BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi saat ini berkembang sangat pesat, jaringan komputer yang merupakan bagian dari teknologi inormasi pun berkembang cepat. Jaringan komputer merupakan serangkaian komputer yang saling berhubungan antara yang satu dengan yang lain sehingga memudahkan dalam hal berbagi informasi antara komputer yang terhubung dalam jaringan tersebut. Teknologi-teknologi baru dalam jaringan komputer saat ini mulai banyak ditemukan. Pada jaringan komputer maka diperlukan lah sebuah sistem keamanan server untuk melindungi komputer server dari ancaman baik dalam bentuk kesengajaan ataupun bukan.

Dibalik kemudahan mengakses informasi yang disediakan oleh internet, terdapat bahaya besar yang mengintai jaringan WiFi. Sebuah jaringan harus dilindungi dari segala macam serangan dan usaha - usaha penyusupan atau pemindahan data oleh pihak yang tidak berhak. Maka dalam pembangunan perancangannya, sistem keamanan jaringan WiFi harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif dan meminimalisir terjadinya serangan. Serangan – serangan itu dapat mengakibatkan kerusakan data bahkan dapat mengakibatkan kerusakan pada hardware. Serangan pada suatu data dalam jaringan dapat dikategorikan menjadi 2 yaitu, Serangan pasif dan serangan aktif. Serangan pasif

adalah serangan yang mengambil suatu unit data dan kemudian menggunakannya untuk memasuki sesi autentikasi dengan berpura - pura menjadi user yang autentik / asli disebut dengan replay attack. Sedangkan serangan aktif adalah serangan yang mencoba memodifikasi data, mencoba mendapatkan autentikasi, atau mendapatkan autentikasi dengan mengirimkan paket - paket data yang salah ke data stream atau dengan memodifikasi paket - paket yang melewati data stream. Terdapat beraneka macam jenis dan teknik intrusi yang dapat mengganggu jaringan WiFi Seperti Port Scanning, Trojan Horse, Network Flooding, Denial of Service, Packet Interception, dan lain sebagainya. Pada saat ini, serangan Denial of Services merupakan salah satu ancaman utama dalam perkembangan teknologi informasi. Cara untuk menangani serangan tersebut menggunakan teknik IDS dan IPS.

IDS (Intrusion Detection System) merupakan sistem untuk mendeteksi adanya “intrusion” yang dilakukan oleh “intruder” atau pengganggu / penyusup di jaringan (Komputer, 2015). Tujuan dari Intrusion Detection System diantara yaitu mengawasi jika terjadi penetrasi kedalam sistem, mengawasi traffic yang terjadi pada jaringan, mendeteksi anomali terjadinya penyimpangan dari sistem yang normal atau tingkah laku user, serta mendeteksi signature dan membedakan pola antara signature user dengan attacker (Setiawan, 2015). Sistem pendeteksi jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan, tetapi masih belum mampu mengambil tindakan lebih lanjut. Dibutuhkan sebuah sistem yang mampu menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan otomatis. Dalam penanggulangan yang bisa

digunakan oleh seorang Sistem Administrator, yaitu Intrusion Prevention System (IPS).

IPS atau yang biasa disebut Intrusion Detection Prevention System (IDPS), adalah peralatan keamanan jaringan yang memonitor jaringan dan kegiatan sistem dari aktifitas yang berbahaya (Korcák, Lámer, & Jakab, 2014). Selain itu IPS dapat secara aktif mencegah gangguan yang terdeteksi. IDPS (Intrusion Detection and Prevention System) berfungsi untuk mengautentikasi aktivitas yang mencurigakan, menyimpan kedalam log dan mencoba untuk memblok atau menghentikan serta melaporkan aktifitas tersebut (Scarfone & Mell, 2007). Salah satu mesin IDPS yang mampu mengatasi permasalaham diatas yaitu Suricata.

Suricata adalah sebuah perangkat lunak berbasis aturan mesin IDS / IPS yang memanfaatkan aturan yang dikembangkan untuk memonitor lalu lintas jaringan dan memberikan peringatan kepada sistem administrator ketika terdapat aktifitas yang mencurigakan (Kacha, 2012). Suricata adalah open source dan dimiliki oleh masyarakat yang dikelola yayasan non-profit, Open Information Security Foundation (OISF). Suricata dikembangkan oleh OISF dan vendor pendukungnya. Suricata bekerja sebagai mesin multithreaded (Alhomoud, 2011). Multithereaded yaitu Suricata akan lebih akurat karena menggunkan multi-core pada sistemnya (Day & Burns, 2011). Jadi Suricata menggunakan seluruh inti prosesor yang ada dalam komputer yang digunakan. Pencegahaan yang paling sering dilakukan untuk masalah ini adalah dengan menempatkan seorang administrator. Seorang administrator bertugas untuk mengawasi dan melakukan tindakan preventif ketika terjadi aksi penyusupan dan serangan.

