BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan Jaringan merupakah hal yang penting bagi dunia teknologi informasi maupun di dunia digital saat ini. Akan tetapi disisi lain timbul masalah – masalah yang begitu serius, masalah tersebut timbul khususnya pada faktor Keamanan sebuah Jaringan Komputer. Hal ini menjadi sangat mungkin untuk pelayanan yang diberikan kurang begitu aman, yang terkoneksi melalui Jaringan Komputer. Sehingga keamanan terhadap server yang dimiliki dapat meningkat.

Berdasarkan masalah tersebut yang menjadi pokok pembicaraan ini adalah DDoS (Distrubuted Denial of Service) dimana serangan tersebut bisa melakukan Downtime terhadap server agar user tidak bisa mengaksesnya. Serangan terhadap server ini umumnya membanjiri dengan paket – paket dengan memanfaatkan kelemahan sebuah *server three way hansking* pada TCP sehingga server tersebut traffic bisa tinggi atau menjadi sibuk. Paket yang dikirim agar jumlah tersebut bisa besar, maka si penyerang membutuhkan Pasukan atau bisa disebut DDoS Attacker (yang disebut pasukan ddos) untuk membantu melakukan penyerangan tersebut. Alasan kenapa Penelitian ini memilih solusi ini, Serangan ini bagi Peneliti lebih mudah di implementasikan dibandingkan serangan lainnya.

Pusat Operasi keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN) mencatat 88.414.296 serangan siber telah terjadi sejak 1 Januari hingga 12 April 2020. Pada bulan Januari terpantau 25.224.811 serangan dan kemudian pada bulan Februari terekam 29.188.645 serangan lalu kemudian pada bulan Maret terjadi 26.423.989 serangan dan sampai dengan 12 April 2020

telah tercatat 7.576.851 serangan. Puncak jumlah serangan terjadi pada tanggal 12 Maret 2020 yang mencapai 3.344.470 serangan dan setelah itu jumlah serangan mengalami penurunan yang cukup signifikan saat diberlakukannya kebijakan work from home (WFH) di berbagai tempat. Namun demikian selama WFH berlangsung telah terjadi serangan siber yang memanfaatkan isu terkait dengan Covid-19[1].

Snort merupakan bagian dari Instrusion Detection System (IDS) yang merupakan sebuah perangkat lunak *Open Source Nerwork*. Snort saat ini sangat bermanfaat bagi Keamanan suatu Jaringan yang memberi laporan bug atau kerusakan server secara detail, dan *up to date* sehingga segala serangan yang terdeteksi dapat diketahui. Kelamahan aplikasi ini pengeporasian yang cukup rumit dan butuh ketelitian dan kecepatan saat pembacaan paket tersebut. Snort ini nantinya akan di gunakan untuk mendeteksi serangan - serangan DDoS dan mencari si penyusup tersebut.

Kali Linux adalah sistem operasi yang menganut sistem UNIX yang menggunakan model pengembangan, serta didalam sistem operasinya terdapat software secara gratis. Dikarenakan memakai Kali Linux Peneliti lebih terbiasa menggunakan sistem operasi Kali Linux untuk server. Sehingga memudahkan dalam mencari serangan DDoS terhadap server tersebut. Selain itu juga sistem operasi ini handal dan tangguh, meskipun anda tidak membutuhkan biaya untuk memakai sistem operasi ini. Kali Linux ini nantinya akan di operasikan sebagai server dan attacker.

Pada tugas akhir ini Peneliti akan melakukan sebuah penelitian dengan membuat sistem keamanan dan menganalisa sistem keamanan serangan DDoS menggunakan Snort pada Kali Linux. Hal ini yang melatarbelakangi Peneliti untuk

menganalisa dan mengimplementasikan suatu sistem deteksi serangan DDoS terhadap jaringan yang memiliki kemampuan untuk mendeteksi adanya ancaman sebuah jaringan yang mencurigakan seperti serangan DDoS dan melaporkan dengan notifikasi pelaporan menggunakan Snort pada Kali Linux sebagai Firewall.

Oleh karena itu, sesuai dengan permasalahan di atas yang telah dikemukakan, maka Peniliti mencoba membahas suatu masalah dengan Judul **"Analisis Serangan DDoS di Jaringan Komputer Menggunakan Metode Instrusion Detection System (IDS) Snort pada Linux"**

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka permasalahan yang dimunculkan, antara lain :

1. Bagaimana menerapkan serangan DDoS pada server?
2. Bagaimana Sistem pendeteksi mengamankan jaringan dari serangan DDoS?
3. Bagaimana mengetahui yang berpotensi melakukan serangan tersebut?

1.3 Batasan Masalah

Agar Penelitian lebih terarah dan tidak menyimpang maka pokok permasalahan dan tujuan yang hendak dicapai, maka peneliti membatasi lingkup :

1. Jaringan yang akan diuji berupa Local Area Network (LAN).
2. Sistem operasi yang akan digunakan adalah Kali Linux 2020 sebagai server.

