

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Pesatnya perkembangan teknologi informasi pada saat ini, terutama munculnya jaringan internet yang dapat memberikan kemudahan dalam bertukar informasi. Semakin mudahnya mendapatkan informasi melalui jaringan internet menimbulkan masalah baru yaitu pengaksesan data atau informasi penting secara ilegal oleh pihak yang tidak bertanggung jawab maupun serangan terhadap jaringan oleh pihak dalam maupun dari luar. Sistem keamanan jaringan menjadi salah satu aspek penting yang perlu diperhatikan pada saat ini.

Dari beberapa survei yang telah dilakukan memperlihatkan telah terjadi serangan jaringan yang kebanyakan merupakan serangan *denial of service* (dos) dan *exploit buffer-overflow*. Survei juga menyebutkan ancaman yang terjadi dari pelanggaran *internal* maupun *external* hampir mempunyai perbandingan yang sama.

Semakin bertambahnya pengguna jaringan informasi, pelanggan dan meningkatnya node pada jaringan *unduk-unduk.net* harus selalu dimonitoring guna meningkatkan pelayanan terhadap pelanggan. Pelayanan merupakan salah satu faktor yang sangat penting guna memenangkan persaingan.

*Troubleshooting* yang bisa terjadi sewaktu-waktu dan *technical support* yang harus *standby* merupakan kendala yang terjadi di *unduk-unduk.net*. Dalam manajemen setiap *node client* belum adanya sistem yang dapat memberikan *report* adanya serangan jaringan kepada *technical support* guna membantu dalam

melakukan analisis terhadap masalah yang terjadi ketika mengalami *trouble* dalam jaringannya.

Dari latar belakang tersebut, penulis ingin menganalisis masalah yang dihadapi dan membuat solusi. Dengan membuat *intrusion detection system* menggunakan mikrotik berbasis *sms gateway* dan *mail report* guna memudahkan *technical support* melakukan monitoring keamanan dan pencegahan serangan jaringan dari luar maupun dalam dan analisis terhadap *trouble* pada jaringan Unduk-unduk.net Wireless Internet Service.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang masalah, dapat diambil suatu rumusan masalah sebagai berikut :

Bagaimana membangun *intrusion detection system* menggunakan mikrotik versi 5.20 yang dapat mengirim *sms* dan *email report* ke admin Undukunduk.net Wireless Internet Service ?

## 1.3 Batasan Masalah

Untuk menghindari pembahasan masalah yang terlalu luas, pada penulisan skripsi ini diberikan batasan yang jelas. Berikut batasan masalah tersebut.

1. Membangun rancangan *intrusion detection sistem* menggunakan mikrotik pada jaringan Undukunduk.net.
2. Tidak membahas uji coba jenis-jenis serangan yang dilakukan ke jaringan secara lebih mendalam.

3. Sistem *intrusion detection* yang akan dibangun menggunakan jenis *network-based IDS* (NIDS).

## 1.4 Maksud dan Tujuan

### 1.4.1 Maksud

Sebagai salah satu syarat menyelesaikan pendidikan S1 pada program studi Teknik Informatika di STMIK AMIKOM Yogyakarta.

### 1.4.2 Tujuan

Membangun *intrusion detection system* menggunakan mikrotik versi 5.20 pada Undukunduk.net Wireless Internet Service dengan memanfaatkan *firewall* pada mikrotik ketika terjadi gangguan ataupun serangan terhadap jaringan pada router. Gangguan ataupun serangan dengan cara melakukan percobaan serangan FTP Bruteforce, SSH Bruteforce, ICMP Flood, dan Port Scanner. *Firewall* pada router akan merespon dan mengirimkan notifikasi gangguan atau serangan melalui *sms* dan *email* kepada administrator jaringan Undukunduk.net.

## 1.5 Metode Pengumpulan Data

Metode pengumpulan data yang dilakukan penulis adalah sebagai berikut :

### 1.5.1 Metode Observasi

Observasi dilakukan dengan berbagai tahapan sebagai berikut :

1. Melakukan survei langsung ke Undukunduk.net Wireless Internet Service untuk mengetahui system dan model jaringan yang sedang berjalan untuk mengetahui masalah yang dihadapi.
2. Melakukan analisis tahapan temuan survey.

