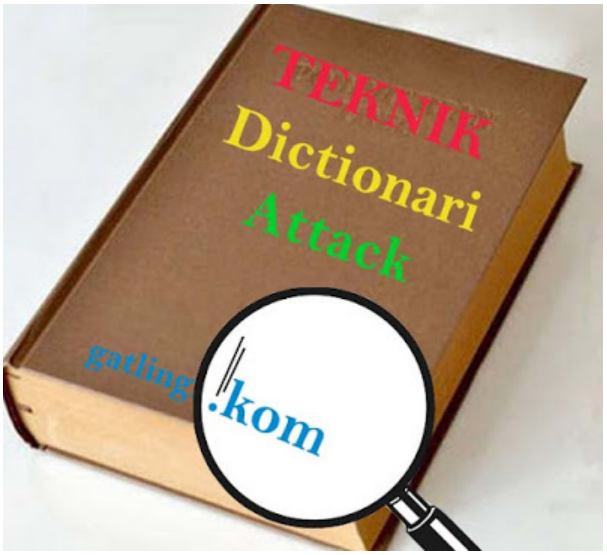
Waspada, 10 Teknik Cracking Password yang Sering Dipakai Hacker

Dunia Digital tidak ada ubahnya seperti dunia nyata dimana kejahatan dan kebaikan selalu ada, jika Anda tidak mempunyai kunci rumah maka dapat dipastikan pencuri akan masuk tapi lain halnya jika rumah Anda memiliki kunci didalamnya maka pencuri akan kesulitan masuk. Nah kejahatan didunia digital seperti itu, jika Anda tidak memiliki pengaman atau password pada komputer maupun akun Anda maka dapat dipastikan pencuri dapat masuk dan mencuri data-data penting Anda, meskipun Anda memiliki kunci atau password tapi jika passwordnya terlalu lemah maka sama saja seperti Anda memberi peluang pada pencuri untuk menduplicate password tersebut, biasanya teknik seperti ini disebut dengan password cracking. Password cracking adalah istilah umum yang menggambarkan sekelompok teknik yang digunakan untuk memperoleh password atau menemukan kata kunci rahasia dari data yang telah disimpan atau yang dikirim oleh sistem komputer. Pendekatan umumnya dengan secara terus-menerus menebak password yang ingin di-crack. Sebenarnya Tujuan password cracking adalah untuk membantu user memperoleh kembali password yang hilang/lupa, ini sama halnya ketika kunci motor kita hilang maka teknik password cracking ialah untuk mencari dan menemukan kunci tersebut, jika kunci masih belum ditemukan maka yang perlu kita lakukan ialah menebak atau menduplicate kunci tersebut agar cocok dengan motor kita. Password Cracking berguna juga untuk mendapatkan hak-hak akses ke sebuah sistem, atau sebagai ukuran pencegahan oleh administrator sistem untuk mengecek password-password yang dapat di-crack dengan mudah. Istilah password cracking terbatas untuk menemukan kembali satu atau lebih plaintext password dari password yang di-hash. Password cracking membutuhkan attacker yang dapat mengakses hashed password, ataupun dengan membaca database verifikasi password maupun dengan mencegah hashed password dikirim ke jaringan luar. Andapun dapat juga dengan mencoba-coba memasukkan password sampai benar seperti yang dikenal dengan metode Password Guessing . Jadi sudah mengertikan apa itu Password cracking. Nah artikel kali ini akan menjelaskan teknik-teknik Cracking yang biasanya digunakan para hacker untuk mencari, menebak, memperoleh, menemukan, ataupun membobol password pada sebuah sistem, dan katanya teknik ini sering digunakan para hacker.

