

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan Internet yang semakin hari semakin meningkat baik teknologi dan penggunaannya, membawa banyak dampak baik yang bersifat positif maupun yang bersifat negatif. Dampak positif misalnya jaringan Internet saat ini dapat membantu manusia untuk saling berkomunikasi serta bertukar informasi, Namun tidak sedikit juga dampak negatif yang ditimbulkan karena adanya Internet, misalnya seorang *hacker* dapat masuk ke dalam suatu sistem jaringan untuk mencuri data dan informasi penting. Maka dari itu diperlukan adanya sistem keamanan jaringan komputer

Keamanan jaringan komputer adalah suatu proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dalam jaringan komputer. Langkah-langkah pencegahan dapat membantu menghentikan pengguna yang tidak sah yang disebut penyusup untuk mengakses setiap bagian dari sistem jaringan komputer. Salah satu metode untuk mengamankan jaringan adalah dengan *Honeypot*.

Honeypot 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. *Honeyd* adalah sebuah produk *honeypot* yang dibuat oleh Niels Provos. Inti dari *Honeyd* adalah sistem ini akan mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya. *Honeyd* memiliki kemampuan untuk mensimulasikan TCP dan UDP selain itu sistem ini mampu memahami dan merespon ICMP dengan baik,serta memiliki kemampuan untuk membuat *virtual honeypot* dengan nomor IP yang banyak secara bersamaan.

Pada penelitian ini akan diimplementasikan sebuah sistem *Honeypot* menggunakan *Honeyd* 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 permasalahan yang ada yaitu :

1. Bagaimana mengimplementasikan metode *Honeypot* sebagai solusi dalam mengatasi masalah pada keamanan jaringan?
2. Bagaimana melakukan analisa kinerja *honeypot* menggunakan *honeyd* terhadap serangan yang dilakukan oleh *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 aplikasi *Honeyd*.
2. *Honeyd* akan membuat 3 *Host* Palsu yaitu Windows, Linux, dan Router Cisco.
3. *Service* yang digunakan dalam *Host* antara lain : *web server*, *ftp server*, *telnet server*, dan *ssh server*.
4. Pengujian pada sistem *Honeypot* yang telah dibuat menggunakan jenis serangan : *Footprinting*, *DoS*, dan *Bruteforce*.

1.4 Tujuan

1. Mengimplementasikan *Honeypot* Menggunakan *Honeyd* Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan.
2. Melakukan analisa kinerja *honeypot* menggunakan *honeyd* terhadap serangan yang dilakukan oleh *attacker*.

1.5 Manfaat

1. Dapat memberikan gambaran tentang kinerja metode *Honeypot* sebagai sistem 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.