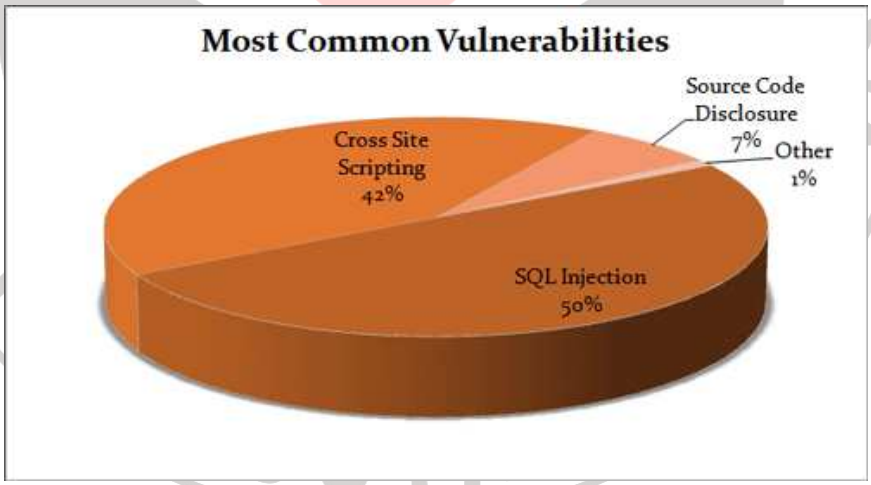
BAB 1. PENDAHULUAN

1.1 Latar Belakang

Ancaman keamanan terhadap penyedia layanan *web* semakin meningkat seiring dengan meningkat pesatnya pemanfaatan *web* sebagai media penyebaran informasi, baik untuk bisnis maupun organisasi *non*-profit. Menurut survey terdapat 70% aplikasi *web* di internet yang *vulnerable* untuk di eksploitasi. Setengah diantaranya berpotensi dari tindakan SQL *Injection* dan 42% cenderung untuk tereksploitasi dengan *Cross Site Scripting* (Acunetix, 2007). Hasil survey lengkap dalam bentuk grafik bisa dilihat pada gambar 1.1 berikut ini.



Gambar 1.1 Grafik Intrusi yang Biasa Terjadi pada Web

Selain potensi serangan pada protokol HTTP, server *provider* juga berpotensi untuk mendapatkan serangan pada protokol SSH yang biasa digunakan untuk *remote login* penggunanya. Perhatian *Network Administrator* untuk melindungi SSH adalah dari serangan *bruteforce login*. Yaitu percobaan *login* dengan kombinasi *username* dan *password* berbeda secara terus-menerus yang dikhawatirkan akan mengganggu kelangsungan layanan server.

Sebenarnya untuk mengantisipasi hal tersebut telah dikembangkan program pendeteksi intrusi atau lebih dikenal dengan nama *Intrusion Detection System* (IDS). Tetapi seiring dengan perkembangan teknologi keamanan jaringan, IDS dianggap tidak efisien mengingat cara kerjanya yang pasif. Sesuai dengan namanya, IDS hanya mendeteksi serangan yang terjadi. Semua yang terdeteksi dilaporkan kepada *Network Administrator* untuk kemudian dilakukan tindak lanjut terhadap serangan yang terdeteksi.

Beberapa tahun belakangan ini, dikembangkan IDS yang proaktif terhadap intrusi. Lebih dikenal dengan sebutan *Intrusion Prevention System* (IPS). Sistem ini bisa mencegah terjadinya intrusi terhadap serangan yang terdeteksi dengan berbagai cara (Scarfone, 2007). Dari sini dapat disimpulkan bahwa IPS lebih efisien karena IPS bisa secara otomatis melakukan tindakan preventif tanpa campur tangan *Network Administrator*.

Namun cara kerja IPS/IDS mendeteksi intrusi sering kali menimbulkan *false positive* (kesalahan mendeteksi). Jika terdeteksi *false positive* di IDS, mungkin tidak

menjadi masalah yang fatal karena keputusan pemblokiran tetap ada pada *Network Administrator*. Tetapi jika *false positive* terdeteksi di IPS yang proaktif, dikhawatirkan dapat merugikan pihak *host* yang menjadi korban pemblokiran. Bahkan dapat merugikan pihak penyedia layanan konten pada server yang proaktif tersebut. Hal ini dapat mengakibatkan efek samping, yaitu kredibilitas penyedia layanan konten *web* bisa menurun dikarenakan server dianggap *down* oleh *host* yang menjadi korban pemblokiran.

1.2 Rumusan Masalah

Rumusan masalah dalam perancangan ini adalah:

1. Bagaimana cara IDS memilah *request* yang termasuk serangan atau bukan dari *client*?
2. Bagaimana cara mengkombinasikan IDS dengan *Firewall* pada sistem operasi server sehingga menjadi sebuah IPS yang andal?
3. Bagaimana mengembangkan IPS yang memiliki statistik serangan dari *host* tertentu? Untuk selanjutnya jika jumlah kumulatif serangan lebih dari batas toleransi akan di anggap *host blacklist* dan diblokir permanen?
4. Bagaimana cara me-*redirect traffic* menuju Honeypot server?
5. Bagaimana cara merekayasa *source* IP *address header* paket yang sebenarnya berasal dari Honeypot server tapi dibuat seakan-akan berasal dari server asli?

