

BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet menjadi kebutuhan yang semakin berkembang dimasa ini, bahkan hampir setiap rumah terdapat anggota keluarga yang mengerti penggunaan *internet*. Sekarang hampir setiap sekolah, lembaga pemerintahan, bahkan organisasi masyarakat memiliki akses *internet*. Namun disamping memberikan kemudahannya, *internet* juga memiliki dampak yang kurang baik. Sering terjadinya penipuan, memuat konten dewasa, pencurian data pribadi atau intansi, bahkan serangan dari *hacker* yang masih sering terjadi.

Peningkatan sistem keamanan adalah suatu hal yang mutlak harus dilakukan oleh *administrator* jaringan. Penggunaan *Intrusion Prevention System* (IPS) dapat membantu *administrator* menangani masalah keamanan jaringan. Salah satu software IPS yang dapat digunakan adalah *IPS Suricata*, *software IPS open source* yang dapat digunakan pada jaringan dengan kinerja tinggi. *IPS Suricata* dapat memberikan *alert* ketika terjadi serangan kepada *Server* atau jaringan. Namun terkadang dalam suatu area jaringan terdapat lebih dari satu *Server* atau jaringan yang harus dilindungi, sehingga untuk melakukan pemantauan akan menyulitkan *administrator* jaringan.

Untuk mempermudah *administrator* jaringan dalam melakukan pemantauan, dibutuhkan suatu perangkat yang dapat memantau, dan melakukan tindakan kepada setiap IPS yang bertugas mengamankan masing-masing jaringan atau *Server*. *Android* merupakan sistem operasi untuk perangkat *smartphone* atau *tablet* yang saat ini paling banyak digunakan. *Android* juga memiliki performa yang tinggi dalam melakukan akses *internet*. Dengan menggunakan *Android*, *administrator* jaringan dapat melakukan pengawasan bahkan dari jarak yang jauh dari IPS. Ketika terjadi serangan, IPS akan memberikan pemberitahuan kepada *Android* untuk selanjutnya dilakukan penanganan terhadap serangan yang terjadi.

Berdasarkan latar belakang diatas, penulis akan melakukan penelitian dengan judul “Perancangan Sistem *Monitoring* Aktif Berbasis *Android* Pada *Intrusion Prevention System* (IPS) *Suricata*”. Penulis menggunakan *IPS Suricata* karena bersifat *open source* namun memiliki performa yang tinggi dalam melakukan analisa jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasalahan diatas, maka penulis merumuskan permasalahan pada penelitian ini sebagai berikut:

1. Bagaimana melakukan *monitoring* secara *realtime* terhadap komputer *IPS Suricata* dengan perangkat *Android*.
2. Bagaimana memberikan perintah dan *update rule* kepada *IPTables* dengan menggunakan *Android*.
3. Bagaimana mendeteksi adanya serangan yang menuju *server local* dengan *IPS Suricata*.
4. Bagaimana mengirimkan *alert* pada perangkat *Android* tentang serangan yang terjadi pada jaringan.
5. Bagaimana melakukan pemblokiran pada *IP Address* penyerang.

1.3 Tujuan dan Manfaat Penelitian

Tujuan dan manfaat yang diperoleh dalam penelitian ini adalah sebagai berikut.

1.3.1 Tujuan

Berdasarkan perumusan masalah diatas, maka tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

1. Melakukan *monitoring* terhadap *IPS Suricata* secara *realtime* dengan perangkat *Android*.
2. Memberikan perintah dan *update rule* kepada *IPTables* dengan menggunakan perangkat *Android*.
3. Melakukan analisa paket data yang menuju *Server Local*, dan mendeteksi adanya serangan dengan *IPS Suricata*.
4. Mengirimkan *alert* pada perangkat *Android* tentang serangan yang terjadi pada jaringan.
5. Melakukan pemblokiran pada *IP Address* penyerang.

1.3.2 Manfaat

Adapun manfaat yang diharapkan oleh penulis dari penelitian ini adalah sebagai berikut:

1. Memberikan kemudahan dalam melakukan pengawasan dan memberikan perintah kepada *IPS Suricata* secara *realtime* dengan perangkat *Android*.
2. Dapat mendeteksi paket data yang dianggap sebagai ancaman pada *server* atau jaringan.

3. Diharapkan dapat mempercepat penanganan ancaman yang terjadi.

1.4 Batasan Masalah

Dalam penelitian ini, agar penulis dapat melakukan penelitian secara terarah dan tidak menyimpang, serta sesuai dengan yang telah penulis rencanakan. Maka penulis membuat batasan-batasan masalah untuk penelitian ini sebagai berikut:

1. Penulis menggunakan *IPS Suricata* untuk melakukan analisa pada *traffic* paket data yang menuju ke *server*.
2. Deteksi serangan menggunakan metode *signature-based*, yang berarti serangan yang dapat dicegah hanya berdasarkan aturan-aturan *IPS Suricata*.
3. Penulis menggunakan *tools* penguji serangan seperti:
 - a. *Nmap* untuk melakukan *scanning* pada *port* yang terbuka.
 - b. *Nikto* untuk melakukan deteksi kelemahan pada *web server*.
 - c. *Superscan* untuk melakukan *scanning port* yang terbuka.
 - d. *Havij* untuk melakukan *SQL injection* pada suatu *website*.
4. Perangkat *Android* hanya akan memberikan *alert* tentang serangan yang terjadi dan kondisi *IPS Suircata* ketika perangkat terkoneksi *internet* dengan kecepatan tinggi.
5. *Monitoring Agent* dapat melakukan *update* informasi ke *web server* hanya bila terdapat koneksi *internet* yang stabil.
6. *Web server* menggunakan layanan *hosting* pada *NiagaHoster*.

