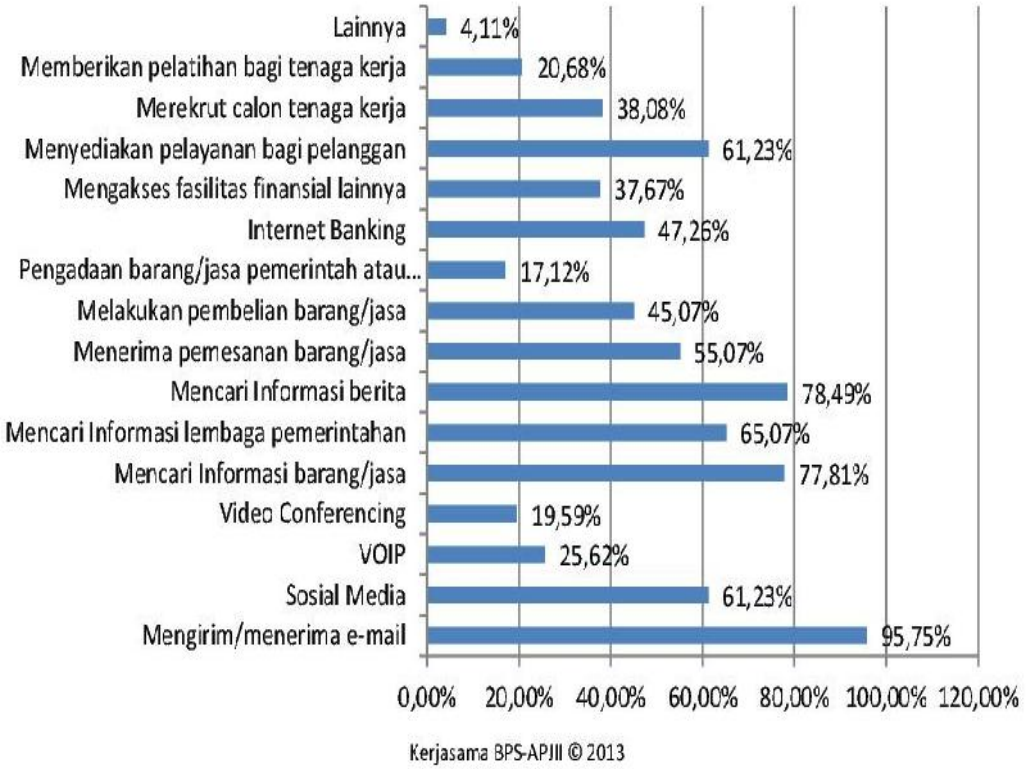
BAB 1

PENDAHULUAN

1.1 Latar Belakang

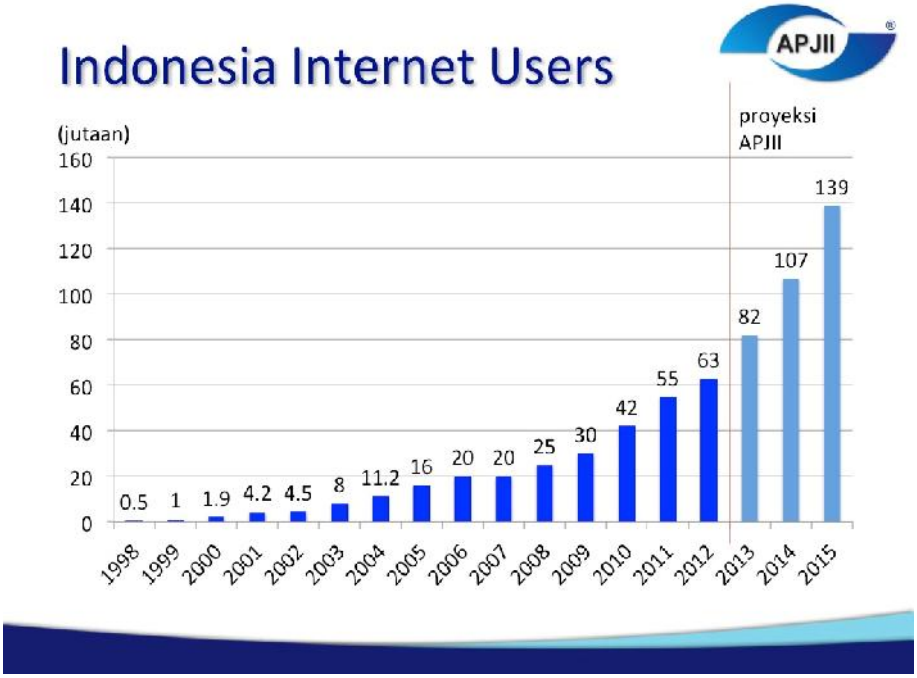
Internet saat ini telah merambah ke hampir semua aspek kehidupan. Hal itu dapat dilihat, misalnya, dari data sebaran bidang pemanfaatan internet di Indonesia yang terdapat di situs APJII (Asosiasi Penyelenggara Jasa Internet Indonesia), sebagaimana yang ditunjukkan di Gambar 1.1.



