BAB I

PENDAHULUAN

1.1 Latar Belakang

Pada era yang serba canggih ini terjadi peningkatan yang signifikan pada pengguna internet dari tahun 2018 - 2020 dikarenakan berbagai aktivitas dapat dilakukan melalui internet seperti *streaming*, berbelanja *online*, belajar, dll. Menurut Lembaga APJII pengguna internet pada tahun 2018 - 2020 meningkat pesat yaitu 64.8% naik hingga 73.7%. Seiring dengan banyaknya pengguna internet, maka banyak pula web *server* yang menyediakan layanan jasa. Web *server* tersebut mempunyai system *server* nya masing-masing sehingga terdapat banyak cara untuk melakukan serangan terhadap sistem jaringan web *server*. Para penyerang dapat dengan sangat mudah untuk melakukan serangan terhadap sistem jaringan dikarenakan metode dan alat yang dipakai semakin banyak dan efisien. Selain itu, dengan jumlah pengguna internet yang semakin banyak, maka semakin besar pula kemungkinan akan banyaknya penyerang yang mengincar pengguna internet tersebut. [1]

Saat ini serangan luar yang diluncurkan oleh penyerang semakin banyak dan lebih bervariatif. Salah satu contohnya adalah serangan *DDoS (Distributed Denial of Service)*. Serangan *DDoS* mengakibatkan sistem yang diserang mengalami gangguan berupa *error request, halt*, kegagalan sistem, dan sebagainya. *DDoS* memiliki beberapa metode serangan, yaitu Ping Of Death, UDP Flood, TCP Syn Flood dll. Umumnya setiap sistem *server* yang menyediakan layanan jaringan berbasis *TCP*, berpotensi terkena serangan *DDoS*

syn flood attack. Menurut jurnal penelitian yang berjudul "Analisis Ketersediaan Layanan dan Kinerja Sumber daya", penyerang menggunakan *half-open connection* untuk menguras sumber daya pada *server* agar koneksi yang datang pada *server* tersebut ditunda. Pada penelitian ini, dilakukan pendeteksian serangan pada trafik jaringan. Pendekatan yang digunakan untuk mendeteksi trafik normal dan trafik serangan adalah dengan menggunakan metode *filtering Logical* yang ada pada *Wireshark 3.4*.[2]

Berdasarkan latar belakang masalah diatas maka peneliti mengambil judul "Analisis serangan *DDoS* pada *Resource Server* menggunakan *Wireshark*". Penelitian ini berfokus pada hasil analisis yang diperoleh dari *Wireshark* dengan pendekatan menggunakan metode *filtering*, dan kemudian menganalisa *DDoS TCP SYN Flood*.

1.2 Rumusan Masalah

Pada penelitian ini, algoritma yang digunakan dalam melakukan analisis serangan adalah algoritma *Filtering Logical* sehingga mendapatkan perumusan masalah sebagai berikut:

1. Bagaimana melakukan analisis data serangan *DDos* dari trafik jaringan menggunakan *Wireshark* 3.4.
2. Bagaimana cara menghasilkan analisis serangan berupa fitur dan *rules* menggunakan algoritma filter *wireshark* 3.4.
3. Bagaimana cara melakukan pembuktian data pada serangan *DDoS* untuk mendeteksi serangan pada *server*.

1.3 Batasan Masalah

Hal yang dibatasi dalam penelitian Skripsi ini adalah sebagai berikut:

1. Penelitian ini hanya berlingkup pada data yang dapat dianalisis oleh aplikasi *Wireshark* 3.4.
2. Kegiatan pembuktian data penelitian ini bersifat *Live Forensics* (dilakukan pada saat sistem operasi jaringan sedang beroperasi).
3. *Resource bandwidth server* pada pengujian ini hanya berkisar 10 MB.
4. Menggunakan *Wireshark* 3.4 sebagai *monitoring* dan *capture packet*.
5. Menggunakan data dari hasil *filtering Wireshark* sebagai penentuan *rules* serangan.
6. Serangan yang diuji dan dianalisa berupa *DDoS* pada *resource server*.
7. Serangan *DDoS* berupa *TCP syn flood attack*.
8. Penelitian ini dibatasi pada proses analisis serangan *DDos* pada *capture packet Wireshark* 3.4. Artinya tidak ada proses pengembangan proteksi pada *resource* yang sedang diserang.

