

# **BAB I**

## **PENDAHULUAN**

### **1.1. Latar Belakang Masalah**

Di arus globalisasi pada saat ini dimana teknologi telah berkembang dengan pesatnya, hampir semua aspek kehidupan masyarakat dan ilmu pengetahuan telah terkontaminasi dengan teknologi itu sendiri, sebagai contoh digunakannya sarana-sarana berteknologi tinggi, diantaranya teknologi dan informasi dalam bidang komputer dan jaringan, yang kemudian perkembangan ini membawa perubahan dalam kehidupan manusia sehari-hari bahkan banyak *software* yang dibuat untuk membantu kebutuhan pengguna namun pengguna, tidak menyadari jika aplikasi yang digunakan dapat menjadi sebuah *vulnerability* atau celah yang berbahaya bagi pengguna dan memungkinkan akan terjadi eksploitasi pada suatu saat dari kelemahan aplikasi tersebut dan mengambil keuntungan dari sistem yang tereksploitasi.

Pada penelitian ini akan melakukan sebuah *buffer Overflow* yang digunakan untuk melakukan eksploitasi dengan cara mengirim kode – kode yang melebihi kapasitas

dari memori untuk melakukan *buffer* pada aplikasi tersebut, ini dilakukan dengan cara mentransfer atau mengirimkan sebuah *fuzzer* untuk menemukan sebuah *vulnerbility* pada aplikasi tersebut.

### **1.2. Rumusan Masalah**

Berdasarkan latar belakang permasalahan diatas, maka rumusan masalahnya adalah bagaimana mengetahui *vulnerbility* pada aplikasi di *windows*, serta mengetahui rentang kelemahan aplikasi.

### **1.3. Ruang Lingkup**

Untuk mengetahui *vulnerbility* ini maka dibuat beberapa lingkup permasalahan yang meliputi :

- a. Membuat sebuah *fuzzer* menggunakan bahasa *python*
- b. Proses Penetrasi.
- c. Mengetahui *vulnerbility* aplikasi pada windows yaitu:
  - *Cool Player*
  - *RM-MP3 Converter*

#### 1.4. Tujuan Penelitian

Penelitian ini bertujuan untuk seseorang mencari *Vulnerbility* yang meliputi :

- a. Menemukan dan mempelajari sebuah *vulnerbility* pada aplikasi.
- b. Melakukan Penimpaan pada Register EIP agar terjadi *error* dan kemudian akan di lakukan *exploitasi* agar bisa memata-matai sistem.
- c. Informasi dan dampak terjadinya eksploitasi pada suatu sistem dan aplikasi.