Gambar 1.1 Sebaran bidang pemanfaatan internet di Indonesia (sumber: apjii.or.id)

Jumlah pengguna internet tiap tahun terus bertambah secara signifikan. Di

Indonesia, misalnya, tercatat 82 juta orang telah menggunakan internet pada tahun 2013, dan angka tersebut diproyeksikan akan meningkat menjadi 107 juta orang dan 139 juta orang pada tahun 2014 dan 2015.



Gambar 1.2 Jumlah pengguna internet di Indonesia (sumber: apjii.or.id)

Di balik kemudahan pengaksesan informasi yang disediakan oleh internet terdapat bahaya besar yang mengintai, yaitu berbagai macam serangan yang berusaha mencari celah dari sistem keamanan jaringan komputer yang digunakan. Serangan-serangan itu dapat mengakibatkan kerusakan data dan bahkan kerusakan pada *hardware* (Syujak, 2012).

Saat ini di Indonesia setiap hari terjadi ratusan ribu serangan terhadap keamanan internet, seperti tindakan menyadap transmisi yang terjadi antara satu pihak dengan pihak yang lain, tindakan yang mengakibatkan terjadinya

pemutusan komunikasi antara dua pihak yang seharusnya berinteraksi, dan tindakan lain yang berpotensi untuk menghancurkan informasi yang berjalan di atas infrastruktur internet. Data dari Id-SIRTII mencatat pada kurun waktu bulan Januari-September 2013 terjadi 42 juta serangan, yang tertinggi terjadi pada tanggal 5 April 2013 yaitu sebesar 517 ribu serangan.

Tabel 1.1 Jumlah serangan terhadap jaringan komputer di Indonesia, dalam jutaan

(sumber: Id-SIRTII.or.id)

Jan	**Feb**	**Mar**	**Apr**	**Mei**	**Jun**	**Jul**	**Ags**	**Sep**
2.4	1.9	10.7	9.9	5.8	3.1	3.8	2	2.4

Perkembangan perangkat lunak ternyata juga menimbulkan resiko keamanan yang besar, hal tersebut dapat dilihat dari kerentanan yang terus muncul dalam perangkat lunak. Menurut laporan CERT/CC, *buffer overflow* merupakan penyebab dari 50% bug keamanan yang dilaporkan dan dijadikan advisori oleh CERT/CC.

Buffer overflow merupakan salah satu penyebab yang paling banyak menimbulkan masalah pada keamanan komputer baik yang bersifat lokal maupun jaringan. *Buffer overflow* adalah suatu keadaan ketika sebuah proses menunjukkan perilaku yang tidak wajar karena data yang disimpan melebihi kapasitas memorinya. Perilaku tersebut bisa menjadi celah keamanan yang dapat dimanfaatkan oleh pihak-pihak yang tak bertanggung jawab untuk menguasai sistem dan memanfaatkannya menurut kehendaknya. Mengingat besarnya kerugian yang dapat disebabkan oleh terjadinya *buffer overflow* maka diperlukan

pengetahuan yang lebih mendalam tentangnya agar dapat dilakukan pengamanan maksimal terhadap sistem yang dipakai.

Karena serangan dapat terjadi kapan saja, dibutuhkan suatu sistem keamanan yang mampu mengenali suatu paket data, apakah data itu asli atau berhubungan dengan serangan. Ketika paket data itu asli maka sistem akan mempersilakannya masuk, tetapi jika paket data tersebut terindikasi serangan maka sistem secara otomatis menghentikannya.

