BAB I

PENDAHULUAN

1.1 Latar Belakang

Seorang administrator diharuskan untuk mampu menjaga kestabilan dan kehandalan koneksi pada jaringannya, salah satu cara untuk menjaga kestabilan dan kehandalan koneksi yaitu dengan mengimplementasikan *Simple Network Managment System* (SNMP) pada jaringan. SNMP mampu memantau keadaan trafik dalam satu lingkup jaringan setiap saat, sehingga penyedia jasa dapat menganalisis performansi dari jaringan layanan mereka. SNMP server tentu menyimpan informasi-informasi yang sangat peting terkait dengan jaringan yang dimonitoring oleh SNMP server tersebut. Oleh karena itu SNMP server harus memiliki sebuah sistem autentikasi untuk menjaga informasi yang dimiliki tidak dapat dibaca orang lain dan hanya orang yang memiliki wewenang yang dapat mengaksesnya.

Salah satu sisten autentikasi yang banyak digunakan untuk melindungi informasi yang ada adalah menggunakan sebuah sistem *Two Factor Authentication*. Pada pengimplementasiannya, sistem *Two Factor Authentication* terkendala banyak aspek seperti mahalnya biaya pengimplementasian sistem dan tingkat kerumitan yang tinggi dalam pengimplementasian sistem tersebut.

Sistem *Two Factor Authentication* menggunakan metode *One Time Password* (OTP) merupakan suatu metode autentikasi dimana setiap klien yang hendak mengakses suatu layanan harus terlebih dahulu memasukkan sebuah *dynamic token* pada kotak autentikasi. Token menjadi bentuk pengimplentasian sistem *Two Factor Authentication* karena memiliki tingkat kompleksitas yang tidak terlalu tinggi dan biaya pengimplementasian yang lebih ekonomis.

Oleh karena itu dipilihlah *Mobile One Time Password* (MOTP) sebagai layanan autentikasi yang mendukung metode autentikasi OTP, akan tetapi MOTP merupakan sebuah layanan autentikasi yang bersifat *opensource* dan belum terstandarisasi oleh suatu institusi sehingga menimbulkan pertanyaan apakan MOTP dapat diimplementasikan pada

SNMP server dan mampu melakukan proses autentikasi dengan baik. MOTP menggunakan algoritma MD5 sebagai fungsi utama pembangkit token, dimana MD5 sangat familiar dengan isu *Collision*. Untuk itu dibutuhkan pengujian untuk menguji *Collision Vulnerability* pada metode autentikasi MOTP[1].

1.2 Tujuan Penelitian

Berdasarkan latar belakang permasalahan yang telah dijelaskan di atas, maka tujuan dari penelitian ini adalah:

1. Menganalisis performa dari MOTP dilihat dari CPU *Usage*, RAM *Usage*, dan *Delay authentication.*
2. Menganalisis *Collision Vulnerability* MOTP pada token yang dihasilkannya.
3. Memberi fitur tambahan pada MOTP berupa pembatasan durasi *login* dan pembatasan otoritas klien.

1.3 Manfaat Penelitian

Manfaat yang diharapkan akan diperoleh dalam melakukan penelitian ini adalah:

1. Dengan memahami cara kerja dari dan sistem autentikasi OTP diharapkan menjadi solusi dalam pemilihan sistem autentikasi pada SNMP server.
2. Memahami pengaruh pemasangan metode autentikasi OTP pada suatu sistem.
3. Mengetahui performansi metode autentikasi MOTP.
4. Mengetahui kelemahan dari metode autentikasi OTP.

1.4 Rumusan Masalah

Berdasarkan tujuan di atas, maka masalah yang ada dapat dirumuskan sebagai berikut:

1. Bagaimanakah merancang sebuah sebuah sistem autentikasi *Two Factor Authentication* pada sebuah SNMP server?
2. Apakah dengan pemasangan metode autentikasi OTP dapat mempengaruhi sistem yang lain?

1.5 Batasan Masalah

Dalam Tugas Akhir ini dilakukan beberapa pembatasan masalah diantaranya adalah:

1. SNMP yang digunakan adalah SNMP versi 1.

2. Jenis OTP yang digunakan adalah *Mobile One Time Password* (MOTP).
3. Tidak membahas serangan aktif yang terjadi pada SNMP server.
4. Jenis token yang digunakan adalah token dengan *Time Synchronized.*
5. Menggunakan telepon genggam sebagi pembangkit token.
6. Analisis difokuskan pada karakteristik dari token yang dihasilkan MOTP.
7. SNMP hanya memonitoring sebuah server *Cloud*
8. Analisis difokuskan pada keamanan sistem autentikasi bukan pada keamanan pengiriman token
9. Menggunakan trafik *streaming* pada server *Cloud* sebagai pembangkit trafik

1.6 Metode Penelitian

Sistematika penulisan Tugas Akhir ini disusun dalam lima bab sebagai berikut:

BAB I : PENDAHULUAN

Berisi latar belakang, tujuan dan manfaat penelitian, perumusan dan pembatasan masalah, metode penelitian yang dilakukan dan sistematika penulisan.

BAB II : DASAR TEORI

Berisi teori-teori dasar tentang sistem *Two Factor Authentication*, *Mobile One Time Password* , SNMP dan teori lainnya yang digunakan untuk menganalisis karakteristik OTP dan cara kerjanya.

BAB III : PERANCANGAN SISTEM

Berisi tahap-tahap perancangan implementasi *Two Factor Autentication* menggunakan metode autentikasi OTP pada SNMP server. Dimulai dari penentuan jenis OTP yang akan digunakan, penetuan aplikasi yang mendukung OTP pada SNMP server, instalasi dan konfigurasi.

BAB IV : PENGUJIAN dan ANALISIS

Berisi pengujian terhadap sistem dan analisis mengenai OTP yang digunakan terhadap hasil yang diperoleh dari tahap perancangan dan implementasi sistem.

BAB V : PENUTUP

Berisi kesimpulan atas hasil pengujian dan evaluasi yang telah dilakukan, beserta saran dan rekomendasi untuk pengembangan dan perbaikan penelitian selanjutnya.