BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini yang sedemikian pesatnya terutama dalam dunia teknologi informasi dan komunikasi terlebih dalam bidang komputer dan jaringan, yang kemudian perkembangan ini membawa perubahan dalam kehidupan manusia sehari-hari bahkan ada banyak *softwere* dan aplikasi yang dibuat dengan tujuan untuk membantu seorang pengguna, namu seorang pengguana terkadang tidak menyadari jika aplikasi yang digunakan dapat menjadi sebuah *vulnerability* atau celah yang berbahaya bagi pengguna dan memungkinkan akan terjadinya eksploitasi pada suatu saat dari kelemahan aplikasi tersebut dan mengambil keuntungan dari sistem yang telah tereksploitasi. Ada berbagai macam contoh aplikasi atau perangkat lunakyang digunakan pada komputer-komputer yang menggunakan sistem *windows* seperti aplikasi *VU Player* dan M*ini-Stream RM-Mp3* begitu banyaknya yang menggunakan aplikasi tersebut, dalam penulisan tugas akhir ini mengapa tidak menggunakan aplikasi yang ada

dalam bawaan dari *windows* tersebut dalam alasan pemilihan aplikasi tersebut adalah karena pada umumnya seorang pengguna suka untuk menggunakan aplikasi tambahan yang di instal oleh pemiliknya sendiri.

Pada penelitia ini akan melakukan sebuah *buffer ofervlow* yang digunakan untuk melakukan eksploitasi dengan cara mengirim kode-kode yang melebihi kapasitas dari *memory* aplikasi untuk melakukan sebuah *buffer* pada aplikasi tersebut, ini dilakukan dengan cara mentranfer atau mengirimkan sebuah *fuzzer* untuk menemukan suatu *vulnerability* pada aplikasi tersebut. *Buffer overflow* adalah merupakan sebuah proses yang terjadi didalam sistem *memory* komputer, dimana terdapat sebuah proses yang tidak normal pada saat melakukan penyimpanan data sementara dalam *memory* (Mada R. Perdana 2011). Ini terjadi pada saat data-data yang akan disimpan melebihi kapasitas *buffer* pada *memory.*

Fuzzer adalah suatu proses metode yang digunakan untuk menemukan sebuah kesalahan logika dan kegagalan proses pengolahan data pada sebuah aplikasi dan melihat serta mempelajari bagaimana aplikasi

menangani proses exception (Mada R. Perdana 2011). Dengan menggunakan *Ollydbg* kita dapat mengetahui sebuah *vulnerability* yang ada di dalam aplikasi tersebut dan kemudia akan dimasukan sebuah *shellcode* untuk mengontrol sistem dengan aplikasi yang tereksploitasi tersebut. Eksploitasi adalah sebuah kode yang digunakan untuk melakukan sebuah penetrasi baik secara legal maupun ilegal untuk mencari dan mengetahui *vulnerability* pada aplikasi atau komputer. *Shellcode* adalah suatu bagian kecil dari kode yang digunakan untuk eksploitasi. Adapun dampak apabila aplikasi dapat tereksploitasi adalah kita dapat dengan bebas mengontrol sistem secara keseluruhan melalui *CMD* dan mengambil data dari komputer tersebut dapat juga menghapus data yang ada dalam komputer tersebut, melihat proses yang sedang berjalan dan mematikan proses yang sedang berjalan. Adapun langkah untuk mencegah terjadinya eksploitasi tersebut adalah seperti mengupdate aplikasi yang digunakan, berhati-hati dalam menggunakan jaringan umum, mengupdate antivirus yang digunakan kemudian selalu mengaktifkan *filrewall.*

1.2 Rumusan Masalah

Bagaimana cara untuk menemukan dan mengetahui *vulnerability* yang ada di dalam latar belakang tersebut maka akan dilakukan studi kasus pada aplikasi *VU Player* dan *Mini-Stream RM-mp3 converter* untuk mengetahui *vulnerability* pada aplikasi tersebut.

1.3 Ruang Lingkup

Dalam penelitian tugas akhir ini mengambil sebuah judul Pengembangan Program *Fuzzer* untuk Mengetahui *Vulnerability* Aplikasi *Windows* dalam penelitian ini hasil yang akan dikeluarkan adalah sebuah informasi dan bahayanya jika terjadinya eksploitasi pada sebuah sistem atau aplikasi dan manfaat bagi *user* sendiri adalah sebuah saran untuk lebih berhati-hati dalam penggunaan aplikasi, dan ruang lingkup yang akan di bahas adalah sebagai berikut:

1. Membuat sebuah *fuzzer* dengan menggunakan bahasa *python* untuk melakukan *buffer overflow* pada aplikasi.
2. Mengirim sebuah *fuzzer* untuk melihat *vulnerability* pada aplikasi tersebut dengan menggunakan *Ollydbg.*
3. Membuat sebuah data *dummies* yang telah terstruktur dengan menggunakan *pattern_creabe.rb*

4. Menghitung besarnya *byte* dari kumpulan *pattern* yang dihasilkan oleh *pattern_creab.rb*
5. Mencari alamat JMP ESP (batu loncatan)
6. Membuat *payload* untuk kemudian dimasukan kedalam *fuzzer* untuk mengontrol sistem windows melalui *CMD.*

1.4 Tujuan

Dalam penelitian ini bertujuan bagaimana seseorang mencari, menemukan dan mempelajari sebuah *vulnerability* pada aplikasi yang kemudian akan dilakukan proses eksploitasi dan kemudian digunakan untuk mengontrol sistem. Dan juga akan memberikan informasi dan dampak jika terjadinya eksploitasi pada suatu sistem atau aplikasi. Dan menyarankan pada setiap pengguna aplikasi untuk terus mengupdate aplikasi yang digunakan untuk menghindari terjadinya eksploitasi.