1. Dictionary Attack



Dictionary attack ialah serangan yang digunakan untuk menduga key dari suatu ciphertext dengan mencoba berbagai kata kunci yang umum digunakan oleh manusia , biasanya kata-kata dalam kamus. Dictionary attack bisa lebih efektif bila dibandingkan dengan brute force, karena tidak perlu mencoba berbagai kemungkinan, hanya sebatas kata-kata yang ada dalam kamus. Hanya saja ada kelemahan fatal, yakni bila key yang digunakan ialah kata yang tidak ada dalam kamus. Karna Dictionary attack hanya mengadalkan segala kemungkinan-kemungkinan yang ada, artinya Anda tidak akan langsung berhasil menemukan passwordnya, mungkin hingga puluhan atau ratusan kali mencoba akan berhasil, tergantung kesulitan password tersebut dan juga isi kamus tersebut.

Dictionary Attack menggunakan teknik target berturut-turut mencoba semua kata dalam daftar yang lengkap disebut kamus (Kamus ini bisa dibilang berisi kata-kata atau password-password Aneh). Berbeda dengan brute force attack, di mana sebagian besar kuncinya dicari secara sistematis, Maka lain halnya dengan Dictionary Attack yang hanya mereka-reka kemungkinan yang paling mungkin berhasil, dengan menggunakan kamus tadi. Umumnya, dictionary attack berhasil karena banyak orang memiliki kecenderungan untuk memilih password yang pendek (7 karakter atau kurang), satu kata-kata yang ditemukan dalam kamus atau sederhana, Maka akan mudah diprediksi variasi pada kata-katanya, seperti menambahkan angka. Untuk mengatasi dari kejahatan ini biasanya dengan menggunakan password yang panjang dan pastinya sulit, usahakanlah jangan menggunakan password yang umum dan tak mengandung kata-kata mudah.

2. Brute force attack

Brute force attack atau dalam bahasa Indonesia disebut juga dengan Serangan brute force ini adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci password yang memungkinkan atau istilah gampangnya mungkin menggunakan Random password atau password acak. Brute Force Attack akan meretas *password* (password cracking) dengan menggunakan kombinasi yang ada pada "*wordlist*". Metode ini dijamin akan berhasil menemukan *password* yang ingin diretas. Namun, proses untuk meretas *password* dengan menggunakan metode ini akan memakan banyak waktu dan kesabaran tingkat dewa benar-benar harus dijalankan. Lamanya waktu akan ditentukan oleh panjang dan kombinasi karakter *password* yang akan diretas.

Jadi sudah jelaskan kalau Brute Force Attack sangat berbahaya, jika Anda tidak waspada bisa saja saat ini seluruh sistem atau akun Anda sudah diretas. Oleh karena itu saya tidak menyarankan untuk menggunakan password sembarangan seperti menggunakan Nama, Tempat Tanggal lahir, Telepon atau informasi pribadimu. Apalagi password yang digunakan hanya 7 karakter saja sangat tidak disarankan. Serangan brute force attack bisa saja memakan waktu yang sangat lama bahkan sampai berbulan-bulan atau tahun tergantung dari tingkat kerumitan password dan kecepatan prosesornya, tapi yang perlu di ingat serangan ini selalu berhasil. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: **"When in doubt, use brute-force"** (jika ragu, gunakan brute-force). Teknik ini paling banyak digunakan para hacker untuk memecahkan password, kunci, kode atau kombinasi.

