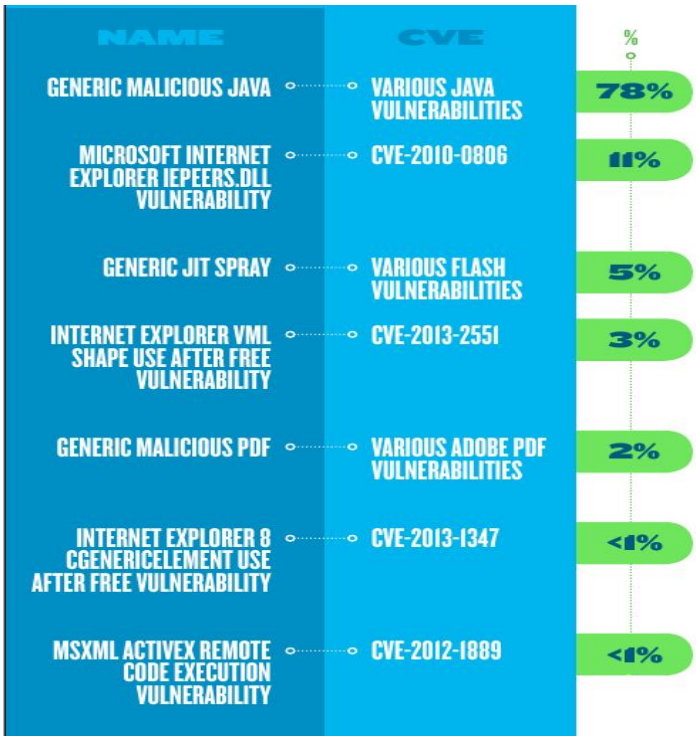
BAB I

PENDAHULUAN

1.1 Latar Belakang

System Administration Networking Security (SANS) *Institute* menyatakan bahwa dalam 5 tahun terakhir jenis serangan *client-side attacks* jumlahnya meningkat secara dramatis. Peningkatan serangan terhadap klien terjadi karena saat ini serangan terhadap *server* semakin sulit dilakukan sehingga penyerang mengalihkan fokus mereka ke sisi klien yang memiliki celah lebih besar karena klien mempunyai perlindungan terhadap sistem yang lebih sederhana daripada *server*. Beragam tujuan yang dimiliki oleh penyerang untuk melakukan jenis serangan tersebut salah satunya adalah untuk mengumpulkan data sensitif seperti informasi rekening, nomor kartu kredit dan informasi lain yang ada pada sistem klien, selain itu sistem klien yang telah dikuasai dapat dimanfaatkan oleh penyerang dengan memanfaatkan sumber daya yang ada pada sistem klien untuk menyerang pihak lain (Shimonski dan Oriyano, 2012).

Menurut *Global Security Report* yang dirilis oleh perusahaan riset keamanan *Trustwave* pada tahun 2014, eksploitasi dengan menggunakan *malicous Java* yang memanfaatkan kerentanan pada *Java* adalah yang paling sering terdeteksi oleh *Trustwave Secure Web Gateway anti-malware technology* dengan persentase sebesar 78% dan sebagian besar penjahat *cyber* mengandalkan *Java applet* sebagai metode untuk mengirimkan *malware* maupun *payload*.



Gambar 1.1 Persentase e*xploit* yang terdeteksi oleh *Trustwave*

Java applet attack method adalah salah satu teknik serangan yang memanfaatkan kerentananan pada *Java* untuk mengeksplotasi sistem *user* dan dapat menyerang ke berbagai sistem operasi termasuk *Windows* 8 yang merupakan sistem operasi keluaran terbaru dari *Microsoft*. Teknik ini menggunakan *malicious Java applet* yang diinjeksikan kedalam *website*. Saat *user* mengakses *website* tersebut dan menjalankan *Java applet* maka tanpa disadari oleh *user* penyerang telah mendapatkan akses ke sistem *user* secara *remote*.

Menyikapi permasalahan tersebut, peneliti mencoba untuk menganalisa serangan tersebut dan hasil dari analisa ini dapat digunakan untuk melakukan antisipasi sehingga sistem dapat bertahan dari serangan tersebut.

1.2 Perumusan Masalah

Perumusan masalah berdasarkan latar belakang tersebut adalah :

1. Bagaimana cara melakukan serangan *remote exploi*t terhadap sistem operasi *Windows* 8 menggunakan *Java applet attack method* sehingga penyerang dapat mengambil alih sistem korban tanpa terdeteksi oleh *firewall* ?
2. Bagaimana mengidentifikasi serangan tersebut sehingga diketahui perilaku maupun karakteristik dari serangan tersebut ?
3. Bagaimana melakukan optimalisasi pada *firewall* sehingga dapat mengantisipasi serangan tersebut ?

1.2 Batasan Masalah

Pembatasan masalah ini dimaksudkan untuk menghindari perluasan pokok masalah sehingga tujuan dari penelitian tercapai. Batasan masalah tersebut diantaranya :

1. Penelitian dilakukan dengan melakukan analisa *runtime* pada sistem yang mendapat serangan untuk mengetahui perilaku dan karakteristik serangan tersebut.
2. Penelitian dilakukan pada sebuah lingkungan kerja yang dibangun untuk digunakan sebagai media ujicoba yang tidak terhubung kedalam jaringan umum untuk menghindari kekacauan yang ditimbulkan oleh serangan tersebut.
3. Langkah-langkah yang diambil untuk melakukan optimalisasi *firewall* pada sistem klien berdasarkan semua informasi dari hasil analisis.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk menganalisa serangan *remote exploit* melalui *Java applet attack method* terhadap sistem operasi *Windows* 8 yang terproteksi *firewall*. Dengan menganalisa serangan tersebut akan diketahui perilaku dan karakterisiknya yang dapat digunakan untuk melakukan antisipasi sehingga sistem dapat bertahan dari serangan tersebut.

1.5 Manfaat Penelitian

1. Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya untuk mengoptimalkan keamanan pada jaringan komputer, khususnya dari serangan *remote exploit* melalui *Java applet attack method.*
2. Memberikan referensi bagi penulisan Karya Ilmiah selanjutnya dan menambah sumber pustaka bagi pengembangan sistem keamanan jaringan.
3. Dapat memberikan referensi dalam mengembangkan kemampuan di kalangan akademis dalam menerapkan perancangan keamanan jaringan komputer.

1.6 Sistematika Penulisan

Adapun sistematika penulisan laporan skripsi terdiri dari :

BAB I PENDAHULUAN

Mendeskripsikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Berisi tentang telaah penelitian terdahulu yang berhubungan dengan penelitian, landasan teori yang berkaitan dengan masalah yang diteliti dalam penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini didalamnya mencakup kegiatan penelitian mulai dari awal sampai akhir, diantaranya adalah: gambaran umum penelitian, alokasi waktu, perangkat yang dibutuhkan, metode penelitian, serta tahapan penelitian.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang hasil daripada penelitian yang dilakukan beserta pembahasannya.

BAB V PENUTUP

Berisi kesimpulan dan saran dari seluruh penelitian yang telah dilakukan.