BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring pesatnya kemajuan teknologi informasi khususnya di bidang teknologi komputer dan jaringan, Software dan Aplikasi semakin banyak di ciptakan guna untuk membantu dan mempermudah pengguna. tetapi aplikasi ini bisa jadi celah berbahaya tanpa disadari yang memungkinkan terjadinya *eksploitasi* dari kelemahan yang ada, yang kemudian mengambil keuntungan dari sistem yang telah *tereksploitasi*. *Eksploit* adalah sebuah kode yang menyerang keamanan komputer secara spesifik. *Exploit* banyak digunakan untuk penetrasi baik secara legal ataupun ilegal untuk mencari kelemahan (Vulnerability) pada komputer *victim*.

Salah satu aplikasi perangkat lunak yang banyak digunakan baik diperkantoran maupun individu yaitu *BigAnt server* dan *Winamp*. Karena aplikasi ini begitu familiar, hal ini lah yang menyebabkan penulis mempelajari kelemahan terhadap aplikasi tersebut. Aplikasi *BigAnt server* atau bisa disebut juga dengan *server messaging*. Cara kerja apllikasi ini melakukan

transfer file dari PC ke PC dan juga bisa mentransfer folder dengan beberapa kontak sekaligus.

Disini penulis akan melakukan *buffer overflow* yang sering sekali di *exploitasi* dengan cara mengirimkan input – input yang berlebih dari kapasitas memory *buffer* pada aplikasi. Dengan cara mengirimkan *fuzzer* yang memungkinkan aplikasi memberikan celah atau bug pada aplikasi tersebut, dan dengan menggunakan *ollydbg* kita dapat melihat *vulnerability* dalam memory aplikasi. Sehingga dapat memasukkan *shellcode* untuk mengontrol sistem melalui aplikasi yang telah *terexploitasi*.

1.2 Rumusan Masalah

Permasalahan yang terdapat dalam studi kasus ini adalah melakukan *buffer overflow* pada aplikasi *Bigant server* dan *Winamp*.

1.3 Ruang Lingkup

Dalam pembuatan Tugas Akhir ini dengan judul *vulnerability development* dan mengkonfigurasikannya ini sangat beragam bentuk dan jenis yang dapat dibuat, sehingga dalam pembuatan Tugas Akhir ini penulis memberikan ruang lingkup yang akan dibahas adalah sebagai berikut :

1. Membuat *fuzzer* atau di sebut juga dengan *fuzzing* dengan menggunakan bahasa *python* untuk memancing *buffer overflow*pada aplikasi.
2. Membuat payload yang akan dimasukkan ke dalam fuzzer dan di gunakan untuk mengontrol sistem.
3. Mengontrol sistem windows XP secara keseluruhan.

1.4 Tujuan

Penelitian ini bertujuan untuk bagaimana teknik seorang attacker untuk mencari vulnerability pada aplikasi. Dan dalam studi kasus ini adalah aplikasi Bigant server dan winamp.