3. Shoulder Surfing

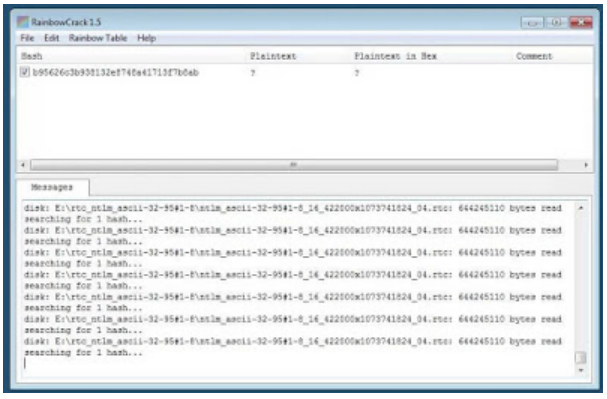
Shoulder Surfing merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi tentang targetnya dengan menggunakan teknik-teknik pengamatan langsung atau memata-matai korbannya secara langsung. Hacker akan selalu mengawasi gerak-gerik targetnya, hal ini jelas untuk mendapatkan segala informasi targetnya. Teknik pengamatan langsung ini umumnya efektif dan sering dilakukan di dalam tempat-tempat yang penuh sesak, bahkan dikantor ataupun di warnet-warnet , karena hal ini akan relatif mudah untuk mengamati tingkah laku seseorang yang akan dijadikan target. Hacker akan selalu mengawasi korbanya dan mendapatkan password dari sana Seperti Saat seseorang mengisi form informasi baik di perangkat elektronik lainnya ataupun disebuah berkas, Memasukkan PIN di ATM atau suatu mesin POS (Point of Sale), Menggunakan kartu nama pada suatu telepon prabayar yang publik, Memasukkan kata sandi pada suatu cybercafe, pustaka-pustaka publik dan universitas, atau kios-kios ,warnet, pelabuhan udara, dan lain-lain.

Umunnya teknik Shoulder Surfing ini bisa dilakukan secara langsung ataupun menggunakan alat bantu seperti teropong dua lensa, kamera-kamera mini yang diletakan ditempat tersembunyi atau langit-langit, dinding sebagai peralatan untuk mengamati entri data, dan tak jarang mereka menggunakan teknik keylogger pada keypad ATM hanya semata-mata untuk mendapatkan informasi penting.

Untuk mencegah seseorang melakukan teknis Shoulder Surfing, bisa dilakukan dengan cara sebagai berikut :

- Membatasi pandangan seseorang, waktu kita menulis atau menggunakan keypad untuk memasukkan informasi yang rahasia dengan menggunakan tubuh kita atau tangan.
- Pilihlah tempat ATM yang memiliki tampilan tertutup seperti terbatasnya jarang pandang saat dilihat dari luar, sehinga orang-orang diluar tidak dapat mengetahui gerak gerik Anda.
- Apabila melakukan transaksi menggunakan Mesin POS (Point of Sales) yang umum tersedia di dalam toko-toko, supermarket-supermarket , hendaknya menghalangi dengan badan atau tangan kita sewaktu memasukkan PIN atau dengan tidak meletakkan mesin tersebut ditempat yang datar yang mudah untuk dilihat oleh seseorang waktu mengetik PIN di mesin POS tsb.
- Jangan memasukkan PIN atau melakukan transaksi aplikasi tranfer dan pembayaran online, seperti internet banking menggunakan fasilitas komputer umum, seperti di warnet pustaka-pustaka publik dan universitas, kios-kios pelabuhan udara. Apabila terpaksa menggunakan pastikan komputer yang digunakan bebas dari aplikasi seperti keyloger dan yang sejenisnya, pastikan site yang ada kunjungi untuk melakukan transaksi tersebut benar.
- Dan jangan lupa untuk selalu perhatikan teman disekitar Anda karna teknik ini bisa dilakukan oleh semua orang, bahkan orang tuamu bisa mendapatkan password dan emailmu dengan memantau mu, jadi pastikan tidak ada siapun saat memasukan akunmu pada komputer.

