BAB I

PENDAHULUAN

1.1. Latar Belakang

Keamanan jaringan saat ini menjadi isu yang sangat penting dan terus berkembang, Berbagai macam teknologi telah dikembangkan untuk membantu manusia dalam berkomunikasi. Jika pada tahun 1980-an teknologi jaringan komputer hanya mengandalkan teknologi jaringan berbasis kabel, saat ini teknologi tersebut mulai banyak ditinggalkan karena beberapa keterbatasannya, seperti besarnya biaya yang harus dikeluarkan, selain itu teknologi ini juga tidak fleksibel karena sangat tergantung pada kabel, dan hanya bisa digunakan 1 perangkat (Arief, 2007).

Dibalik kemudahan mengakses informasi yang disediakan oleh internet, terdapat bahaya besar yang mengintai jaringan WiFi. Sehingga internet tetap menjadi lingkungan yang kurang bersahabat untuk sistem jaringan komputer. Terlepas dari itu, dalam hal ini keamanan jaringan WiFi telah menjadi salah satu bagian yang sangat penting untuk menjaga validitas dan integritas data, serta menjamin ketersediaan layanan bagi penggunanya.

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 (Nugroho, 2012). Serangan – serangan itu dapat mengakibatkan kerusakan data bahkan dapat mengakibatkan kerusakan pada *hardware.*

Menurut Simarmata (2006), 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 (Arbor Networks, 2012). 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.

Iptables merupakan satu dari beberapa aplikasi firewall yang dapat dijalankan di Linux. Sebenarnya ada beberapa aplikasi firewall yang dapat berjalan di linux seperti, ipfwadm, ipchains, dan Iptables. Secara default Iptables ini sudah terinstall pada sistem operasi open sources, jadi kita tak perlu menginstallnya lagi. Dalam pengaturan paketnya, ada 3 buah tabel paket yang terdapat pada Iptables (Sularno, 2016).

Bro adalah open-source, Network Intrusion Detection System (NIDS) berbasis sumber terbuka yang secara pasif memonitor lalu lintas jaringan dan mencari aktivitas yang mencurigakan. Bro mendeteksi intrusi dengan memparsing lalu lintas jaringan untuk mengekstraksi semantik tingkat aplikasi dan kemudian mengeksekusi analisis berorientasi peristiwa yang membandingkan aktivitas dengan pola yang dianggap merepotkan (Varadarajan, 2005). Analisisnya mencakup deteksi serangan tertentu termasuk dapat berbasis *signature* atau berbasis *anomaly* tergantung dari konfigurasi yang dilakukan. Dan juga bisa didefinisikan dalam hal peristiwa dan aktivitas yang tidak biasa (misal., Host tertentu yang terhubung ke layanan tertentu, atau pola upaya koneksi yang gagal).

Universitas Hang Tuah adalah sebuah perguruan tinggi di Surabaya, Indonesia yang memiliki pola ilmiah pokok iptek kelautan. Perguruan tinggi ini didirikan sebagai wujud partisipasi TNI Angkatan Laut dalam pembangunan pendidikan nasional. Universitas Hang Tuah diselenggarakan oleh Yayasan Nala, suatu badan hukum yang didirikan berdasarkan Akta Notaris R. Soedjono No. 5

tanggal 4 Maret 1987 di Surabaya dan dibina oleh TNI Angkatan Laut. Peresmian berdirinya berdasarkan Surat Keputusan Kasal No. Skep/1482/1987 tanggal 11 Mei 1987. Upacara peresmiannya oleh Kasal Laksamana Rudolph Kasenda di Jalan Teluk Bayur No. 6 Surabaya pada tanggal 12 Mei 1987. Sementara itu Teknik Elektro berdiri pada tahun 1996 dengan Status Terdaftar pada tanggal 23 Oktober 1996 berdasar Skep. Mendiknas No 506/DIKTI/Kep/1996. Jurusan Teknik Elektro mempunyai 2 (dua) konsentrasi yaitu: Konsentrasi Elektronika dan Konsentrasi Energi Listrik, dengan penambahan keilmuan dibidang listrik perkapalan dan elektronika perkapalan.

