BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Teknologi Informasi saat ini semakin pesat,salah satunya adalah Internet, jaringan internet digunakan banyak orang untuk berkomunikasi, bertukar informasi maupun melihat berita terkini. Pengguna Internet tiap harinya semakin bertambah, mulai dari anak-anak sampai orang dewasa. Karena mengakses jaringan Internet saat ini sangat mudah dan murah, bisa melalui PC/Laptop dan Smarthphone. Untuk melakukan semua itu maka di butuhkan sebuah Server dan administrator Server untuk memperhatikan keamanan data di dalam Server tersebut. Maka harus dilakukan pengawasan untuk orang yang tidak bertanggung jawab yang menyusup ke dalam Server tersebut.

Serangan yang paling sering digunakan adalah Port Scanning dan DOS (Denial Of Service). Port Scanning adalah serangan yang bekerja untuk mencari port yang terbuka pada suatu jaringan komputer. dari hasil port scanning akan di dapat letak kelemahan sistem jaringan komputer tersebut. DOS adalah serangan yan g bekerja dengan cara mengirimkan request ke server berulang kali untuk bertujuan membuat server menjadi sibuk menanggapi request dan server akan mengalami kerusakan atau hang (Renuka P, Dr Annamma, Suhas.V, Kundan Kumar, 2010).

Guna mengamankan dan mencegah dari serangan *Ddos* (*Distributed Denial Of Service*) perlu adanya penerapan system dalam sebuah jaringan

tersebut dengan menggunakan Suricata sebagai aplikasi *Network Intrusion Detection System* (NIDS) dan Iptables.

Menurut Brian Cusack dalam jurnalnya yang berjudul *Acquisition of Evidence from Network Intrusion Detection Systems*, disimpulkan bahwa Suricata mampu mendeteksi aktivitas mencurigakan dan mengumpulkannya menjadi *evidence* yang dapat digunakan sebagai antisipasi serangan berikutnya (Cusak, 2013).

Sedangkan Iptables akan membatasi paket data yang masuk dengan menggunakan *–hashlimit-upto* dalam membatasinya. Pada penelitian ini akan membahas kinerja sistem dalam mengatasi dan membatasi *Ddos TCP Flood* dengan menggunakan *iptables –hashlimit-upto* dengan nilai 50, 500, 5000, 50000 dan 100000, yang kemudian di analisa setiap sekali pengujian dengan 10 kali serangan mana yang stabil digunakan untuk membatasi serangan *TCP Flood* sehingga tidak membebani penggunaan *resource* CPU server.

1.2 Rumusan Masalah

Dari latar belakang diatas dapat disimpulkan bahwa *Ddos TCP Flood* ini akan berdampak pada penggunaan *resouce* server yang berlebihan sehingga menyebabkan kinerja server menjadi lambat dalam menanggapi request tersebut.

1.3 Batasan Masalah

Batasan masalah penelitian yang dilakukan adalah :

1. Penelitian hanya berfokus untuk menganalisa hasil dari batasan serangan *Ddos TCP Flood* dengan menggunakan *iptables –hashlimit-upto* dengan nilai telah yang ditentukan.
2. Menggunakan Linux Ubuntu sebagai server IDS (*Intrusion Detection System*) .
3. Menggunakan aplikasi IDS (*Intrusion Detection System*) Suricata.
4. Penyerangan menggunakan 2 IP berbeda.
5. Menggunakan aplikasi LOIC untuk *Ddos* nya.
6. Menggunakan mode *faster* di aplikasi LOIC nya.
7. Penyerangan yang digunakan adalah, *Ddos TCP Flood.*
8. Pengujian pertama dilakukan tanpa mengaktifkan *Iptables* untuk dilihat berapa *resource* CPU yang naik akibat serangan tersebut dalam rentan 10 kali serangan.
9. Pengujian ini akan menguji serangan *TCP Flood* dengan dibatasi hashlimit di *Iptables.*
10. Pengujian pertama dibatasi *--hashlimit-upto* dengan nilai 50, dalam rentan 10 kali serangan.
11. Pengujian kedua dibatasi *--hashlimit-upto* dengan nilai 500, dalam rentan 10 kali serangan.
12. Pengujian ketiga dibatasi *--hashlimit-upto* dengan nilai 5000, dalam rentan 10 kali serangan.
13. Pengujian keempat dibatasi *--hashlimit-upto* dengan nilai 50000, dalam rentan 10 kali serangan.

14. Pengujian keempat dibatasi *--hashlimit-upto* dengan nilai 100000, dalam rentan 10 kali serangan.
15. Menggunakan *--hashlimit-burst* 500 pada pengujian nya.
16. Dari semua pengujian tersebut dianalisa dengan grafik dilihat mana yang paling stabil membatasi serangan sehingga tidak berlebihan dalam penggunaan *resource* CPU.

1.4 Maksud dan Tujuan Penelitian

Adapun maksud dari penelitian ini adalah sebagai berikut :

Sebagai salah satu syarat kelulusan untuk memperoleh gelar Sarjana pada jurusan Teknik Informatika Universitas Amikom Yogyakarta. Sedangkan Tujuan dari penelitian ini adalah sebagai berikut :

1. Untuk mengetahui bahwa dalam membatasi serangan *Ddos TCP Flood* agar tidak berlebihan menggunakan *resource* server. Dengan menerapkan *iptables –hashlimit-upto* 50, 500, 5000, 50000, 100000 ini rata - rata resource CPU yang digunakan 10 % sampai 60 %.
2. Mengetahui batasan yang stabil untuk diterapkan di sistem agar tidak berlebihan dalam penggunaan *resource* CPU.
3. Membandingkan hasil sebelum menggunakan Iptables dan sesudah menggunakan Iptables yang stabil.

1.5 Metode Penelitian

Metode penelitian ini akan menggunakan metode penelitian ekserimental dalam menguji coba sistem yang akan di bangun.

1.6 Sistematikan Penulisan

Untuk mempermudah dan memperjelas pembahasan, maka tugas akhir ini disusun dalam sistematika sebagai berikut :

BAB I **PENDAHULUAN**

Dalam bab ini penulis menguraikan mengenai latar belakang masalah, indentifikasi masalah, batasan masalah, maksud dan tujuan penelitian , dan sistematika penulisan.

BAB II **TINJAUAN PUSTAKA**

Pada bab ini akan di perkenalkan serta dijelaskan teori-teori yang dipakai dan berkaitan dengan *Intrusion Detection System.*

BAB III **METODE PENELITIAN**

Bab ini membahas lebih rinci tentang metode yang digunakan dalam penelitian yaitu metode pengembangan sistem.

BAB IV **IMPLEMENTASI DAN PEMBAHASAN**

Pada bab ini menjelaskan tentang implementasi dan hasil dari pengujian sistem dimana nantinya di bab ini akan dibandingkan keadaan normal dan pada saat terjadinya serangan.

BAB V **PENUTUP**

Pada bab ini penulis akan mennyimpulkan apa yang telah dilakukan pada bab sebelumnya, dan juga memberikan saran dalam mengembangkan sistem yang lebih baik.