Masalah timbul ketika administrator sedang tidak berada pada posisi siap sedia, misalnya sakit, berada di luar jam kerja, atau adanya kepentingan mendadak. Sedangkan serangan terhadap server bisa terjadi kapan saja. Karena hal tersebut, diharapkan dari penggunaan sistem Intrusion Detection Prevention System (IDPS) tersebut dapat mencegah gangguan yang terdeteksi didalam jaringan meskipun administrator sedang tidak berada di tempat. Berdasarkan permasalahan tersebut, administrator membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan.

Dalam skripsi kali ini akan membahas tentang perancangan intrusion detection prevention system (IDPS) dalam jaringan wifi berbasis suricata pada PfSense sebagai sebuah teknik pendeteksian dan pencegahan dalam menangani sebuah serangan dalam jaringan wifi.

1.2. Perumusan Masalah

Dari latar belakang yang telah diuraikan sebelumnya, maka dapat dibentuk rumusan masalah sebagai berikut.

a. Bagaimana Cara implementasikan suricata pada jaringan menggunakan pfsense ?
b. Bagaimana teknik IDPS suricata dalam mengamankan jaringan wifi jika terjadi serangan ?
c. Bagaimana cara melakukan serangan pada jaringan wifi ?

1.3. Batasan Masalah

Untuk menghindari meluasnya pokok pembahasan, maka pengerjaan proyek akhir ini terbatas pada :

a. Jaringan yang digunakan adalah jaringan wifi.

b. Terdapat 2 serangan yaitu ICMP Flood dan SYN Flood.

c. Sistem Operasi yang digunakan untuk serangan adalah Kali Linux

d. Menggunakan Sistem Operasi PfSense versi 2.4.4.

1.4. Tujuan

Dalam hal ini tujuan yang ingin dicapai yaitu, mengetahui teknik "Implementasi Intrusion Detection Prevention System (IDPS) dalam Jaringan Wifi menggunakan Suricata pada PfSense".

1.5. Manfaat

Adapun manfaat yang dapat diperoleh dari proposal tugas akhir "Implementasi Intrusion Detection Prevention System (IDPS) dalam Jaringan Wifi berbasis Suricata pada PfSense" ini adalah :

Penulis :

a. Menerapkan ilmu yang diperoleh di bangku kuliah.

b. Memahami bagaimana teori, konsep dan praktek tentang Intrusion Detection System / Intrusion Prevention System dalam keamanan jaringan wifi dalam pfsense.

c. Penulis dapat menggabungkan hasil bacaan dari berbagai sumber, mengambil manfaatnya dan mengembangkan ke tingkat pemikiran yang lebih matang.

Pembaca :

a. Pembaca dapat mengetahui memahami dan mampu mengimplementasikan teori konsep dan langkah – langkah penulisan skripsi dan unsur – unsurnya.

b. Pembaca dapat menambah wawasan serta dapat mengembangkan karya – karya yang baru.

c. Memeberikan pemikiran tentang teknologi informasi yang bermanfaat bagi masyarakat dan pada Universitas UPN "Veteran" Jawa Timur.

1.6. Sistematika Penulisan

Untuk mempermudah pembahasan skripsi dan memberikan gambaran yang sistematis dalam memahami masalah yang disajikan, maka penulisan dibagi ke dalam bagian-bagian berupa bab yaitu:

BAB I PENDAHULUAN

Dalam bab ini diuraikan tentang masalah pokok yang dibahas dalam skripsi ini, yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan menguraikan teori atau konsep yang melandasi hal – hal yang terdapat dalam penelitian ini, secara umum dijelaskan tentang teori – teori

yang berhubungan dengan kinerja strategi baik dikurip dari berbagai referensi maupun hasil riset yang didapat.

BAB III METODOLOGI

Bab ini menjelaskan metode – metode yang dilakukan saat penelitian skripsi berlangsung yang meliputi alur penelitian, rancangan sistem, skenario uji coba, serta analisa dan pembuktian serangan. Alur penelitian berisi tentang proses penelitian tugas akhir, mulai dari studi pustaka sampai kesimpulan. Rancangan sistem berisi tentang definisi kebutuhan sistem, rancangan jaringan, serta rancangan sistem. Skenario uji coba berisi tentang alur / proses serangan pada jaringan.

BAB IV HASIL DAN PEMBAHASAN

Dalam bab ini ini berisi tentang konfigurasi IP pada laptop, tes koneksi, instalasi Suricata dan paket – paket pendukung, konfigurasi Suricata, simulasi serangan, analisa pendeteksian. Proses analisa dilakukan dengan membandingkan traffic normal dan traffic serangan pada log Suricata yang telah membuat recird aktifitas jaringan saat mulai dijalankan.

BAB V KESIMPULAN DAN SARAN

Pada bab terakhir ini berisi tentang kesimpulan yang diperoleh dari hasil implementasi Suricata yang telah diuji pada bab sebelumnya. Serta saran – saran yang bermanfaat bagi pembaca dan memberikan pengembangan lebih lanjut tentang isi laporan skripsi.