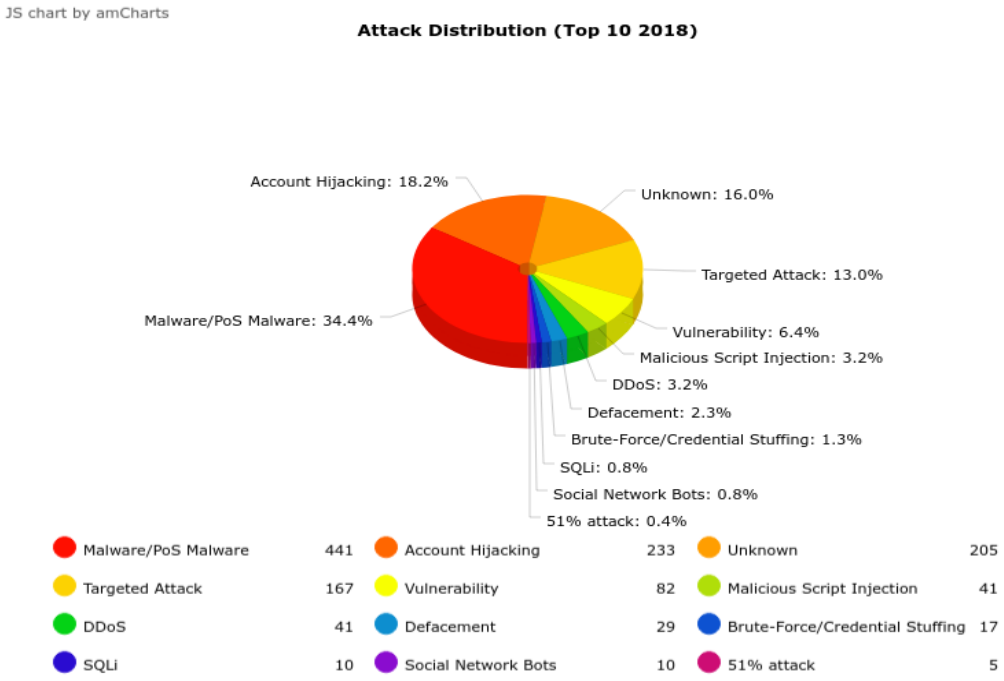
BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam pengembangan keamanan Teknologi Informasi (TI) dilakukan pemfokusan yang mengutamakan data informasi sebagai aset terpenting dan harus dijaga keasliannya, dimana aset tersebut dikontrol untuk menghindari munculnya ancaman seperti pencurian dan pemalsuan data, hal tersebut dapat ditangani dengan melihat kelemahan pada sistem itu sendiri seperti mengenal jenis ancamannya yang diantaranya serangan *port scanning* SSH *brute force*, MiTM dan DDoS.



Gambar 1.1.Data serangan siber tahun 2018

Berdasarkan Gambar 1.1 data serangan siber yang dikumpulkan oleh HACKMAGEDDON [1] *Information Security Timelines and Statistic* pada tahun 2018 memperlihatkan kondisi keamanan jaringan yang terlihat aman ternyata rentan akan serangan yang mengakibatkan kerugian dari segi materil, segi waktu maupun segi biaya. Dikhawatirkan apabila tidak ditangani maka data yang dicuri

bisa digunakan untuk kegiatan ilegal. Serangan siber tersebut dapat ditangani dengan menerapkan beberapa aspek keamanan informasi yang meliputi aspek *Confidentiality*, *Integrity*, *Availabilty* (CIA) *triad* [2]. Dari aspek tersebut mengharuskan sistem pengamanan jaringan mampu melakukan pendeteksian dan pencegahan adanya ancaman dan gangguan dari dalam maupun luar. Teknologi yang dapat membantu permasalahan sistem keamanan jaringan tersebut adalah IPS.

Pada sistem keamanan jaringan ini dirancang menggunakan topologi *star* supaya sistem bergantung satu *node* pusat dengan administrasi jaringan. Pusat administrasi jaringan dikontrol penuh oleh perangkat PC *Router* yang memberikan akses layanan *web server* dan DNS *server*. Layanan tersebut dapat terjadi karena jalur protokol dan *port* dikontrol menggunakan metode pengamanan jaringan DMZ sebagai garis pertama pada sistem keamanan jaringan yang memanfaatkan *firewall* [3]. Jaringan DMZ memiliki tiga zona yaitu *untrusted*, *trusted* dan *semi-trusted*. Berikutnya IPS digunakan sebagai garis kedua pada sistem keamanan jaringan dengan fungsi layaknya IDS dan *firewall* dengan melakukan penekanan *early detection* dan *prevention* secara *real-time,* kemudian IPS bekerja berdasarkan *rules* yang telah dibuat dan mengidentifikasi kecocokan *True Positive* (TP) pada *rules* terhadap serangan. Jenis IPS yang digunakan adalah NIPS [4], dimana NIPS bekerja secara *proactive protection* pada OSI *Layer* (2, 3 dan 7) dengan melakukan *sniffing packet* yang mencurigakan pada protokol. Selanjutnya IPS ini akan mendeteksi adanya serangan menggunakan metode AD [5]. Secara umum AD merupakan pengamanan dengan mengamati pola trafik jaringan yang tidak normal dari *log* IPS dari rentang waktu tertentu ditunjukkan untuk mendeteksi adanya ancaman yang belum terindikasi berdasarkan *rules.* Hasil dari *log* Snort yang didapatkan akan divitualisasikan melalui aplikasi SIEM yang membantu penganalisaan *event* dan *reseouces* sistem yang sedang di *monitor* atau diamankan, aplikasi SIEM yang digunakan adalah WUI ELK *stack*. Setelah melakukan kegiatan *prevention* akan dilakukan analisa paket masuk menggunakan aplikasi *network analyzer* yaitu

