BAB I
PENDAHULUAN

1.1 Latar Belakang

Keamanan Jaringan pada server adalah hal penting di dunia teknologi informasi dan digital pada era saat ini. Keamanan yang baik dapat memberikan rasa percaya pada suatu server yang digunakan. Masalah menjadi sangat mungkin terjadi apabila fasilitas yang diberikan kurang aman. Sehingga keamanan terhadap server memiliki banyak celah, maka dari itu diperlukan peningkatan keamanan.

Pokok pembicaraan ini adalah masalah tentang penyerangan DDoS (Distributed Denial of Service) yang serangan tersebut dapat mengakibatkan Downtime server sehingga user tidak bisa mengaksesnya. Serangan server ini umumnya membanjiri dengan paket paket dan memanfaatkan kelemahan dari *server three way handsking* yang ada pada TCP sehingga membuat server tersebut terdampak lonjakan traffic tinggi dan sibuk. Paket yang dikirim agar jumlah tersebut bisa besar, si penyerang membutuhkan Pasukan atau biasa disebut DDoS Attacker untuk membantu kelancaran penyerangan tersebut. Alasan mengapa Penelitian ini memilih solusi ini, Serangan ini bagi Peneliti lebih mudah diterapkan dibanding serangan yang lain.

Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Kriptografi Nasional (BSSN) mencatat, sejak 1 Januari hingga 12 April 2020 tercatat sebanyak 88.414.296 serangan siber, pada Januari tercatat 29.188.645 serangan dan kemudian menjadi 26.423.989 serangan. di bulan Maret dan per 12 April 2020 .56.851 serangan telah tercatat. Jumlah serangan maksimum terjadi pada 12 Maret 2020 yang mencapai 3.344.40 serangan dan setelah itu jumlah serangan mengalami penurunan yang cukup signifikan saat diberlakukannya work from home (WFH) di berbagai tempat. Namun demikian selama WFH berlangsung telah terjadi serangan siber yang memanfaatkan isu terkait dengan dengan Covid-19.

Topik pembahasan kali ini adalah Distributed Denial of Service (DDoS) dimana serangan tersebut dapat menyebabkan Downtime server sehingga pengguna tidak dapat mengaksesnya. Serangan terhadap server umumnya dibanjiri paket dengan memanfaatkan kelemahan server yang melakukan three-way handsking over TCP sehingga server dapat memiliki traffic yang tinggi atau sibuk. Paket-paket tersebut dikirim agar jumlahnya bisa besar, sehingga penyerang membutuhkan pasukan atau bisa disebut DDoS Attacker (yang disebut pasukan ddos) untuk membantu melakukan serangan. Alasan investigasi ini memilih solusi ini, serangan ini untuk penyelidik adalah lebih mudah diterapkan daripada serangan lainnya.

Snort adalah bagian dari Intrusion Detection System (IDS) yang merupakan sebuah aplikasi atau perangkat lunak *Open Source Network*. Aplikasi Snort sangat berguna untuk Keamanan suatu Jaringan yang memberi laporan tentang kerusakan server, bug secara detail dan *up to date* sehingga segala serangan yang terdeteksi dapat terbaca. Kekurangan pada aplikasi Snort yaitu pengoperasian yang lumayan rumit, butuh ketelitian pada setiap detail-detail, dan kecepatan saat pembacaan paket tersebut. Aplikasi Snort ini kedepannya akan digunakan untuk mendeteksi serangan – serangan DDoS dan mencari si penyerang tersebut.

Sistem operasi Kali Linux adalah sistem operasi yang menganut sistem UNIX yang menggunakan model pengembangan, serta dalam sistem operasinya terdapat software secara gratis. Alasan menggunakan Kali Linux karena Peneliti lebih terbiasa menggunakan sistem operasi Kali Linux untuk server sehingga memudahkan dalam mencari serangan DDoS terhadap server. Disamping sistem operasi yang handal dan tangguh ini, anda tidak membutuhkan biaya untuk memakai sistem operasi ini. Kali Linux ini nantinya akan dioperasikan sebagai attacker dan server. Alasan sederhana mengapa Peniliti lebih memilih menggunakan Snort karena menurut opini pribadi, sistem ini lebih mudah diimplementasi.

