilham Arismawan, 09011381621064

Berdasarkan pada beberapa artikel seperti [1] dan [2] password merupakan sebuah kunci keamanan yang mengidentifikasikan seorang end-user. Password menjadi resiko terbesar dalam menidentifikasi sebuah user. Dengan password yang lemah, meskipun sebuah sistem memiliki keamanan yang sangat tinggi, maka sistem tersebut sama saja menjadi incaran yang mudah bagi seorang penyerang [3]. Melalui password cracking, password yang lemah terbut akan dibobol dan penyerang akan dapat mengambil alih akun bahkan sistem tersebut. Password cracking merupakan proses untuk menebak atau memulihkan kata sandi yang sebelumnya telah tersimpan dalam sistem [4] dengan tujuan untuk mengambil alih atau mencuri data dari atau melalui user yang sah.

Kenapa keamanan password sangat penting?

Seperti yang dikatakan pada artikel [1] bahwa keamanan password merupakan hal yang sangat penting. Password merupakan satu-satunya hal yang dapat mengidentifikasikan seorang user terhadap sistem. Jika seorang user memilih password dengan kombinasi yang mudah untuk di tebak atau dengan keamanan yang rendah, maka user tersebut telah memberikan sebuah kunci terhadap seluruh informasi user tersebut kepada para hacker atau penyerang.

Menjaga keamanan password merupakan salah satu hal yang cukup mengeluarkan banyak biaya. Dibandingkan dengan keamanan terhadap serangan seperti Flooding, serangan seperti ini hanyalah serangan yang bersifat sementara, sedangkan serangan yang mengincar password dapat menjadi ancaman yang bersifat lama hingga sistem tersebut benar-benar bersih dari penyerang. Hal yang paling berbahaya ketika seorang penyerang berhasil mendapatkan password adalah, mereka dapat mengambil informasi yang sensitif, seperti nomor rekening, data pribadi bahkan password terhadap sistem yang lainnya. Jika hal ini terjadi pada sebuah perusahaan besar, maka bias saja penyerang tersebut mengambil data perusahaan tersebut dan menjualnya. Hal ini tentu sangat berbahaya apalagi jika menyangkut informasi yang sensitif.

Dalam survey yang dilakukan [1] password yang paling sering digunakan oleh banyak user di seluruh dunia adalah seperti password, abc23, qwerty123, 123456, <username>, <username>123, admin dan <tanggal ulang tahun>. Tentu saja penyerang mengetahui hal tersebut, dengan begitu penyerang terkadang cukup menggunakan kamus/wordlist dan program cracking seperti john the ripper yang berisikan banyak kalimat yang paling sering digunakan untuk password.

Sistem algoritma hashing untuk mengenkripsikan sebuah password diperkenalkan pertama kali oleh Microsoft dalam LANMAN hashing protocol meskipun sistem ini masih lemah dan mudah untuk dibobol. Saat ini hampir seluruh sistem penyimpanan password menggunakan algoritma hashing. Algoritma hashing merupakan sebuah fungsi satu arah yang mengubah string menjadi "sidik jari" dengan panjang tetap yang tidak dapat di balik. hanya fungsi hash kriptografi yang dapat digunakan untuk mengimplementasikan hashing dalam sebuah password. Beberapa contoh algoritma hasihing yang banyak di gunakan adalah MD5, SHA-1, LM, NTLM, dan whirpool [2]

Serangan apa saja yang mungkin dapat terjadi terhadap keamanan password?

Hal pertama yang akan di lakukan penyerang terhadap targetnya adalah menemukan username, kemudian menemukan algoritma hashing yang digunakan dalam sistem tersebut. Dengan 2 hal tersebut, password cracking menjadi hal yang mudah bagi mereka.

Ketika seorang penyerang melakukan sebuah serangan password cracking, ada kemungkinan 2 jenis cara yang paling umum dilakukan yaitu :

a. Brute force attacks, dan
b. Dictionary attacks

Namun demikian ada juga beberapa penyerang yang menggunakan metode lain seperti metode hybrid dengan menggabungkan beberapa metode yang ada dalam melakukan serangan. Brute force merupakan cara yang paling pasti dalam melakukan password cracking, serangan ini bekerja dengan mengulang semua karakter yang ada dalam keyboard dan mengkombinasikannya hingga password ditemukan. Meskipun akan memakan waktu yang lebih lama dengan mengkombinasikan seluruh karakter

yang ada dalam keyboard, serangan brute force memiliki kemungkinan yang lebih banyak dalam menebak password yang akan dibobol.

Sedangkan serangan dictionary akan bebasis pada kamus “word list” yang digunakan dalam serangan tersebut. Berbagai kalimat atau kata dalam word list akan di coba terhadap password yang akan di bobol. Meskipun lebih cepat namun kemungkinan password tertebak akan lebih sedikit dibandingkan dengan serangan brute force, karena keterbatasan terhadap kalimat yang ada didalam word list tersebut.

Sedangkan pada serangan hybrid, penyerang akan menggabungkan beberapa metode sperti misalnya adalah metode dictionary attacks, namun dengan mengkombinasikan dan membuat variasi baru berdasarkan pada word list yang telah ada seperti pada hal serangan brute force.

Serangan-serangan yang dapat terjadi dapat diminimalisir dengan menggunakan enkripsi menggunakan algoritma hashing terhadap password yang digunakan. Dalam beberapa kasus belakangan ini enkripsi tersebut dapat mudah di tebak dengan menggunakan tools yang telah tersedia seperti jack the ripper ataupun ophcrack dan tools lainnya [1].

Bagaimana menjaga dan memanajemen password yang tepat?

Lalu bagaimana menjaga agar password tetap aman dan sulit untuk di bobol melalui serangan password cracking?. Beberapa hal yang dapat meningkatkan keamanan password adalah:

1. Gunakan password yang tidak mengandung unsur nama pribadi, nama teman, nama hewan peliharaan ataupun tanggal lahir.
2. Panjang password usahakan lebih dari 15 karakter, dengan unsur yang kompleks menggunakan huruf, angka, simbol dan gunakan uppercase serta lowercase pada penggunaan huruf.
3. Ganti password secara rutin, 90 hari sekali ganti password merupakan hal yang bagus di gunakan untuk mengganti password baru.

Password cracking merupakan serangan yang sangat berbahaya. Banyak cara yang dapat dilakukan oleh penyerang dalam melakukan password cracking. User saat ini harus memiliki password yang bagus dan kuat dalam menjaga agar penyerang tidak dapat melakukan password cracking. Selain itu user harus mengganti password secara rutin. Sistem keamanan hash yang digunakan saat ini untuk mengenkripsi password

tidak cukup kuat jika user hanya menggunakan password yang lemah dan tidak pernah di ganti sama sekali.

Daftar Pustaka

[1] A. N. Solutions, “Everything Administrators need to know about Windows password security .,” 2008.

[2] G. Khalil, “Information Security Reading Room Password Security-- Thirty-Five Years Later _____,” 2019.

[3] W. Paper, “Trusted Internet Services from the Sign of Trust on the ‘ net.,” *DisClosure*.

[4] J. A. Chester and " Analysis, “IdeaExchange@UAkron Analysis of Password Cracking Methods & Applications Recommended Citation Analysis of Password Cracking Methods & Applications,” 2015.