1.4 Maksud dan Tujuan Penelitian

Tujuan yang diharapkan pada penelitian Skripsi ini adalah sebagai berikut:

1. Menghasilkan data dari trafik jaringan menggunakan *Wireshark* 3.4.
2. Mencari informasi lalu-lintas serangan pada jaringan yang sedang menyerang *server*.
3. Melakukan simulasi serangan menggunakan aplikasi *TCP Flood Tools* dari sistem operasi *Kali Linux*.

4. Pendeteksi sederhana dari jenis serangan *DDoS* dan hasil analisis serangan menggunakan algoritma *filtering Wireshark*.
5. Menguji keakuratan dari algoritma *filtering Wireshark*, berdasarkan fitur dan *rules* serangan yang dimasukkan sebagai pendeteksi awal dari virus.

1.5 Manfaat Penelitian

Adapun beberapa manfaat dari penelitian ini adalah sebagai berikut:

1. Peneliti

   Diharapkan dapat menjadi referensi bagi peneliti selanjutnya agar dapat memberi hasil penelitian yang optimal. Selain itu, para peneliti selanjutnya juga berkesempatan memodifikasi dan mengembangkan karya penelitian ini.

2. Pengguna

   Memberikan jaringan yang nyaman dan aman untuk digunakan sebagai alternatif pemilihan metode dalam membangun sebuah jaringan *server*.

1.6 Metode Penelitian

Terdapat beberapa metode yang digunakan peneliti saat melakukan penelitian dan metode tersebut akan dijadikan sebagai informasi untuk menangani masalah yang dihadapi saat penelitian, yaitu:

1.6.1 Studi Literatur

Melakukan dan mengumpulkan referensi dan materi yang berkaitan dengan deteksi serangan. Selain itu, melakukan pencarian referensi yang berhubungan dengan *Wireshark*, analisis data, dan algoritma yang digunakan yaitu *Filtering Logical*.

1.6.2 Metode Pengumpulan Data

Pada tahap ini, dilakukan pengumpulan data simulasi yang akan diolah menggunakan algoritma *filtering logical*. Data simulasi dikumpulkan menggunakan *Wireshark* 3.4 pada serangan *DDoS*.

1.6.3 Perancangan Sistem

Melakukan perancangan sistem deteksi untuk mendeteksi serangan *DDoS*, dan dapat di integrasikan terhadap *library Wireshark*.

1.6.4 Analisis Sistem

Pada tahap ini sistem yang telah dibangun akan analisis berdasarkan hasil data dari hasil *capture filtering logical* yang menghasilkan fitur dan *rules* serangan. Hasil dari analisa tersebut diantaranya adalah kemampuan sistem untuk menghasilkan jumlah data *SYN-ACK* yang ditentukan dan kemampuan sistem untuk mendeteksi serangan berdasarkan fitur dan *rules* serangan yang diinputkan ke dalam sistem deteksi.

1.7 Sistematika Penulisan

Pada sistematika penulisan laporan "Analisis Serangan *DDoS* pada *Resource Server* Menggunakan *Wireshark*" adalah sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan, manfaat penelitian, metode penelitian dan sistematika penulisan penelitian.

BAB II LANDASAN TEORI

Landasan teori-teori yang digunakan untuk menunjang penelitian ini, terdiri dari teori Serangan *DDoS, Network Protocol Analyzer, Process Attack, Resource Server, TCP*, Aplikasi *WireShark, Filtering WireShark, Aplikasi Hping3, Laragon, Appache, DDoS TCP SYN Flood Attack.*. Bab ini menjelaskan hal-hal mengenai tinjauan pustaka, serta dasar teori-teori yang berasal dari studi pustaka yang dilakukan, untuk digunakan dalam penelitian agar dapat mendukung pelaksanaan penulisan penelitian.

BAB III METODE PENELITIAN

Bab ini akan menganalisa kebutuhan yang diperlukan dalan penelitian, dimana kebutuhan tersebut berupa hardware maupun software, serta alur penelitian simulasi serangan *DDoS TCP SYN Flood Attack* dengan pendekatan menggunakan metode *Live Forensics* terhadap *Resource Server*.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas skenario simulasi serangan *DDoS TCP SYN Flood Attack* terhadap *Resource Server* serta melakukan pembuktian data guna mendapatkan hasil analisis yang akurat., yang mana objek diuji dengan metode *filtering logical* dengan pendekatan *live forensics*.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran. Kesimpulan, menyimpulkan hasil dari penelitian yang telah dilakukan. Sedangkan saran, mengemukakan pendapat atau saran untuk menunjang pengembangan penelitan selanjutnya.

DAFTAR PUSTAKA