BAB I
PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Banyak pengguna internet yang mulai menggunakan jaringan internet nirkabel sebagai jalur akses penggunaan layanan internet, namun tingkat keamanan sistem jaringan nirkabel tidak begitu kuat. Sehingga dibutuhkan jaringan keamanan dan manajemen sistem jaringan nirkabel yang dapat memberi keamanan bagi penggunanya. Menggunakan fasilitas nirkabel ini tidaklah sepenuhnya aman dari serangan *hacker*, karena jaringan nirkabel ini tidak menggunakan enkripsi pada saat berlangsungnya komunikasi data. Sehingga memungkinkan terjadinya *hacking* seperti *Port Scanning, DoS* dan DDoS mengakibatkan kerugian bagi pengguna layanan jaringan internet nirkabel ini, contohnya pada saat kita melakukan transaksi e-banking dan menggunakan akses nirkabel, maka dibutuhkan keamanan di sisi akses masuk nirkabel yaitu akses poin, maupun keamanan di sisi server e-banking untuk melakukan sistem redundan dan sistem *blocking* saat keamanan jalur akses masuk tidak berfungsi. Salah satu cara meredam terjadinya penyusupan melalui akses jaringan nirkabel adalah menggunakan *Captive Portal* sebagai mesin autentikasi di sisi akses poin dan *Intrusion Prevention System* (IPS) di sisi server penyedia layanan.

Dengan adanya masalah tersebut diharapkan keamanan akses jaringan nirkabel dapat diperkuat dan dihasilkan sebuah rancangan infrastruktur jaringan nirkabel yang memadukan *Captive Portal* dengan *Intrusion Prevention System* (IPS) pada rangkaian redundansi *Hot Standby* yang dapat mendeteksi dan melakukan proteksi secara dini jika ada serangan berupa trafik yang berbahaya (*intruder traffic*) maupun saat server

penyedia layanan sedang down. Sehingga keamanan dan kenyamanan para pengguna akses nirkabel dapat terjamin.

1.2 RUMUSAN MASALAH

Rumusan masalah dari penelitian tugas akhir ini adalah sebagai berikut:

1. Bagaimana performansi IPS ini ketika dikombinasikan dengan sistem *Captive Portal* untuk manajemen dan keamanan jaringan.
2. Captive Portal yang akan diintergrasikan pada distro linux harus dapat kompatibel dan dapat berjalan dengan stabil.
3. Perancangan *Captive Portal* ini diharapkan dapat seefektif mungkin dalam sistem kerjanya sehingga mengurangi beban sistem IPS saat menerima serangan.
4. Perancangan pada sebuah sistem redundansi diharapkan dapat bersifat siaga jika terjadi berbagai serangan maupun saat server mangalami *failure* atau *down*.
5. Perancangan IPS harus mampu menangkal terjadinya serangan Port Scanning, DoS, dan DDoS.

1.3 TUJUAN

1. Menghasilkan sistem manajemen akses internet yang terintegrasi menjadi suatu sistem keamanan jaringan yang bersifat *redundant hot-standby* untuk mendapatkan kondisi *high availability system* .
2. Analisis performansi dan kemanan sistem yang berhasil dilakukan dengan kombinasi antara *Intrusion Prevention System* (IPS) dan *Captive Portal.*
3. Membuat sebuah sistem keamanan ganda yang kuat untuk akses sebuah server yang diakses melalui jaringan nirkabel.
4. Dapat mengkonfigurasi s*nort* yang merupakan jenis dari (IDS) *Intrussion Detection System* agar dapat menjadi sebuah sistem keamanan jaringan yang dapat mendeteksi dan memblok intrusi dalam jaringan secara otomatis.
5. Menyediakan jaringan akses yang aman dan terauthentikasi menuju *server* penting seperti untuk penggunaan transaksi bank menuju *server* bank pada tempat-tempat umum seperti cafe, hotel, dan lainnya.

1.4 BATASAN MASALAH

Pada penelitian tugas akhir ini akan dilakukan beberapa batasan masalah, diantaranya adalah sebagai berikut:

1. Server yang digunakan adalah *Web Server* dan *DNS Server* pada *Operating System Ubuntu*
2. Arsitektur Jaringan IPS dan *Captive Portal* ini menggunakan wireless router sebagai akses poin dan penyedia layanan hotspot.
3. IPS yang digunakan adalah *Snort + BlockIT*
4. Uji coba Distributed Denial of Service (DDoS) menggunakan TFN2000 (Tribe Flood Network 2000)
5. Uji coba Denial of Service (DoS) menggunakan software LOIC (Low Orbit Ion Cannon)
6. Uji coba yang dilakukan dengan menggunakan teknik *port scanning* nmap sebagai teknik *hacking*nya.
7. Tidak membahas mengenai pembuatan *web* dan konten-kontentnya.

1.5 METODE PENELITIAN

Beberapa metode yang digunakan pada penelitian tugas akhir ini adalah:

1. Melakukan studi pustaka, untuk mengumpulkan literatur dan proses pembelajaran materi melalui buku maupun jurnal-jurnal ilmiah dari berbagai sumber yang digunakan sebagai acuan penelitian tugas akhir ini.
2. Menentukan pemodelan sistem dan parameter-parameter yang digunakan untuk simulasi sehingga menghasilkan data-data pendukung penelitian.
3. Melakukan pengambilan data-data parameter dari penelitian yang telah dilakukan sebelumnya sebagai data pendukung pada penelitian tugas akhir ini.

1.6 SISTEMATIKA PENULISAN

Sistematika yang digunakan dalan penulisan proyek akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Berisi latar belakang masalah, maksud dan tujuan, perumusan masalah, batasan masalah, pemodelan sistem, metode penyelesaian masalah, dan sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini dikemukakan berbagai teori yang mendukung dalam pembuatan proyek ini diantaranya *Captive Portal*, *Intrusion Prevention System*, *Redundant Hot-standby*.

BAB III PERANCANGAN

Berisi tentang tahap-tahap perancangan dan tahap-tahap implementasi awal sistem.

BAB IV ANALISIS HASIL IMPLEMENTASI

Bab ini membahas hasil uji performansi dari Sistem keamanan yang akan dibuat.

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan akhir dan saran pengembangan Tugas Akhir.