Jurusan Teknik elektro terdapat laboratorium elektronika dan didalam laboratorium tersebut terpasang jaringan komputer sebagai media untuk melakukan kegiatan praktikum oleh para mahasiswa jurusan elektro, adapun permasalahan yang ada pada jaringan komputer di laboratorium elektro adalah belum adanya sistem keamanan jaringan yang berguna untuk mendeteksi serangan yang dapat merusak jaringan komputer yang ada di laboratorium elektro.

Dalam proposal ini akan membahas tentang perancangan intrusion detection system (IDS) dalam jaringan komputer menggunakan ids bro sebagai pendeteksian dan memberikan pemberitahuan jika terjadi serangan pada jaringan komputer melalui email.

1.2. Perumusan Masalah

Dari latar belakang diatas, rumusan masalah yang dapat disimpulkan adalah:

1. Bagaimana cara mengimplementasikan *IP Tables* dan *IDS Bro* pada jaringan komputer?

2. Bagaimana cara konfigurasi agar dapat mengirimkan notifikasi email jika terjadi serangan pada jaringan komputer ?

1.3. Batasan Masalah

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

1. Sistem Operasi yang digunakan adalah *Ubuntu* versi 16.04.
2. Menggunakan aplikasi *Bro IDS* versi 2.5.1.
3. Sistem Operasi yang digunakan untuk serangan adalah *Kali Linux* versi 2017.2.
4. Terdapat 3 serangan yaitu *SYN Flood, Port Scanning* dan *SSH Bruteforce Attack.*
5. Menggunakan *IP Tables*.
6. Mengirimkan notifikasi ke email secara otomatis saat terjadi serangan.

1.4. Tujuan

Dalam hal ini tujuan yang ingin dicapai yaitu, mengetahui Teknik Implementasi Keamanan Jaringan Komputer menggunakan IP Tables dan Bro IDS (Intrusion Detection System) dengan notifikasi Email pada Laboratorium Elektro Universitas Hang Tuah Surabaya.

1.5. Manfaat

Adapun manfaat yang dapat diperoleh dari proposal tugas akhir "Implementasi Keamanan Jaringan Komputer menggunakan IP Tables dan Bro IDS (Intrusion Detection System) dengan notifikasi Email pada Laboratorium Elektro Universitas Hang Tuah Surabaya" ini adalah:

Penulis

1. Menerapkan ilmu yang diperoleh di bangku perkuliahan.
2. Memahami bagaimana teori, konsep dan praktek tentang *IP Tables* dan *Intrusion Detection Syst*em (*IDS*) *Bro* dalam keamanan jaringan komputer pada *OS ubuntu*.
3. Dapat memfilter dan mendeteksi serangan pada jaringan komputer yang terdapat pada laboratorium elektro Universitas Hangtuah Surabaya.
4. Penulis dapat menggabungkan hasil bacaan dari berbagai sumber, mengambil manfaatnya dan mengembangkan ke tingkat pemikiran yang lebih matang.

Pembaca

1. Pembaca dapat mengetahui memahami dan mampu mengimplementasikan teori konsep dan langkah–langkah penulisan skripsi dan unsur–unsurnya.
2. Pembaca dapat menambah wawasan serta dapat mengembangkan karya-karya yang baru.

3. Memberikan pemikiran tentang teknologi informasi yang bermanfaat bagi masyarakat dan pada Universitas UPN “Veteran” Jawa Timur.

Instansi

1. Membantu instansi agar memiliki keamanan jaringan pada laboratorium elektro.
2. Memberikan pemikiran tentang teknologi informasi yang bermanfaat pada Universitas Hang Tuah Surabaya.

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 Bro dan paket–paket pendukung, konfigurasi IP Tables dan Bro, simulasi serangan, analisa pendeteksian. Proses analisa dilakukan dengan membandingkan traffic normal dan traffic serangan pada log Bro yang telah membuat record aktifitas jaringan saat mulai dijalankan.

BAB V KESIMPULAN DAN SARAN

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