6. Bagaimana mengembangkan Honeypot yang interaktif dan *vulnerable* sebagai tempat interaksi sementara bagi *host* penyerang? Untuk selanjutnya segala aktifitas *attacker* akan direkam untuk dijadikan keputusan *Network Administrator*, apakah termasuk intrusi atau tidak? Selain itu juga Honeypot akan dimanfaatkan sebagai *knowledge base* terhadap jenis pola serangan baru yang mungkin diperagakan *attacker* terhadap Honeypot Server (server palsu).
7. Demi kemudahan manajemen dan keamanan server, bagaimana cara agar yang diizinkan mengakses *port* tertentu pada server hanya IP *address* atau subnet tertentu saja?
8. Bagaimana mengamankan server dari serangan *bruteforce* menuju *port* tertentu?

1.3 Batasan Masalah

Batasan masalah yang diteliti meliputi:

1. IPS yang akan dikembangkan hanya dapat berjalan di sistem operasi GNU/Linux karena akan memanfaatkan IPTables sebagai *firewall* bawaan yang hanya ada pada sistem operasi tersebut.
2. Layanan server yang diteliti dibatasi pada protokol SSH dan HTTP. Hal ini sudah mencakup masalah yang melatarbelakangi penelitian. Proteksi terhadap SSH server dengan melakukan pencegahan terhadap aktifitas SSH *bruteforce attack*. Sedangkan proteksi terhadap intrusi secara umum difokuskan pada HTTP Server.

3. Untuk percobaan intrusi dari jaringan internal (*trusted network*) tidak dianggap sebagai intrusi. Demi kemudahan *Network Administrator* dalam memilah ratusan/ribuan *alert* yang mungkin saja dapat dideteksi dan direspon oleh IPS.
4. IPS tidak mendeteksi paket diluar *signature*-nya sebagai paket *malicious*. Dengan kata lain, sistem IPS bukan merupakan sistem yang *heuristik*.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah membangun IPS yang bekerja secara proaktif melakukan pencegahan terhadap aktifitas intrusi. Namun memiliki toleransi dari statistik jumlah serangan yang terdeteksi.

Selain itu juga akan dibangun sebuah Honeypot sebagai tempat interaksi sementara bagi *host* yang dicurigai melakukan intrusi untuk selanjutnya dianalisis oleh *Network Administrator*. Sehingga meminimalisir terjadinya *false positive* juga sebagai bahan pembelajaran bagi *Network Administrator* terhadap jenis pola serangan baru yang mungkin dilakukan oleh *attacker*.

1.5 Manfaat Penelitian

Manfaat yang bisa diambil dari penelitian ini adalah:

1. Melindungi server terhadap intrusi. Sehingga dapat membuat server tetap dalam kondisi aman dan bisa menjalankan layanan sebagaimana mestinya, tanpa gangguan dari luar.

2. Menganalisa *log* aktifitas *host* yang dicurigai terhadap server palsu (Honeypot). Apakah benar-benar termasuk kegiatan intrusi yang dapat mengganggu keberlangsungan layanan pada server. Serta dapat mempelajari jenis pola serangan baru yang mungkin saja dilakukan oleh *attacker* sehingga kedepannya dapat dilakukan *patching* oleh *Network Administrator* terhadap server asli.
3. Produk yang dikembangkan oleh penulis bisa dimanfaatkan di server penyedia layanan hostingan *web*. Mengingat intrusi yang dicegah adalah intrusi terhadap protokol HTTP (*web*) dan SSH, dua protokol yang biasa terdapat pada layanan hostingan *web*.

1.6 Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut:

1. **BAB I PENDAHULUAN**

   Bab ini meliputi pembahasan masalah secara umum meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

2. **BAB II TINJAUAN PUSTAKA**

   Bagian ini memuat landasan teori yang berfungsi sebagai sumber atau alat dalam memahami permasalahan yang berkaitan dengan teori IDS, *Firewall*, IPS, dan Honeypot.

3. BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran dari metode pengembangan IDS/IPS dan Honeypot. Mencakup analisis, desain model topologi, serta peran IPS dan Honeypot dalam memproteksi server dari kegiatan intrusi.

4. BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Pada bagian ini akan dibahas secara mendalam hal-hal yang akan menjawab apa yang sudah dirumuskan dalam rumusan masalah.

5. BAB V KESIMPULAN DAN SARAN

Kesimpulan merupakan jawaban atas rumusan masalah dalam penelitian dan juga intisari dari BAB IV. Rekomendasi pengembangan sistem penulis diutarakan pada sub bab Saran.