BAB 1. PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan merupakan aspek terpenting pada sebuah jaringan. Terkadang untuk masalah keamanan jaringan masih dipandang sebelah mata oleh administrator jaringan. Padahal aspek tersebut cukup vital dalam pengembangan infrastruktur suatu organisasi yang memiliki ketergantungan di dunia IT.

Peran pertahanan sistem, pada umumnya terletak pada administrator sebagai pengelola jaringan yang memiliki akses penuh terhadap infrastruktur jaringan yang dibangunnya. Khususnya keamanan terhadap sebuah *server*. *server* memainkan peranan penting dalam jaringan. Ancaman keamanan pada *server* sangat beragam, mulai dari *scanning port* hingga *exsploitasi*. Untuk mengatasi masalah tersebut dibutuhkan sistem keamanan jaringan yang dapat mendeteksi segala sesuatu yang akan mengancam *server*.

Honeypot merupakan solusi terbaru dari segi keamanan, dalam terminologi komputer, *honeypot* adalah sebuah *server* palsu (perangkap) yang dibuat untuk mendeteksi, membelokkan atau dalam beberapa cara, melawan upaya penggunaan yang tidak sah dari sistem informasi.

Pada tugas akhir ini, penulis mengimplementasikan sebuah aplikasi *Honeypot* berbasis *opensource* yaitu *dionaea*. *dionaea* merupakan salah satu bentuk *low-interaction honeypot* terbaru, *dionaea* adalah perangkat lunak yang menawarkan layanan jaringan yang dapat di *eksploitasi*.

Dalam tindakannya untuk menjebak dan mengumpulkan informasi dari *attacker*, *dionaea* bertujuan untuk mendapatkan salinan *code malware*. Sehingga dengan mengimplementasikan *honeypot* sebagai sistem keamanan, dapat memudahkan administrator dalam menganalisa serta mempelajari aktifitas-aktifitas yang mempunyai kecenderungan membahayakan sistem sesungguhnya. Dari permasalahan tersebut maka penulis mengambil judul tugas akhir "Impelementasi *Honeypot dionaea* Pada *Server* Sebagai Penunjang Keamanan Jaringan"

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dapat diperoleh beberapa rumusan masalah yaitu :

a. Bagaimana cara *dionaea* dalam menjebak *attacker* ?
b. Bagaimana *dionaea* dalam mengidentifikasi jenis serangan ?
c. Bagaimana *dionaea* dalam mendapatkan salinan *code malware* ?

1.3 Batasan Masalah

Batasan masalah dalam pengerjaan tugas akhir ini adalah sebagai berikut :

a. *Honeypot* yang digunakan adalah bentuk *low-interaction honeypot*, sehingga informasi yang didapat terbatas.
b. *Tool honeypot* yang digunakan adalah *dionaea*, yang memiliki keistimewaan dalam mendeteksi serangan berupa *malware*
c. Tidak membahas dan membuat antivirus.

1.4 Tujuan

Tujuan pembuatan tugas akhir ini adalah menciptakan keamanan pada sebuah *server*, dengan membangun sebuah *server* palsu menggunakan Metode *Honeypot dionaea*, yang akan dijadikan sebuah target serangan. dimana *dionaea* memiliki keistimewaan dalam menjebak dan menangkap salinan *code malware*, Berdasarkan layanan *port* yang di exsploitasi.

1.5 Manfaat

a. Memudahkan administrator jaringan dalam memonitori maupun mengidentifikasi jenis serangan.
b. Melindungi sistem yang sesungguhnya (*server)* dari serangan *hacker*. Sehingga dapat membuat sistem keamanan yang lebih baik lagi.