Laporan Pendahuluan Praktikum Kemanan Data : SSH Bruteforce Attack & Algoritma Fail 2 Ban

oleh Dimas Rizky H.P. – 2110141011 – 3 D4 IT A

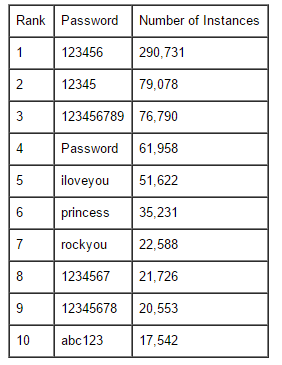
SSH BRUTEFORCE ATTACK & CARA KERJA BRUTEFORCE ATTACK

SSH (Secured Shell) merupakan salah satu aplikasi yang memungkinkan user untuk melakukan *remote login* ke komputer lain di luar jaringan dengan menggunakan proses autentifikasi dan dilengkapi dengan sistem komunikasi yang setiap keluar masuk data akan dienkripsi terlebih dahulu. Dalam pengaplikasiannya, SSH mewajibkan *user* untuk memasukan username dan password agar dapat terhubung dengan *remote computer*-nya.

Dengan segi keamanan yang lebih baik daripada pendahulunya, telnet, SSH juga memiliki beberapa kelamahan dalam segi keamanannya. Beberapa kelemahannya antara lain adalah password dari user dapat ditebak oleh siapapun sehingga jika ada user yang melakukan tebakan yang beruntung, maka user tersebut dapat masuk atau melakukan *remote login*. Kelamahan yang lainnya adalah, default SSH sendiri membolehkan *attempt* atau jumlah percobaan autentifikasi yang tidak terbatas, artinya jika user ingin menebak suatu password, maka user dapat mencoba menebak password tersebut sebanyak yang ia mau. Hal tersebut tentunya membuat SSH rentan terhadap *brute-force attack*.

*Brute-force attack* merupakan metode penyerangan dimana penyerang mencoba menebak kombinasi passwod dan username dengan cara mencoba login dengan banyak kombinasi passphrases yang ada dengan harapan salah satu passphrasenya sama dengan passphrase yang digunakan untuk login ke sistem. Penyerang akan secara sistematis melakukan cek pada setiap kombinasi yang memungkinkan antara username dan password yang ada.

Pada Desember 2009, terjadi *password breach* besar besaran dari website Rockyou.comyang membuat data 32 Juta data password penggunanya tersebar ke publik. Penyerang berhasil membocorkan daftar 32 juta password pengguna rockyou ke internet. Hal ini terjadi karena password disimpan secara *cleartext* pada database Rockyou.com menggunakan metode SQL Injection. Pada Juni 2011, NATO mengalami *security breach* yang mengakibatkan 11,000 data pengguna bookshop mereka tersebar ke internet. Kejadian-kejadian tersebut tidak lain dapat terjadi seringkali karena lemahnya pilihan password yang digunakan oleh user yang terdaftar.



*Gambar 1.1 Password yang paling populer digunakan di Rockyou.com*

Pada awal masanya, bruteforce attack membutuhkan waktu yang cukup lama untuk menebak suatu kombinasi password, tools bruteforce attack seperti Cain and Abel dan John the Ripper digunakan untuk menebak password menggunakan tenaga CPU untuk melakukan kerjanya. Untuk menebak satu kombinasi password bisa sampai memakan waktu seharian atau bahkan tahunan.

TOOLS MEDUSA DAN CARA KERJANYA

Dengan semakin berkembangnya teknologi komputer, dan semakin berkembangnya teknologi hardware serta teknologi yang digunakan dalam password cracking membuat bruteforce attack semakin mudah dilakukan dengan proses yang cepat. Salah satunya adalah tools *Medusa* yang merupakan software login brute-force yang modular dan paralel dan mencakup banyak service yang membutuhkan autentifikasi secara *remote*. Beberapa module yang dapat diserang antara lain, FTP, HTTP, IMAP, MySQL, TELNET, SSH, dll.

Cara kerja medusa adalah dengan melakukan kontak ke service yang diinginkan, seperti SSH, Telnet untuk melakukan login menggunakan kombinasi username dan password yang berbeda. Untuk melakukan tes kekuatan password, medusa memerlukan *wordlist* yang berisi semua kemungkinan password yang akan dicoba oleh Medusa untuk login. Banyak *wordlist* gratis ataupun yang komersial di internet seperti hugewordlist.txt yang berisi 3,5 juta kombinasi nama dan nomor, open wall word list collections yang memiliki kombinasi password dari berbagai bahasa, bahkan penyerang sendiri dapat membuat wordlist sendiri menggunakan wordlist yang sudah ada dan dengan menambahkan “mangling” rulse.

Untuk menggunakan medusa, hal hal ini dibutuhkan, yaitu, alamat ip address host yang akan diserang, username dari host yang diserang, textfile yang memiliki list kombinasi password dan spesifik module yang akan diserang (HTTP, SSH, Telnet, atau yang lainnya).

Pada saat dijalankan, medusa akan melakukan *login attempt* untuk setiap password yang ada pada wordlist yang telah dibuat. Penyerangan akan berakhir ketika password berhasil ditebak dan proses autentifikasi sukses dilakukan.

ALGORITMA FAIL2BAN

Dengan adanya kelemahan dan celah keamanan SSH dari serangan bruteforce pastinya akan sangat beresiko jika menggunakan protokol SSH, namun SSH sendiri sangat sulit untuk ditinggalkan penggunanya. Sehingga, harusnya ada penangkal atau *countermeasure*  untuk mengatasi bruteforce attack, salah satunya adalah algoritma **Fail2Ban**.

Fail2ban akan melakukan scan ke log files (contoh : /var/log/auth.log) dan akan melakukan bans kepada IP yang melakukan tanda tanda yang mencurigakan. Tanda tanda mencurigakan ini antara lain adalah terlalu banyak gagal memasukan password, mencari exploit dan lainnya. Umumnya fail2ban akan digunakan untuk mengupdate firewall rules untuk me-reject semua koneksi dari IP address yang terdeteksi selama beberapa waktu. Fail2ban sendiri memiliki berbagai filter untuk service service yang berbeda seperti apache, ssh, courier dan lainnya

Dengan cara ini, fail2ban dapat mengurangi tingkat serangan dari bruteforce attack dengan membatasi jumlah kegagalan login yang terjadi namun tidak dapat secara penuh mengurangi resiko serangan bruteforce attack pada password yang lemah.