4. Rainbow table Attack

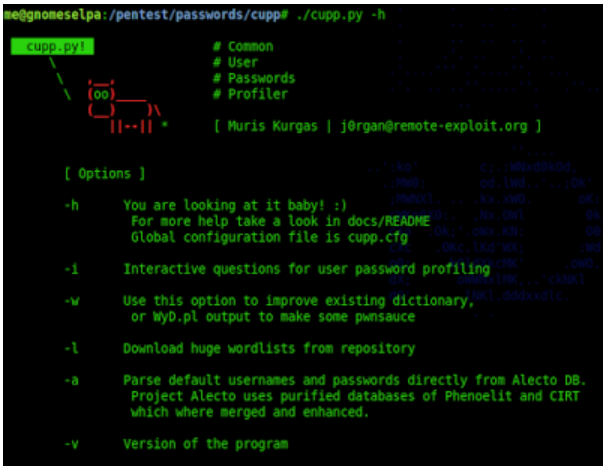


Rainbow table adalah *lookup table* yang digunakan untuk mendapatkan plain text dari password yang telah dirubah menggunakan fungsi hash, Hash adalah hasil dari sebuah enkripsi sebuah password atau informasi yang dianggap penting. Rainbow table ini menggunakan memori berskala besar yang dapat menggantikan teknik brute force konvensional. Teknik Rainbow table diklaim dapat meretas password dengan kecepatan yang lebih tinggi dan baik. Software ini akan menggenerasi table menggunakan algoritma tertentu dan menyimpannya ke dalam table berformat rainbow table. Memang proses menggenerasi table ini cukup menyita waktu bisa sampai 12 jam atau lebih, akan tetapi apabila table tersebut telah siap, maka proses peretasan akan berjalan lebih cepat dibandingkan menggunakan brute force.

Jadi sudah jelas kalau Cracking password menggunakan rainbow table tidaklah sesulit saat kita mengunakan teknik cracking dengan cara brute force. Rainbow table membuat password cracking lebih cepat dibandingkan dengan metode sebelumnya, seperti brute force attack dan dictionary attack. Berdasarkan pada software password cracking yang menggunakan metode rainbow table mampu memecahkan password 14 karakter alfanumerik sekitar 160 detik saja.

Rainbow table dibentuk oleh fungsi hash dan fungsi reduksi. Fungsi hash merubah plaintext menjadi hash, sedangkan fungsi reduksi merubah hash menjadi plain text. Tetapi, perlu diingat bahwa fungsi reduksi bukan merupakan kebalikan dari fungsi hash. Fungsi hash dan fungsi reduksi bersifat *irreversible*. Jadi, apabila kita merubah sebuah hash dengan menggunakan fungsi reduksi, maka plain text yang didapat bukanlah plain text aslinya, melainkan plain text lain. Mencegah dari serangan ini memang sulit, password yang panjang sekalipun masih tetap tidak berpengaruh mungkin satu-satunya cara ialah menggunakan password tanpa kata misal seperti ini, #$@%!#^!#^@$#%^_^%#W*^!^E*8sa^%^64.

5. offline password attack



Pengertian dari serangan offline password attack sebenarnya adalah metode serangan terhadap sebuah karakter sandi yang telah terenkripsi pada berbagai metode enkripsi serta berusaha untuk memecahkannya menjadi berbagai format secara offline atau tidak membutuhkan koneksi internet sebagai media. Serangan Password Offline dilakukan dari lokasi yang berbeda, selain komputer yang sebenarnya di mana password tinggal atau digunakan. Serangan Offline membutuhkan akses fisik ke komputer yang menyimpan password. Penyerang menyalin file sandi dan kemudian mencoba untuk memecahkan password dalam sistem pribadi mereka. Tools offline password attack yang digunakan ini adalah cupp.py. Cupp.py sebenarnya lebih kepada pendekatan "Social Enggineering" ketimbang "Offline Password Attack" betapa tidak tools ini sebenarnya di gunakan setelah pengumpulan informasi melalui teknik Social Engineering.
Cupp.py merupakan singkatan dari "Common User Password Profiller" dan di ciptakan oleh Muris Kurgas. Cupp.p adalah sebuah tools yang secara otomatis akan membuat password lis berdasarkan hasil dari pengumpulan informasi baik lewat Information Gathering atau Social Engineering, Biasanya lewat Social Engincering karena ini lebih kepada "Humanity Social Information".