1.5 Metode Penelitian

Pada penelitian ini penulis menerapkan metode penelitian yang bersifat eksperimen. Adapun langkah-langkah yang diterapkan penulis dalam melakukan penelitian adalah sebagai berikut.:

1. Tahap Pertama (Analisa)

Merupakan tahapan dimana penulis melakukan pengamatan dan identifikasi terhadap masalah yang menjadi objek penelitian penulis. Serta melakukan pengumpulan referensi yang

dibutuhkan oleh penulis yang dapat diperoleh dari buku, jurnal, artikel, dan lain-lain.

2. Tahap Kedua (Merancang Sistem)

Merupakan tahapan dimana penulis telah mengerti permasalahan untuk kemudian membuat rencana untuk menyelesaikan permasalahan. Terdapat tiga hal yang akan dilakukan oleh penulis dalam merancang sistem yaitu sebagai berikut:

a. Perancangan Hardware

Dalam tahapan ini, penulis menentukan jumlah hardware yang dibutuhkan dalam melakukan penelitian dan ketersediaannya.

b. Perancangan Software

Dalam tahapan ini, penulis melakukan beberapa hal yaitu:

- Membuat diagram alur kerja dari sistem.
- Melakukan perancangan antarmuka sistem.

c. Perancangan Jaringan

Dalam tahapan ini, penulis menentukan rancangan jaringan, koneksi, dan *topologi* yang digunakan.

3. Tahap Ketiga (Penerapan Sistem)

Tahap selanjutnya yaitu penulis melakukan penerapan dari hasil perancangan sistem yang telah dibuat. Adapun yang akan dilakukan oleh penulis adalah:

a. Konfigurasi IPS *Suricata*

Pada tahap ini penulis melakukan installasi dan konfigurasi IPS *Suricata* pada komputer yang akan digunakan sebagai *agent* yang melakukan pengawasan terhadap lalu lintas jaringan yang menuju ke *server*.

b. Membuat Agen IPS

Pada tahap ini penulis akan melakukan pembuatan program yang akan menjadi *agent*. *Agent* ini berfungsi untuk melakukan *update* informasi dari IPS kepada *web server* dan menjalankan perintah-perintah yang dikirimkan oleh *user* melalui perangkat *Android*.

c. Membuat Web Service Pada Web Server

Pada tahap ini penulis akan melakukan pembuatan *web service* pada *web server* yang akan berfungsi sebagai penerima informasi dari agen yang terdapat di IPS. Dan sebagai tempat dimana perangkat Android melakukan pengambilan data.

d. Membuat Aplikasi Android

Pada tahap ini penulis akan melakukan pembuatan aplikasi yang akan mengambil data dari *web server* tentang IPS yang dimonitoring. Aplikasi ini juga akan dapat mengirimkan perintah untuk kemudian akan dijalankan pada IPS.

4. Tahap Keempat (Pengujian)

Pada tahap ini penulis akan melakukan pengujian dan melakukan evaluasi dari hasil penelitian yang telah dilakukan sesuai dengan implementasikan pada sistem.

5. Tahap Kelima (Menyusun Laporan)

Pada tahap ini penulis akan melakukan penulisan terhadap hasil yang didapat dari tahap analisa sampai pada pengujian dari penelitian yang dilakukan.

1.6 Sistematika Penulisan

Berikut merupakan sistematika penulisan laporan yang digunakan penulis pada tugas akhir ini yaitu:

BAB I PENDAHULUAN

Pada bab ini, penulis menjelaskan latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II STUDI PUSTAKA

Pada bab ini, penulis menjelaskan penelitian sebelumnya dan dasar teori yang digunakan untuk mendukung penelitian yang dilakukan penulis dalam tugas akhir ini.

BAB III PERANCANGAN SISTEM

Pada bab ini, penulis menjelaskan tentang rancangan sistem pada IPS, *Agent*, *Android*, *Web Server*, dan *Database* yang dibangun serta arsitektur jaringan dan simulasi serangan yang akan dilakukan oleh penulis.

BAB IV IMPLEMENTASI SISTEM

Pada bab ini, penulis menjelaskan kebutuhan sistem dan implementasi metode. Kemudian penulis melakukan uji coba dan analisa terhadap sistem yang sudah diimplementasikan, sesuai dengan simulasi serangan yang telah dirancang oleh penulis.

BAB V PENUTUP

Pada bab ini, penulis menjelaskan kesimpulan dari hasil uji coba terhadap sistem serta memberikan saran yang dapat dijadikan pertimbangan untuk penelitian berikutnya.