BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan jaringan kini menjadi hal utama yang dibutuhkan untuk mengamankan setiap data. Karena semakin berkembangnya teknologi informasi maka serangan yang dilakukan oleh penyerang juga sangat bermacam-macam. Salah satu serangan yang sering dilancarkan serta tergolong mudah untuk diimplementasikan adalah DoS. Serangan DoS memiliki berbagai macam metode dan biasanya memanfaatkan sumber daya target dengan cara menghabiskan sumber daya servernya sehingga tidak bisa diakses atau mengalami *down*. Berdasarkan survey yang dilakukan oleh salah satu situs perusahaan keamanan jaringan yaitu kapersky lab menyatakan sepanjang tahun 2017 hingga 2018 serangan DoS terus meningkat di berbagai negara, adapun serangan yang dilancarkan dikelompokkan menjadi beberapa jenis seperti pada table 1.1.

Tabel 1. 1 Hasil Survey Serangan DoS Berdasarkan Jenisnya

SYN	ICMP	TCP	HTTP	UDP
57,30%	6,10%	14,70%	8,80%	6,10%

Untuk mencegah resiko terkena serangan, maka dibutuhkan langkah dalam pencegahan dengan suatu sistem untuk mengamankan jaringan agar tidak menjadi target seorang penyerang yang bisa merugikan. Salah satu sistem yang dapat digunakan untuk mencegah resiko terkena serangan yaitu *Intrusion Detection System* (IDS) yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah jaringan dan memberikan sebuah peringatan kepada administrator[1][2][3][4].

Metode deteksi dari IDS terbagi menjadi 2, yaitu *Signature-Based Detection* dan *Anomaly-Based Detection*[1]. Pada penelitian sebelumnya [4][5] telah dilakukan analisis terhadap metode deteksi *signatured-based* yang mampu mendeteksi bermacam-macam *malware* dengan waktu pendeteksian yang relatif cepat serta hasil yang cukup akurat, tetapi kelemahan dalam deteksi *signature-*

based yaitu tidak dapat mendeteksi pola serangan baru dan selalu memerlukan pembaruan *rules database* secara manual, sehingga dalam penelitian ini mengusulkan untuk membangun sebuah sistem IDS dengan melakukan analisis menggunakan metode deteksi serangan *Anomaly-based* agar dapat mendeteksi serangan yang mencurigakan dan tidak normal bagi sistem tanpa harus melakukan *update rules* secara manual.

1.2 Tujuan dan Manfaat

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Melakukan simulasi sistem keamanan IDS untuk melindungi jaringan,
2. Mengetahui akibat dari berbagai *tools* serangan DoS terhadap Web Server serta FTP Server,
3. Mengetahui performansi efektivitas system yang telah dibangun terhadap serangan DoS.

Selain itu, manfaat dari penelitian ini adalah sebagai berikut:

1. Dapat menganalisa kinerja IDS dalam memonitoring serangan dari luar serta trafik yang masuk kedalam jaringan dengan memanfaatkan sistem IDS,
2. Mendapatkan peringatan jika terdapat serangan maupun aktivitas yang dianggap mencurigakan yang masuk ke dalam jaringan,
3. Dapat melakukan pencegahan sebelum terjadi serangan.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, perumusan masalah yang dapat diuraikan adalah sebagai berikut:

1. Bagaimana melakukan simulasi sistem keamanan IDS menggunakan metode deteksi *Anomaly-Based?*
2. Bagaimana akibat dari setiap *tools* serangan DoS terhadap target*?*
3. Bagaimana hasil performansi dari system yang telah dibangun berdasarkan pendeteksian serangan DoS?

1.4 Batasan Masalah

Agar dalam pengerjaan proposal ini mendapatkan hasil yang optimal, maka masalah akan dibatasi sebagai berikut:

1. Sistem yang dibangun merupakan Network-IDS menggunakan tools *Zeek* yang dapat mendeteksi metode *Anomaly-Based* secara otomatis.
2. IDS dibangun didalam OS utama Linux Ubuntu 16.04.
3. Target akan dibangun didalam sebuah mesin virtual dengan OS Linux Ubuntu 16.04.
4. Server yang digunakan sebagai target adalah Web Server serta FTP Server
5. Pengujian serangan berupa DoS menggunakan Kali Linux.
6. Analisis yang dilakukan yaitu melihat akibat serangan DoS dengan memasang IDS dan tanpa memasang IDS.

1.5 Metode Penelitian

Dalam melaksanakan implemenatasi proposal ini, metode yang akan digunakan adalah sebagai berikut:

1. Identifikasi masalah

   Melakukan identifikasi masalah untuk mengatasi serangan yang dilakukan pihak luar berupa metode deteksi *Anomaly-Based* yang akan dianalisis.
2. Studi Literatur

   Melakukan proses pencarian semua informasi yang dibutuhkan dan referensi dari jurnal, buku, artikel, maupun diskusi langsung dengan dosen yang berkaitan dengan topik *Intrussion Detetction System* (IDS) untuk mendeketsi *Anomaly-Based.*
3. Perancangan sistem

   Melakukan perancangan sistem yang akan digunakan untuk mendeteksi *Anomaly-Based* serta kemungkinan untuk diimplementasikan.
4. Implementasi sistem

   Melakukan implementasi sesuai dengan hasil perancangan yang telah dibuat serta *tools* yang telah ter*install* berdasarkan metode *Anomaly-Based* serta mengumpulkan data-data yang telah ditentukan dari pengujian implementasi.

5. Pengujian dan Analisis Sistem

   Melakukan pengujian terhadap sistem yang dibuat berupa serangan DoS terhadap sistem untuk mengetahui performansi dari metode deteksi *Anomaly-Based* dan melakukan analisis terhadap hasil dari pengujian sistem yang telah dibuat.

6. Pembuatan Laporan

   Melakukan pembuatan laporan berdasarkan data yang didapat dari analisis sistem serta dokumentasi yang telah dilakukan sebagai tahap akhir dari penelitian.