

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kebutuhan dan penggunaan akan teknologi informasi yang diaplikasikan dengan Internet dalam segala bidang seperti *e-banking*, *e-commerce*, *e-government*, *e-education* dan lain sebagainya telah menjadi sesuatu yang tidak asing lagi. Internet telah menciptakan dunia baru yang dinamakan *cyberspace* yaitu sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru berbentuk virtual. Kita dapat seolah-olah ada di tempat tersebut dan melakukan hal-hal yang dilakukan secara nyata, misalnya berinteraksi, berdiskusi dan lain sebagainya.

Pemanfaatan jaringan internet untuk memudahkan komunikasi antar manusia di dunia sudah sangat meluas. Misalnya saja penggunaan internet pada media sosial, media pemberitaan, media jual-beli, dan media lainnya yang dilakukan secara *online*. Di mana kita ketahui media – media tersebut merupakan media penghubung antar banyak pihak dan juga merupakan media yang memungkinkan untuk dapat diakses oleh semua orang melalui internet. Dengan semakin tingginya tingkat kompleksitas penggunaan jaringan komputer, maka semakin tinggi pula ancaman yang ada. Misalnya saja untuk mengambil alih hak akses komputer lain sebagai *user*, penyerang dapat melakukan kontrol jarak jauh atau *remote* melalui *port ssh* dari komputer yang akan di-*remote*. Dan apabila hal ini dilakukan oleh para pelaku *cybercrime* tentunya dapat merugikan pihak – pihak tertentu. Untuk itu dalam penelitian ini akan dikembangkan sebuah *kippo honeypot* yang merupakan emulasi dari *port ssh*. Teknik *brute-force* memang merupakan sebuah teknik usang yang masih sering menjadi andalan para pelaku *cybercrime* dalam mencari hak akses utama menuju suatu aplikasi komputer.

Brute force bekerja dengan cara menginputkan semua kombinasi *username* dan *password* secara acak dalam jumlah banyak dan dalam kurun waktu yang cepat untuk mendapatkan kombinasi *username* dan *password* yang memang telah tercatat oleh sistem yang akan diserang.

Honeypot sendiri merupakan sebuah sistem yang di bangun menyerupai dengan sistem yang sesungguhnya, dengan tujuan agar para *attacker* teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut.

Pada tugas akhir ini berkaitan dengan analisa dan implematasi *honeypot kippo ssh* yang mampu memberikan laporan aktivitas serangan jaringan kepada administrator, sehingga dapat dipelajari pola serangan yang terjadi terhadap jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang ada maka dapat dirumuskan berapa pemasalahan yang ada yaitu :

1. Bagaimana mengimplementasikan *Honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan?
2. Bagaimana melakukan analisa kinerja *honeypot* menggunakan *kippo* terhadap serangan *attacker*?

1.3 Batasan Masalah

Untuk pembuatan tugas akhir ini agar sesuai dengan judul yang telah dibuat, maka penulis akan memberikan batasan-batasan masalah yang akan dibahas antara lain :

1. Metode pengamanan jaringan yang digunakan adalah *honeypot* menggunakan *kippo*.
2. Pengujian pada sistem *honeypot* yang telah dibuat menggunakan jenis serangan *bruteforce*.

1.4 Tujuan

Adapun tujuan dari tugas akhir ini antara lain:

1. Merancang dan menciptakan *honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan.
2. Melakukan analisa kinerja *honeypot* menggunakan *kippo* terhadap serangan *attacker*.

1.5 Manfaat

Manfaat dari penelitian tugas akhir yang dilakukan oleh penulis adalah sebagai berikut:

1. Dapat memberikan gambaran tentang kinerja metode *honeypot kippo* sebagai system keamanan jaringan komputer.
2. Dapat memberikan informasi kepada administrator jaringan tentang teknik atau pola – pola serangan yang digunakan oleh *attacker* yang nantinya akan dianalisa lebih lanjut untuk menemukan solusi yang tepat dalam menangani keamanan suatu jaringan komputer.
3. Manfaat lainnya dapat di jadikan acuan untuk pengembangan selanjutnya dengan menggunakan teknologi yang berbeda-beda.