Upaya untuk meningkatkan keamanan jaringan komputer salah satunya adalah dengan *firewall.* Implementasi dari *firewall* ini dapat berupa software atau *hardware* yang bersifat aktif dengan melakukan penyaringan paket data yang lewat berdasarkan pengaturan yang diinginkan. Cara yang lain adalah dengan mengimplementasikan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS). Berbeda dengan *firewall,* IDS adalah sebuah sistem yang digunakan untuk melakukan deteksi adanya usaha-usaha penyusupan (intrusi) terhadap sebuah sistem dengan melakukan pengamatan trafik data secara *real-time,* sedangkan IPS bertugas untuk mengambil keputusan berdasarkan data yang sudah terekam oleh IDS (Syujak, 2012).

Hal-hal yang dikemukakan pada paragraf-paragraf di atas melatarbelakangi penelitian ini. Secara spesifik, penelitian ini akan membahas deteksi dan pencegahan *buffer overflow* terhadap (EFM) Web Server menggunakan Snort. Snort adalah software IDS yang mudah digunakan serta dapat diperoleh secara gratis, sedangkan EFM Web Server adalah software yang masih memiliki celah untuk diserang dengan *buffer overflow*. Dengan demikian kedua software tersebut

dipandang cocok untuk digunakan dalam penelitian ini.

1.2 Rumusan Masalah

Akan dibangun sebuah sistem yang mampu mendeteksi dan mencegah serangan *buffer overflow* terhadap Easy File Management (EFM)Web Server menggunakan Snort.

1.3 Batasan Masalah

Untuk menghindari perluasan pokok masalah sehingga tujuan dari penelitian dapat tercapai sesuai dengan target yang diinginkan maka dilakukan pembatasan masalah sebagai berikut.

1. Sistem yang dibangun hanya digunakan untuk memantau aktivitas jaringan komputer jika terjadi serangan *buffer overflow* terhadap EFM Web Server saja.
2. Sistem yang dibangun menggunakan Snort sebagai *Intrusion Detection System* (IDS) dan *firewall* untuk memblokir IP penyerang.
3. Trafik data yang diamati dalam penelitian ini dibatasi pada paket data yang mengarah pada *server Intrusion Detection System* (IDS) yang berhubungan dengan keamanan *server*.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengidentifikasi bagaimana suatu serangan *buffer overflow* bekerja terhadap EFM Web Server, dan kemudian membuat

penanggulangannya menggunakan Snort.

1.5 Manfaat Penelitian

1. Peneliti mendapatkan khasanah ilmu pengetahuan baru yang belum pernah didapatkan dari perkuliahan.
2. Hasil penelitian ini dapat digunakan sebagai masukan terhadap upaya untuk mengoptimalkan keamanan pada jaringan komputer, khususnya dari serangan *buffer overflow*.
3. Sebagai bahan referensi bagi penulisan karya-karya selanjutnya dan menambah sumber pustaka bagi pengembangan sistem keamanan jaringan berbasis *open source* yang aman.
4. Sebagai bahan referensi bagi para akademisi untuk mengembangkan kreatifitasnya dalam menerapkan perancangan keamanan jaringan komputer.

1.6 Sistematika Laporan Penelitian

Untuk memudahkan pembaca mengikuti laporan ini, maka digunakan sistematika penulisan sebagai berikut.

BAB 1, PENDAHULUAN, berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika laporan penelitian.

BAB 2, TINJAUAN PUSTAKA, berisi telaah tentang penelitian terdahulu yang berhubungan dengan penelitian ini, serta landasan teori yang berkaitan dengan masalah yang diteliti dalam penelitian ini.

BAB 3, METODE PENELITIAN, berisi uraian mengenai kegiatan penelitian mulai dari awal sampai akhir, yang terdiri atas gambaran umum penelitian, alokasi waktu, perangkat yang dibutuhkan, metode penelitian, serta tahapan penelitian.

BAB 4, HASIL DAN PEMBAHASAN, berisi uraian mengenai hasil dari penelitian ini berikut pembahasannya, yang terdiri atas dua tahap yaitu tahap pengujian dan implementasi sistem yang sudah dirancang, serta tahap analisa dari sistem yang sudah dibuat.

BAB 5, PENUTUP, berisi kesimpulan yang diambil berdasarkan hasil penelitian dan pembahasannya tadi, dan diakhiri dengan saran yang insya Allah bermanfaat bagi pihak-pihak terkait.