6. dumpster diving

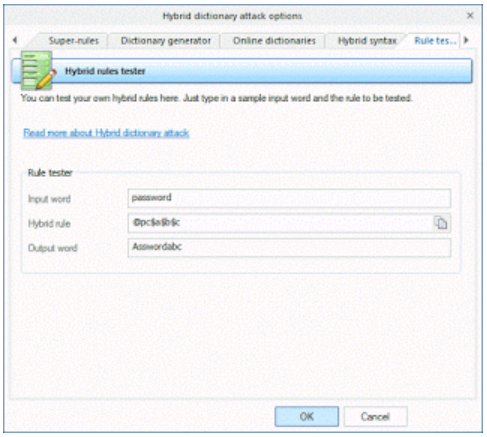
dumpster diving atau scavenging merupakan metode mendapatkan akses ke informasi rahasia dengan cara melihat-lihat catatan perusahaan, pencarian informasi penting ini dilakukan sacara tidak lazim, yaitu mengais-ngais tempat sampah perusahaan. Karena karyawan biasanya tidak terlalu memikirkan dokumen yang telah mereka simpan sehingga copyannya seringkali dibuang begitu saja, mereka tak sadar bahwa copyan itu bisa saja berisi informasi tetang keamanan sistem perusahaan tersebut. Sudah jelas kalau hasil copyan tadi bisa manfaatkan hacker untuk mendapatkan akses entah itu password atau informasi yang berharga lainnya. Teknik ini pernah di-praktekkan oleh sang hacker legendaris yaitu Kevin Mitnik. Di mana dia juga mencari informasi melalui tong sampah korbannya. Jangan meremehkan hal yang satu ini karena banyak informasi yang bisa didapatkan melalui teknik seperti ini seperti memo perusahaan, print-out user-id dan bahkan password. Jika Anda pimpinan atau seorang karyawan maka hal seperti ini jangan dianggap remah, kadang pemulung jauh lebih pintar dari orang yang membuat sampah sembarangan, mereka sadar atau tidak sadar bahwa sampah tersebut bisa bermanfaat.

7. Social Engineering

Social Engineering adalah sebuah teknik pendekatan yang memanfaatkan aspek-aspek sosial di dunia komputer dan internet. Teknik ini biasanya digunakan untuk mendapatkan data-data pribadi seseorang untuk keperluan yang negatif seperti pencurian rekening bank, pencurian password, pencurian akun-akun tertentu atau kejahatan teknologi yang berpotensi lainnya. Semua hal ini dilakukan oleh para hacker dan sejenisnya. Para hacker memanfaatkan kelemahan suatu sistem yaitu manusia, karena tidak ada sitem di dunia ini yang tidak melibatkan interaksi manusia. Secanggih apapun teknologi internet tetap membutuhkan manusia, kelemahan ini bersifat universal, tidak tergantung platform, sistem informasi, protokol, software ataupun hardware. Intinya, semua sistem memiliki kekurangan yang sama pada satu titik yaitu pada faktor sosial manusia.

Social Engineering ini bisa terjadi karena banyak faktor, diantaranya adalah faktor kecerobohan seorang user dalam mengelola passwordnya atau bisa juga seorang hacker berpura-pura menjadi orang yang berkepentingan dalam sebuah sistem dan seolah-olah memerlukan password, akses ke jaringan, peta jaringan, konfigurasi sistem dan semacamnya untuk suatu keperluan tertentu. Masih banyak faktor-faktor lainnnya yang semua itu merupakan diri manusia itu sendiri. Anda tau Kevin Mitnik, ya...dalam filmya dia pernah menggunakan teknik ini hanya demi sebuah tatangan, jika berhasil diakan diberi makanan enak dan pastinya Kevin Mitnik berhasil. Film ini mengajarkan kita untuk selalu waspada pada siapapun dan jangan langsung termakan omongannya bahkan jika itu sifatnya mengancam, usahakan jika Anda mendapatkan serangan seperti ini jangan pernah memberikan username atau password Anda. Teknik ini pernah ngehits di indonesia beberapa waktu yang lalu, apakah Anda tau mama dan papa minta pulsa, yang seperti inilah serangan Social Engineering.