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

Oleh karena itu, sesuai dengan permasalahan yang telah dijabarkan diatas, maka Peneliti mencoba membahas dan memecahkan suatu masalah dengan Judul **"Analisis Serangan DDoS Menggunakan Metode Instrusion Detection Sistem menggunakan Snort"**

1.2 Tujuan

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

- Untuk mempublikasian pembelajaran keamanan jaringan terharap server yang kurang aman.
- Menghasilkan informasi serangan pada jaringan dan meningkatkan keamanan jaringan internet.
- Membantu pengguna atau admin pada sebuah jaringan sehingga kemanan dapat terjaga.
- Mengetahui serangan DDoS yang dilakukan terhadap server.
- Mengatasi serangan DDoS pada jaringan.
- Mendapatkan parameter-parameter yang mempengaruhi serangan DDoS pada server.
- Menemukan user yang berpotensi menyerang server tersebut.

1.3 Batasan Masalah

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

- Jaringan yang akan diuji berupa Local Area Network (LAN).
- Sistem operasi yang akan digunakan adalah Kali Linux 2020 sebagai server.
- Metode yang digunakan adalah SPDLC (Security Policy Development Life Cycle).
- Kali Linux 2020 diinstall pada Virtual Machine.
- Tools yang digunakan DDoS dengan Hping3 dan Port Scanning menggunakan Nmap.
- Pendeteksi yang digunakan menggunakan Snort IDS.
- Terdapat 2 user yang terdiri 1 server dan firewall, dan 1 penyerang.
- Serangan yang akan digunakan dalam pengujian tersebut DDoS dan Port Scanning.
- Hasil yang didapatkan berupa alert Notifikasi akan masuk pada Websnort dan Bot Tele.
- Tidak Membahas teknik Hacking.

1.4 Literatur Review

No.	Peneliti	Tahun	Judul	Metode	Hasil Penelitian
1.	- Sutari, - Adi Putranto Pancaro, - Fembi Isnanto Saputra	2018	Implementasi IDS (Interusion Detection System) pada Sistem Keamanan Jaringan Sma 1 CIKEUSAL	IDS, PfSense	IDS Snort mampu mendeteksi adanya serangan.
2.	-Muhammad Rizky Hasan, -Suhermanto, -Suharmanto	2017	Keamanan Sistem Perangkat Lunak dengan Software Development Lifecycle	Cross Site Scripting, SQL Injection, SDDLC	SSDLC dapat mengevaluasi kerentanan keamanan pada sistem perangkat lunak.
3.	Khairul Saleh	2020	Implementasi Intrusion Detection System (IDS) pada Server Web PT.XYZ	IDS Snort	Snort IDS dapat mengenali jenis gangguan yang ditimbulkan dan dapat menampilkan dengan cepat

			Menggunakan Snort		kapan terjadinya gangguan.
4.	-Barany Fachri - Fadli Hamdi Harap	2020	Simulasi Penggunaan Intrusion Detection System (IDS) Keamanan Jaringan dan Komputer	IDS	IDS dapat membatasi serangan terhadap server tergantung waktu saat memberhentikan serangan pada client.
5.	-Yusuf Abdulloh -Joko Triyono -Uning Lestari	2020	Pengaruh Penempatan Snort Terhadap Keamanan Jaringan (Studi Kasus Laboratorium VI Jaringan Kampus 3	IDS Snort	IPS maupun IDS lebih safety mengelola jaringan, penempatan Snort dalam lebih baik dari segi fungsi kinerja IDS dibanding dengan

			IST Akprind Yogyakarta)		penempatan Snort luar.
6.	-Lukman -Melati Suci	2020	Analisis Perbandingan Kinerja Snort Dan Suricata Sebagai Intrusion Detection System Dalam Mendeteksi Serangan Syn Flood Pada Web Server Apache	IDS Snort dan Suricata	IDS Snort memiliki rasio penggunaan CPU sebanyak 78,31% sedangkan IDS Suricata sebanyak 80,08%, Hasil pengujian IDS Snort memiliki rasio penggunaan ram 23,89%, dan untuk rasio performa *uncaptured* paket untuk IDS Snort 68,2% sedangkan IDS Suricata 3.42%

1.5 Metode Penelitian

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

1.5.1 Metode Pengumpulan Data

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

1. **Studi Literatur**

   Pada metode ini penulis akan melakukan pencarian, pembelajaran dari bebagai 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.

1.5.2 Metode Perancangan

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

1.5.3 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 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 :

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

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, 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 kerja identifikasi masalah, analisis kebutuhan sistem, dan skenario uji coba.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Bab ini mempaparkan dari hasil-hasil tehapan 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.