BAB 1
PENDAHULUAN

1.1 Latar Belakang

Semakin luas teknologi saat ini membuat banyak orang dengan mudahnya memanfaatkan teknologi khususnya jaringan internet sebagai tempat untuk mendapatkan informasi. akan tetapi, keamanan dalam hal teknologi jaringan internet dirasa masih kurang diperhatikan. Keamanan yang kurang dapat mengakibatkan banyak kerugian bagi perusahaan atau instansi yang memanfaatkan jaringan internet sebagai tempat untuk melakukan pertukaran *data*, sehingga banyak peretas atau oknum yang tidak bertanggungjawab di dunia maya dengan mudahnya mencuri dan mengetahui informasi – informasi penting yang ada di sistem komputer, hal tersebut dapat terjadi karena didalam jaringan internet tersebut tidak memiliki *port* yang dapat mengamankan jaringan internet.

SSH *(Secure Shell)* merupakan salah satu *port* yang dapat melindungi akses *remote* jaringan ke *server* dengan cara menyediakan *path* komunikasi yang sudah dienksripsi agar dapat men*transmisi*kan *data* komputer klien dengan komputer *server* melalui jaringan internet. SSH dapat digunakan untuk melindungi *file transfer,* membuat *command shell* aman *(remote login)* dan *port forwarding.* SSH nantinya akan melakukan otentikasi terhadap komputer *client* dengan menggunakan *username* dan *password* yang sudah di enkripsi, SSH akan dirancang dengan menggunakan *Kippo Honeypot*. *Kippo Honeypot* merupakan salah satu *tools honeypot* SSH yang termasuk ke dalam jenis *medium-interaction* yang dapat mengamankan komputer *server* asli dari serangan peretas, *Kippo Honeypot* digunakan sebagai sistem tiruan yang sengaja dibuat untuk menjebak peretas yang ingin mencoba masuk ke sistem komputer asli. *Admin*(pengguna) juga dapat melihat/mendeteksi aktifitas *log* dan interaksi seluruh *shell* yang dilakukan oleh peretas dalam melakukan serangan terhadap sistem komputer palsu dengan menggunakan *Web Interface Kippo Graph*.

Karena permasalahan tersebut, dibuatlah "Implementasi Keamanan SSH menggunakan Kippo" yang dikonfigurasi untuk mengamankan jaringan ssh dari serangan peretas dengan menggunakan *tools kippo honeypot* dan juga untuk mengetahui serangan apa saja yang dapat dilakukan oleh peretas di jaringan sistem komputer *server*.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dari proyek akhir ini sebagai berikut :

1. Bagaimana mengimplementasikan keamanan SSH dengan menggunakan Kippo Honeypot ?
2. Bagaimana mengetahui/mendeteksi aktifitas serangan yang dilakukan oleh penyerang ?

1.3 Tujuan

Tujuan dari penulisan proyek akhir ini sebagai berikut :

1. Dapat mengimplementasikan keamanan SSH dengan menggunakan Kippo Honeypot.
2. Dapat mengetahui/mendeteksi aktifitas serangan yang dilakukan oleh penyerang.

1.4 Batasan Masalah

Batasan masalah dari penulisan proyek akhir ini sebagai berikut :

1. Menggunakan Sistem Operasi Debian server.
2. Menggunakan Kippo Honeypot sebagai sistem *server* tiruan.
3. menggunakan Kippo Graph untuk mendeteksi/mengetahui hasil *log* yang dilakukan penyerang melalui *web interface*.
4. Pengujian serangan hanya menggunakan tiga teknik serangan yaitu; *Brute force attack, Dos attack, dan Dictionary attack*.
5. Menggunakan jaringan *IP Public* untuk melakukan pengujian terhadap serangan.

1.5 Definisi Operasional

Secure Shell atau SSH adalah salah satu *port* yang digunakan untuk mengamankan komunikasi data antar *host* di dalam jaringan dengan cara menggunakan teknik kriptografi.

Kippo merupakan salah satu *tools honeypot* yang dapat digunakan untuk mengamankan jaringan *port* ssh dari serangan peretas. Kippo honeypot termasuk dalam kategori *medium-interaction* yang dapat digunakan untuk mencatat serangan dan interaksi *shell* yang dilakukan penyerang dengan cara membuat *server* palsu untuk menjebak penyerang yang ingin mencoba masuk ke dalam sistem komputer *server* asli. Untuk melihat *log shell* tersebut digunakan Kippo Graph yang dapat menampilkan aktifitas yang dilakukan penyerang melalui *web interface*.

1.6 Metode Pengerjaan

Pada proyek akhir ini menggunakan metode pengerjaan sebagai berikut :

1. Studi Literatur

   Yaitu proses pengumpulan data berupa referensi jurnal, internet dan buku yang ada di perpustakaan. Serta diskusi dengan dosen atau orang – orang yang paham mengenai topik proyek akhir ini.

2. Analisis Kebutuhan Sistem

   Menganalisis kebutuhan yang diperlukan untuk pembangunan sistem yang akan dibuat berupa kebutuhan *hardware* dan *software*.

3. Perancangan Sistem

   Tahap ini merupakan proses perancangan terhadap sistem yang akan dibangun pada proyek akhir ini.

4. Implementasi Sistem

   Tahap dilakukannya implementasi berdasarkan rancangan yang telah dibuat sebelumnya berupa instalasi dan konfigurasi terhadap sistem yang akan dibangun.

5. Pengujian dan Hasil

   Pada tahap ini dilakukan pengujian untuk melihat hasil dari implementasi yang telah dilakukan dalam pembuatan sistem pada proyek akhir ini.

1.7 Jadwal Pengerjaan

Tabel 1. 1. Jadwal Pengerjaan

WAKTU PENGERJAAN PROYEK AKHIR																				
NO	KEGIATAN	Maret 2017				April 2017				Mei 2017				Juni 2017				Juli 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																				
2	Analisis Kebutuhan Sistem																				
3	Perancangan Sistem																				
4	Implementasi Sistem																				
5	Pengujian dan Hasil																				