3. Melakukan identifikasi *hardware* dan *software*.

### 1.5.2 Metode Wawancara

Pengumpulan data yang dilakukan dengan mengadakan tanya jawab secara langsung ke administrator Undukunduk.net Wireless Internet Service guna memperoleh keterangan yang dibutuhkan untuk penelitian.

### 1.5.3 Metode Pustaka

Untuk mendukung analisis dan perancangan *intrusion detection system*, digunakan metode pustaka sebagai referensi. Pustaka yang digunakan berupa buku-buku, dokumen yang relevan, artikel-artikel dan informasi dari internet yang berkaitan dengan topik skripsi.

## 1.6 Metodologi Penelitian

Metodologi penelitian yang dilakukan penulis adalah sebagai berikut :

### 1. Analisa Sistem

Metode analisis yang digunakan untuk mengidentifikasi masalah yang terjadi dengan melakukan wawancara, selanjutnya adalah hipotesis solusi dan analisis kebutuhan sistem.

### 2. Perancangan Sistem

Melakukan konsep pemodelan sistem seperti gambaran umum sistem, perancangan topologi, perancangan *firewall*, logika *scripting* agar dapat mengirim *sms gateway* dan *email report* serta prosedur implementasi.

### 3. Konfigurasi Sistem

Proses konfigurasi sistem antara lain :

1. Konfigurasi *Network Time Protokol (NTP)*.
  2. Konfigurasi *Firewall* pada mikrotik versi 5.20.
  3. Konfigurasi penjadwalan *script* tersebut dieksekusi.
  4. Konfigurasi *script* pada mikrotik versi 5.20.
  5. Konfigurasi *tool sms* dan *tool email* pada mikrotik versi 5.20.
4. Implementasi
- Pada tahap ini dilakukan konfigurasi sub-sistem pada *PC Router* yang terinstal mikrotik versi 5.20 yang selanjutnya diintegrasikan untuk membangun *intekusion detection system*.
5. Pengujian Sistem
- Pengujian sistem dengan melakukan percobaan serangan secara *simultan* dan *stusensial* terhadap sistem, apakah sistem dapat mengirimkan *sms* dan *email report* ketika dilakukan percobaan penyerangan.
6. Evaluasi Sistem
- Evaluasi sistem dilakukan untuk mengetahui apakah sistem berjalan sesuai dengan tujuan penelitian.
7. Pemeliharaan Sistem
- Tahap pemeliharaan sistem dilakukan dengan pemantauan dan pemeriksaan rutin dengan melakukan update *firewall* agar sistem dapat beroperasi dengan baik.

### 1.7 Sistematika Penulisan

Penulisan skripsi ini mempunyai sistematika penulisan sebagai berikut :

## **BAB I PENDAHULUAN**

Bab ini merupakan pendahuluan yang menjelaskan tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode pengumpulan data, pengembangan sistem dan sistematika penulisan.

## **BAB II LANDASAN TEORI**

Bab ini menjelaskan landasan-landasan teori yang digunakan sehubungan dengan perancangan *intrusion detection system* menggunakan mikrotik berbasis *snmp gateway* dan *email report*.

## **BAB III ANALISIS DAN PERANCANGAN SISTEM**

Berisi tentang analisis sistem yang akan dibangun, perancangan dan gambaran umum sistem. Membahas tempat penelitian, identifikasi temuan masalah, hipotesis solusi, analisis kebutuhan sistem, perancangan topologi jaringan, perancangan *firewall* dan prosedur implementasi sistem.

## **BAB IV IMPLEMENTASI DAN PEMBAHASAN**

Bab ini berisi pembahasan langkah-langkah dalam penerapan sistem, konfigurasi, percobaan serangan jaringan, serta pengujian terhadap hasil penelitian apakah telah sesuai dengan tujuan penelitian dan pembahasan terhadap hasil yang telah dicapai.

## **BAB V PENUTUP**

Bab ini merupakan bagian akhir dari penulisan skripsi yang berisi kesimpulan dan saran yang diperoleh dari perancangan *intrusion detection system* menggunakan mikrotik versi 5.20 berbasis *sms gateway* dan *mail report*.