software Wireshark yang dapat membantu dalam menganalisa *harmfull traffic* yang terjadi pada protokol jaringan.

Pada penelitian ini akan dilakukan pembuktian hasil dari pengujian keamanan jaringan menggunakan IPS berdasarkan parameter analisa metode deteksi AD pada IPS yang disimulasikan menggunakan VM. Dari permasalahan tersebut, maka penulis merangkai penelitian dengan judul "ANALISIS KEAMANAN JARINGAN MENGGUNAKAN SNORT3 *NETWORK-BASED INTRUSION PREVENTION SYSTEM* (NIPS) DENGAN TEKNIK *ANOMALY-BASED DETECTION* (AD)".

1.2. Rumusan Masalah

Rumusan dari penelitian ini adalah:

1. Bagaimana melakukan pengamanan jaringan menggunakan *Intrusion Prevention System* (IPS) dalam menangani serangan?
2. Bagaimana hasil uji keamanan jaringan IPS menggunakan metode *Anomaly-based Detection* (AD) terhadap serangan?
3. Bagaimana performansi sistem keamanan jaringan berdasarkan penggunaan sumber daya CPU, memori dan jaringan?

1.3. Batasan Masalah

Batasan masalah dari penelitian ini adalah:

1. Penerapan keamanan jaringan IPS menggunakan aplikasi Snort3
2. Penerapan keamanan jaringan *firewall* menggunakan aplikasi Iptables
3. Sistem operasi Linux Ubuntu LTS sebagai PC Admin dan PC *Router*.
4. Sistem operasi Linux Ubuntu *Server LTS* sebagai PC *Server.*
5. *S*istem operasi Kali Linux sebagai PC Penyerang
6. Pengujiannya jenis serangan *port scanning* menggunakan aplikasi Nmap.
7. Pengujiannya jenis serangan SSH *brute force* menggunakan aplikasi Hydra.
8. Pengujiannya jenis serangan MiTM menggunakan aplikasi Ettercap dan Setoolkit.

9. Pengujiannya jenis serangan DDoS menggunakan aplikasi *Low Orbit Ion Cannon* (LOIC).

1.4. Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Menangani serangan menggunakan IPS dapat mendeteksi ancaman secara *early detection* dan pencegahan secara *inbound-outbound*.
2. Menganalisa pola aktifitas serangan yang tidak teridentifikasi dengan metode *Anomaly-based Detection* (AD) berdasarkan *event timestamp* lalu jumlah *event*.
3. Dapat mengetahui tingkat performansi sebelum dan sesudah adanya pengamanan pada sistem keamanan jaringan dengan menggunakan IPS.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini adalah:

1. Diketahui pengamanan jaringan menggunakan IPS lebih unggul dibanding hanya menggunakan *firewall,* karena IPS dapat mendeteksi dan mencegah adanya serangan pada jaringan *inbound-outbound*.
2. Diketahui pendeteksian serangan menggunakan IPS dengan metode AD secara efektif dapat mendeteksi ancaman yang tidak teridentifikasi pada *rules* dan suatu ancaman dilihat dari *resource* yang bekerja seperti *Central Processing Unit* (CPU), *memory* dan jaringan yang diterima pada sistem dalam rentang waktu tertentu.

1.6. Sistematika Penelitian

Sistematika penulisan penelitian ini dibagi manjadi 3 bagian:

1. BAB I : PENDAHULUAN

   Bagian pendahuluan berisi mengenai latar belakang, rumusan masalah yang diangkat, manfaat, tujuan serta

batasan dalam penelitian.

2. BAB II : TINJAUAN PUSTAKA

   Pada bagian ini membahas tentang penelitian terdahulu serta dasar teori yang digunakan dalam penelitian ini.

3. BAB III : METODE PENELITIAN

   Pada bagian membahas mengenai studi literatur, perancangan sistem, alat dan bahan, instalasi dan konfigurasi, skenario pengujian serta penyerangan dan analisa.

4. BAB IV : PEMBAHASAN

   Pada bagian ini menjelaskan hasil uji coba dan analisa implementasi penelitian

5. BAB V : PENUTUP

   Berisi kesimpulan penelitian dan saran dari peneliti