BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, keamanan informasi menjadi semakin penting, terutama dalam konteks infrastruktur jaringan seperti *server*. *Server* sering menjadi target utama serangan siber, terutama serangan *Brute Force* dan serangan *Distributed Denial of Service* (DDoS), yang dapat menyebabkan kerusakan besar pada infrastruktur IT terutama pada *server* dan menyebabkan gangguan layanan bagi pengguna. Serangan *Distributed Denial of Service* (DDoS) merupakan ancaman besar bagi keamanan jaringan, dengan tujuan membuat layanan atau server tidak dapat diakses oleh pengguna yang sah melalui pembanjiran lalu lintas yang sangat besar. Serangan *DDoS* terbagi menjadi beberapa jenis termasuk *UDP Flood* yang mengirimkan sejumlah besar paket *UDP* tanpa tujuan spesifik untuk membanjiri saluran komunikasi, *TCP SYN Flood* yang *mengeksploitasi* proses *handshake* tiga arah dalam protokol *TCP* dengan mengirimkan permintaan *SYN* tanpa menanggapi tanggapan *SYN-ACK* dari *server* sehingga menyebabkan koneksi setengah terbuka yang menghabiskan sumber daya, dan *ICMP Flood* yang mengirimkan permintaan ping dalam jumlah besar untuk membanjiri *bandwidth* dan sumber daya server. Selain serangan *DDoS*, serangan *Brute Force* juga menjadi ancaman khususnya terhadap layanan *SSH* dengan mencoba menebak kombinasi *username* dan *password* melalui sejumlah besar percobaan *login* dalam waktu singkat. Untuk melindungi *server* dari serangan-serangan ini, dibutuhkan sistem deteksi serangan pada *server*. Salah satu pendekatan yang dapat diambil adalah dengan memanfaatkan *scapy* dari *python*.

Python adalah bahasa pemrograman yang populer dalam *Machine Learning*, sedangkan *Scapy* adalah sebuah pustaka *Python* yang *powerful* untuk melakukan deteksi serangan pada paket jaringan. Dengan memanfaatkan *Python*, dapat merancang sistem deteksi intrusi yang mampu memantau lalu lintas jaringan yang masuk dan keluar dari *server*. *Scapy* dapat melakukan *sniffing* dengan

menangkap paket data yang melewati jaringan serta menerapkan *callback* dengan fungsi yang akan dijalankan setiap kali paket tertentu terdeteksi. Dalam kasus serangan *DDoS* seperti *UDP Flood*, *TCP SYN Flood*, dan *ICMP Flood*, *sniffing* digunakan untuk menangkap semua paket yang masuk dan keluar dari jaringan dan *callback* diterapkan untuk memeriksa karakteristik setiap paket. Untuk mendeteksi *UDP Flood*, callback memeriksa jumlah paket *UDP* yang diterima dalam periode waktu tertentu. Jika jumlahnya melebihi ambang batas yang ditentukan, sistem akan mengidentifikasinya sebagai serangan. Serangan *TCP SYN Flood* dapat dideteksi dengan *callback* yang memeriksa permintaan *SYN* yang tidak diikuti oleh respons *ACK*. Jika terdapat banyak koneksi setengah terbuka dalam waktu singkat, ini merupakan indikasi serangan. Sedangkan *ICMP Flood*, *callback* dapat menghitung jumlah permintaan ping yang diterima. Jika jumlahnya sangat tinggi dalam waktu singkat, ini dapat dianggap sebagai serangan. Untuk serangan *Brute Force* pada layanan *SSH*, *callback* menganalisis percobaan *login* yang gagal. Jika terdapat banyak percobaan *login* yang gagal dari satu alamat IP dalam periode waktu yang singkat, ini menunjukkan adanya upaya serangan *Brute Force*.

Pemanfaatan *Telegram* sebagai media notifikasi memberikan informasi serangan kepada pengguna, yang terintegerasi ke *bot Telegram* dalam sistem deteksi intrusi. Setiap kali serangan terdeteksi, bot dapat mengirim pesan *notifikasi* langsung ke pengguna atau *administrator* jaringan melalui *aplikasi Telegram*. Notifikasi ini berisi tentang informasi detail serangan yang terdeteksi oleh sistem deteksi pada lalu lintas jaringan server. Dengan demikian, Penggunaan bahasa pemrograman *Python* dan pustaka *Scapy* dalam merancang sistem deteksi intrusi untuk mendeteksi serangan *Brute Force* dan serangan *DDoS* dapat memberikan solusi dalam menjaga keamanan layanan jaringan *server*. Serta pengunaan *Telegram* sebagai media notifikasi administrator jaringan dalam menerima *notifikasi* pemberitahuan serangan. Pendeteksian dini memberikan tindakan respons untuk meminimalkan dampak serangan.

1.2 Rumusan Masalah

Ada bebrapa batasan masalah dari penelitian ini antara lain:

1. Bagaimana merancang dan membangun sistem deteksi instrusi dengan menggunakan *library scapy*?
2. Bagaimana memanfaatkan telegram sebagai media *notifikasi* deteksi serangan?
3. Bagaimana melakukan pengujian serangan *UDP Flood, TCP SYN Flood*, *ICMP Flood,* dan *Brute Force* pada server?

1.3 Batasan Masalah

Ada beberapa batasan masalah dari penelitian ini antara lain:

1. Memanfaatkan fungsi packet sniffing dan callback dalam menganalisis lalu lintas jaringan untuk sistem deteksi intrusi.
2. Membuat bot telegram sebagai media notifikasi untuk antarmuka pengguna dalam deteksi serangan.
3. Melakukan skenario serangan menggunakan *tools hydra* untuk serangan *Brute Force* dan *hping3* untuk serangan *UDP Flood, TCP SYN Flood*, dan *ICMP Flood.*

1.4 Tujuan

Adapun tujuan dari penelitian Tugas Akhir ini adalah sebagai berikut:

1. Mendeteksi lalu lintas jaringan terhadap aktifitas yang menjadi potensi serangan pada server.
2. Memberikan pemberitahuan kepada pengguna tentang aktivitas yang mencurigakan yang terdeteksi sistem deteksi.
3. Menguji sistem deteksi intrusi dalam mendeteksi serangan *UDP Flood, TCP SYN Flood, ICMP Flood*, dan *Brute Force*.

1.5 Manfaat

Adapun manfaat dari penelitian ini adalah:

1. Sebagai deteksi dini terhadap aktivitas yang mencurigakan dalam mengawasi lalu lintas jaringan server.
2. Membantu pengguna dalam mendapatkan pemberitahuan serangan yang terdeteksi sistem.
3. Membantu dalam peroses pengujian sistem dalam mengidentifikasi serangan pada server.