3. Metode yang digunakan adalah metode SPDLC (Security Policy Development Life Cycle).
4. Kali Linux 2020 diinstall pada Virtual Machine.
5. Tools yang digunakan DDoS dengan Hping3 dan Port Scanning menggunakan Nmap.
6. Pendeteksi yang digunakan menggunakan Snort IDS.
7. Terdapat 2 user yang terdiri 1 server dan firewall, dan 1 penyerang.
8. Serangan yang akan digunakan dalam pengujian tersebut DDoS dan Port Scanning.
9. Hasil yang didapatkan berupa alert Notifikasi akan masuk pada Websnort dan Bot Tele.
10. Tidak membahas teknik Hacking

1.4 Maksud dan Tujuan Penelitian

1.4.1 Maksud Penelitian

Sesuai dengan permasalahan yang dihadapi, maksud dari penelitian ini adalah:

1. Untuk mempublikasikan pembelajaran keamanan jaringan terhadap server yang kurang aman belakangan ini.
2. Untuk menghasilkan informasi serangan pada jaringan dan meningkatkan keamanan jaringan internet.
3. Untuk membantu pengguna atau admin pada sebuah jaringan sehingga keamanan dapat terjaga.

1.4.2 Tujuan Penelitian.

Sesuai dengan permasalahan yang dihadapi, tujuan penelitian ini adalah:

1. Mengetahui serangan DDoS yang dilakukan terhadap server.
2. Mengatasi serangan DDoS pada jaringan.
3. Mendapatkan parameter-parameter yang mempengaruhi serangan DDoS pada server.
4. Menemukan user yang berpotensi menyerang server tersebut.

1.5 Manfaat Penelitian

Berdasarkan tujuan penelitian yang hendak dicapai, maka penelitian ini diharapkan mempunyai manfaat baik secara langsung maupun tidak langsung. Adapun Manfaat penelitian ini adalah sebagai berikut :

1. Sebagai masukan bagi peneliti sendiri yang ingin memperluas cakrawala berfikir setelah mendapatkan suatu perbandingan teori dengan aplikasinya.
2. Sebagai informasi untuk mengetahui penyusup yang terjadi pada komputer atau laptop kita melalui jaringan internet
3. Sebagai wawasan keamanan pada jaringan internet
4. Mencegah penyusup yang hendak menerobos masuk ke sistem komputer kita

1.6 Metode Penelitian

Dalam penulisan skripsi ini, peneliti melakukan beberapa tahapan dalam menyelesaikan penelitian. Adapun penelitian yang dilakukan adalah:

1.6.1 Metode Pengumpulan Data

Dalam memudahkan pembuatan dan pengumpulan data yang diperlukan dalam sebuah penelitian maka perlu dirumukan metode pengumpulan data pada penelitian ini adalah sebagai berikut

1. Studi Literatur

   Pada metode ini penulis akan melakukan pencarian, pembelajaran dari berbagai macam literatur dan dokumen yang menunjang tugas akhir ini khususnya yang berkaitan dengan Instrusion Detection System (IDS)

2. Studi Pustaka

   Melakukan pendalaman terhadap teori-teori yang berkaitan dengan studi kasus. Serta pengamatan ke berbagai macam website di internet yang menyediakan informasi yang relevan dengan permasalahan penelitian ini.

1.6.2 Metode Perancangan

Tahapan ini nantinya dengan melakukan perancangan sistem yang disesuaikan dengan permasalahan diatas dengan hasil analisis kebutuhan sistem.

1.6.3 Metode Pengembangan

Tahapan ini penulis menggunakan metode Security Policy Development Life Cycle (SPDLC), yang berisi tahap – tahap sebagai berikut:

1. Identifikasi
2. Analisis
3. Design

4. Implementasi
5. Enforcement
6. Enhancement

1.6.4 Metode Testing

Tahapan ini penulis melakukan pengujian sistem keamanan pada server yang nanti akan mendapat serangan DDoS dan bagaimana cara mengamankan server tersebut dari serangan DDoS.

1.7 Sistematika Penulisan

Untuk memberikan gambaran mengenai tugas akhir yang akan dibuat, adapun sistematikan penulisan laporan sebagai berikut:

BAB I PENDAHULUAN

Bab pendahuluan mendekripsikan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud penelitian dan tujuan penelitian, manfaat penelitian, metode penelitian, sistematika penulisan

BAB II LANDASAN TEORI

Bab ini berisi teori-teori yang terkait dengan penelitian yang dilakukan oleh penulis.

BAB III ANALISIS DAN PERANCANGAN

Bab ini menguraikan proses sistem sistem kerja identifikasi masalah, analisis kebutuhan sistem, dan skenario uji coba.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini mempaparkan dari hasil-hasil tahapan penelitian, mulai dari implementasi, pengujian, dan hasil pembahasan.

BAB V PENUTUP

Bab ini berisi kesimpulan yang didapat selama pembuatan laporan tugas akhir serta saran – saran yang akan menjadi masukan bagi penulis serta bisa berguna bagi yang membaca.