BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Jaringan *internet* dan *server* memiliki peran sentral dalam mempermudah akses informasi, berbagi data, dan meningkatkan efisiensi kinerja di perusahaan maupun individu. Melalui jaringan komputer seperti LAN, WAN, dan MAN, terjadi konektivitas dan interaksi antara perangkat secara lokal maupun global via *internet*, di mana *server* berfungsi sebagai inti utama dalam menyediakan layanan dan mengelola data [1][2]. Namun, dengan adanya koneksi yang lebih luas menjadikan *server* rentan terhadap berbagai ancaman keamanan, terutama dari serangan DDoS dengan jenis serangan seperti SYN TCP *Flood* dan UDP *Flood*. Tujuan dari serangan ini adalah untuk menargetkan sumber daya *server* suatu sistem atau situs *web* korban, sehingga tidak mampu diakses atau melayani permintaan (*request*). Akibatnya terjadi pengiriman data yang lambat, rusak, atau bahkan tidak sampai ke tujuan. Masalah lain yang sering terjadi adalah terjadinya *time-out* pada komunikasi, serta masalah keamanan [3][4].

Permasalahan tersebut disebabkan oleh *client* nakal yang berniat ingin menurunkan kinerja *server*, disisi lain belum diterapkannya sistem keamanan pada *server* [5]. Jika merujuk pada limitasi dari penelitian 10, bahwa penelitian 10 menggunakan *OPNSense* sebagai *firewall* sudah mampu melakukan *Blocking* terhadap serangan DoS, namun *OPNSense* masih belum mampu mencatat *log* serangannya. Kemudian dari penelitian 10 menyarankan pengembangan untuk membangun sistem *firewall* dan *Intrusion Detection System* (IDS). Maka dari itu, pada penelitian ini menggunakan Snort sebagai IDS dan *pfSense* sebagai *firewall* sekaligus mampu memberikan *alert* dan disimpan dalam bentuk *log*. Selanjutnya, jika merujuk pada limitasi pada penelitian 11, bahwa pada penelitian 11 dilakukan pemblokiran IP secara manual melalui pesan *firewall rules bot telegram*. Kemudian dari penelitian 11 menyarankan pengembangan dalam upaya pembuatan bot *Telegram* yang lebih *responsive*. Maka dari itu, pada penelitian ini dilakukan pemblokiran IP secara otomatis melalui *pfSense*, artinya ada pengembangan efektif

atau efisiensi waktu bagi *network administrator* dalam melakukan pencegahan melalui pemblokiran IP.

Oleh sebab itu, pada penelitian ini menggunakan Snort sebagai *tools* untuk mendeteksi serangan DDoS jenis SYN TCP *Flood* dan UDP *Flood*. Snort nantinya akan mendeteksi serangan menggunakan *custome rules* dari pengguna sesuai dengan kedua jenis serangannya, jika lalu lintas jaringan cocok dengan *rules* maka peringatan (*alert*) muncul dan teridentifikasi sebagai serangan. Kemudian dari *alert* akan otomatis terintegrasi dengan *pfSense* sebagai *tools Firewall* untuk melakukan *blocking* IP. Setelah sistem IDS dan *Firewall* terintegrasi dengan baik, selanjutnya melakukan pengembangan dengan membangun notifikasi *email* kepada *admin* untuk mengetahui riwayat aktivitas serangan melalui *log* Snort dan kebutuhan analisis [6][7].

Setelah deteksi dan pencegahan dilakukan, maka pada penelitian ini juga melakukan evaluasi kinerja pada Snort, melalui pengukuran berdasarkan parameter akurasi deteksi, kecepatan deteksi, efektivitas deteksi, dan penggunaan sumber daya. Evaluasi kinerja Snort berdasarkan nilai *confusion matrix* dengan pengukuran metode klasifikasi *log* Snort dari parameter akurasi dan efektifitas deteksi. Kemudian Evaluasi kinerja Snort berdasarkan nilai Standar deviasi dengan metode *detection latency* dari parameter kecepatan deteksi dan metode CPU *Usage* dari parameter penggunaan sumber daya. Keempat parameter menggunakan skenario DDoS dan skenario Normal.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian ini adalah:

1) Bagaimana implementasi deteksi dan pencegahan terhadap serangan yang terjadi?
2) Bagaimana implementasi notifikasi serangan yang terjadi?
3) Bagaimana kinerja Snort melalui *confusion matrix* dari metode klasifikasi dan dua skenario terhadap parameter akurasi deteksi dan efektivitas deteksi?