8. Hybrid Attack



Sebuah serangan hybrid adalah tingkat berikutnya dari serangan hacker yang perlu dicoba jika password tidak dapat ditemukan dengan menggunakan dictionary attack. Serangan hybrid dimulai dengan file kamus dan pengganti angka atau simbol untuk karakter pada password. Misalnya, banyak pengguna menambahkan angka 1 atau yang lainnya pada password mereka untuk memenuhi persyaratan sandi yang kuat. Sebuah serangan hybrid dirancang untuk menemukan jenis-jenis anomali dalam password.

9. Password Guessing

Password Guessing merupakan Suatu usaha untuk menebak password sehingga pada akhirnya para Cracker ini bisa menggunakan password tersebut. Biasanya para Cracker akan melakukan hal ini di saat dia sudah tau email Anda dan mulai mereka-reka atau mencoba-coba password yang ada, hal ini juga di sering dilakukan oleh pemiliknya sendiri disaat dia lupa password akunnya, sehingga dia berusaha mengingat password itu kembali, atau menggunakan fitur "LUPA PASSWORD" untuk memulihkan akunnya kembali. Cara ini akan sulit bagi Cracker jika Korbannya mengaktifkan two-steps atau menggunakan 2 langkah masuk ke akun.

10. Rule Based Attack

Jenis serangan ini digunakan ketika penyerang sudah memiliki beberapa informasi tentang password atau sistem yang akan diserang. Ini adalah serangan paling kuat karena cracker tahu tentang jenis password. Teknik ini melibatkan penggunaan brute force, dictionary dan syllabe attack. Dia kemudian dapat menulis aturan sehingga software password cracking akan menghasilkan hanya password yang memenuhi aturan ini. Misalnya, jika penyerang tahu bahwa semua password pada sistem terdiri dari enam huruf dan tiga angka, ia dapat membuat aturan yang menghasilkan hanya jenis password dengan aturan tersebut. Sungguh serangan yang berbahaya bukan, oleh karena itu tingkatkan terus keamanan Anda.

Itulah beberapa Cracking Password yang biasa digunakan para hacker untuk memproleh password dan username Anda, dan masih banyak lagi tipe-tipe teknik cracking seperti, Pre computed hash attack, Passive Online Attack, Active Online Attack, Non Electronic Attack, Syllabe Attack, keylogger, Trojan & Spyware, Hash Injection, port scan Attack, dan lain-lain. Semua teknik ini harus Anda waspadain jika Anda lengah sedikit saja, siap-siap saja Anda akan dirugikan, usahakan lah untuk terus mengupdate Anti Virus, jangan melakukan transaksi di jaringan publik. Pastikanlah untuk membuat password yang panjang dan sulit, tidak menggunakan kata-kata umum, dan lain-lain.

> Banyak orang “Bodoh” yang hanya mengandalkan semangat dan kerja keras plus sedikit kerja cerdas, menjadikannya sukses dalam berbisnis. Dilain sisi kebanyakan orang “Pintar” malas untuk berkerja keras dan sok cerdas. (Bob Sadino)

Sekian dari artikel saya jika ada yang ingin Anda tanyakan atau ingin menambahkan silahkan komentar dibawah ini terima kasih.

Posting Komentar

blogger facebook

Peraturan penting...!!!
1. Usahakanlah untuk Komentar sesuai isi postingan, jika ingin komentar lain maka klik Out Of Topic (OOT)
2. Komentarlah yang sopan santun dan bertata krama
3.Dilarang nyepam, promosi, berjualan, atau berbau porno
4. Komentar yang melanggar akan dihapus

(https://www.blogger.com/comment-iframe.g?blogID=8760495906860983172&postID=5574875105493840489&blogspotRpcToken=4444069)

Masukkan komentar Anda...

Beri komentar sebagai: Dinda AyuiKa (▼ Logout

Publikasikan Pratinjau Beri tahu saya