4) Bagaimana kinerja Snort melalui standar deviasi dari metode *detection latency* terhadap parameter kecepatan deteksi dan CPU *Usage* terhadap penggunaan sumber daya melalui dua skenario?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1) Pengujian akan dilakukan secara simulasi.
2) *Software* yang akan dilakukan pengujian adalah Snort dan *pfSense*.
3) Pengklasifikasian dilakukan melalui *Software Orange*.
4) Sistem deteksi akan dikembangkan dengan membangun notifikasi peringatan melalui *Email*.
5) Pada penelitian ini menggunakan EVE-NG sebagai perancangan topologi keamanan *server* dalam deteksi dan pencegahan serangan DDoS.
6) Mekanisme keamanan jaringan yang digunakan adalah IDS dan *Firewall*.
7) Snort sebagai IDS dan *pfSense* sebagai *Firewall*.
8) Analisis kinerja Snort berdasarkan dua skenario, yaitu DDoS dan Normal.
9) Pengujian menggunakan empat jenis lalu lintas yaitu TCP *Flood,* UDP Flood, TCP Normal, serta UDP Normal.
10) Parameter pengujian meliputi akurasi deteksi, efektivitas deteksi, kecepatan deteksi, dan penggunaan sumber daya.
11) Klasifikasi *log* Snort menggunakan Algoritma *Decision Tree*.
12) Atribut klasifikasi yang digunakan yaitu Protokol, IP Sumber, *Port* Sumber, IP Tujuan, *Port* Tujuan, Label.
13) *Confusion matrix* merujuk pada parameter akurasi dan efektifitas deteksi, sedangkan Standar Deviasi merujuk pada parameter kecepatan deteksi dan penggunaan sumber daya.
14) Klasifikasi mengacu pada parameter akurasi dan efektifitas deteksi, *Detection latency* mengacu pada parameter kecepatan deteksi, CPU *Usage* mengacu pada parameter penggunaan sumber daya.

15) Evaluasi kinerja Snort melalui nilai *Confusion matrix* dan Standar Deviasi.
16) Perhitungan pada *Confusion matrix* meliputi *Accuracy*, *Precision*, *Recall*, *Specificity*, *F1-Score*, serta FPR.

1.4 TUJUAN

Tujuan dari penelitian ini adalah:

1) Analisis cara deteksi dan pencegahan dari serangan DDoS.
2) Analisis cara mengirimkan notifikasi peringatan kepada *network administrator* dari serangan yang terjadi.
3) Analisis nilai kinerja Snort melalui klasifikasi *log* Snort dari dua skenario terhadap parameter akurasi deteksi dan efektivitas deteksi.
4) Analisis nilai kinerja Snort melalui Standar Deviasi dari dua skenario terhadap parameter kecepatan deteksi dan penggunaan sumber daya.

1.5 MANFAAT

Penelitian ini diharapkan dapat memberikan gambaran proses deteksi dan pencegahan serangan DDoS menggunakan Snort dan *pfSense* serta notifikasi *Email* sebagai media pengiriman log aktivitas serangan maupun normal kepada *admin* untuk mempermudah dalam *monitoring* sistem keamanan *server*. Mekanisme keamanan jaringan IDS dan *Firewall* yang diharapkan nantinya dapat mendeteksi melalui custome rules dan memblokir IP serangan DDoS. Selain proses deteksi dan pencegahan, diharapkan dapat mengetahui kinerja Snort melalui parameter akurasi deteksi, efektivitas deteksi, kecepatan deteksi dan penggunaan sumber daya.

1.6 SISTEMATIKA PENULISAN

Penelitian ini terbagi menjadi beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, manfaat dan tujuan penelitian, Batasan masalah dan sistematika penulisan. Bab 2 membahas tentang konsep jaringan komputer, konsep *server*, konsep IDS, konsep Snort, konsep DDoS, konsep *firewall*, dan konsep *Email notification*. Cara penelitian seperti alat yang digunakan, alur penelitian, perancangan topologi, konfigurasi *software*, pengujian topologi, dan skenario

pengujian serta cara pengambilan data dibahas pada bab 3. Bab 4 membahas tentang hasil simulasi dan analisis sistem berdasarkan hasil simulasi. Kesimpulan dan saran pengembangan tesis untuk kedepannya dideskripsikan pada bab 5.