BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi internet telah menjadikan salah satu media utama pertukaran informasi. Tidak semua informasi bersifat terbuka untuk umum. Karena internet merupakan jaringan komputer yang bersifat publik, maka diperlukan suatu usaha untuk menjamin keamanan informasi tersebut. Untuk saat ini saja, penyerangan terhadap aplikasi *web* telah melebihi 60% [17]. Begitu pula dengan adanya serangan yang belum di ketahui atau yang sering disebut zero day exploit. Oleh karena itu, diperlukan suatu sistem yang mampu mendeteksi usaha-usaha dan pola penyusupan tersebut.

Honeypot adalah suatu sistem yang didesain menyerupai *production system* asli dan dibuat dengan tujuan untuk diserang / disusupi. Karena *honeypot* bukan merupakan *production system* asli, maka hanya sedikit atau bahkan tidak ada sama sekali trafik jaringan yang berasal dari atau menuju *honeypot*. Oleh karena itu, semua trafik *honeypot* patut dicurigai sebagai aktivitas yang tidak sah atau tidak terautorisasi. Hal tersebut memungkinkan untuk dilakukan pendeteksian terhadap usaha-usaha tersebut dengan cara melakukan pengawasan (*monitoring*) terhadap sistem *honeypot*.

Untuk menghadapi masalah keamanan jaringan sebenarnya juga dapat menggunakan firewall. Namun firewall yang ada dirasa kurang baik, karena firewall hanya memblokir jaringan yang di lakukan oleh peretas, sehingga tidak dapat mendeteksi serangan yang terjadi beserta pola serangan yang dilakukan oleh peretas.

Server adalah sebuah sistem yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* dapat digunakan untuk implementasi sistem *high interaction honeypot* yang dibuat untuk sengaja diserang tanpa mengakibatkan resiko dan dampak buruk bagi *web server* yang sesungguhnya.

Oleh sebab itu dipersiapkan suatu pengamanan untuk *web server* yaitu sistem *high interaction honeypot* yang diimplementasikan pada *web server* palsu untuk menjadi perangkap dari peretas serta membantu mengamankan *web server* yang sesungguhnya.

1.2 Rumusan Masalah

Dari latar belakang yang sudah ada, maka didapatkan rumusan masalah sebagai berikut:

1. *Server* dengan keamanan *firewall* saja sangat mudah untuk diretas.
2. *Low interaction honeypot* memiliki kekurangan dalam menyimulasikan celah keamanan.
3. Tingkat keamanan yang dimiliki oleh *high interaction honeypot*.

1.3 Tujuan

Untuk mengatasi masalah yang ada, maka disusun tujuan proposal yaitu antara lain:

1. Menerapkan *high interaction honeypot* untuk keamanan *web server*.
2. Membuat sistem *high interaction honeypot* pada *web server*.
3. Melakukan analisis tingkat kemanan *server* yang diberi pertahanan *honeypot*.

1.4 Batasan Masalah

Sedangkan batasan masalah untuk penyusunan proposal ini adalah:

1. Diimplementasikan pada *web server* berbasis sistem operasi LINUX.
2. Pembuatan *web server* menggunakan TikiWiki.
3. Menggunakan 1 buah *server* utama.
4. Tidak membahas keamanan *firewall* pada sistem *honeypot* ini.
5. Metode pengujian yang diterapkan adalah *directory buster brute force*, *denial of service*, *remote file inclusion* dan *SQL injection*.
6. Menggunakan metode *high interaction honeypot*.

1.5 Metodologi Penelitian

Metodologi yang digunakan dalam memecahkan masalah di atas adalah dengan menggunakan langkah-langkah berikut:

1. Tahap Studi Literatur

Tahap awal ini melakukan pendalaman materi, penelitian, serta pekerjaan yang terkait dengan tugas akhir ini. Referensi tersebut berasal dari berbagai macam

sumber seperti jurnal, buku dan artikel resmi dari internet. Juga melakukan diskusi materi dengan dosen pembimbing maupun dengan orang yang berkompeten mengenai *honeypot*.

2. Tahap Perancangan Sistem

Melakukan perancangan, pemodelan, dan konfigurasi pada sistem yang akan diuji. Perancangan dan konfigurasi dilakukan pada sistem satu jaringan yang memuat *web server* asli dan *honeypot* pada *web server*.

3. Tahap Implementasi dan Pengumpulan Data

Mengumpulkan data-data hasil pengujian dari parameter dan metrik yang telah ditentukan dari hasil implementasi.

4. Tahap Analisis dan Penarikan Kesimpulan

Melakukan analisis dari data yang telah didapat. Data tersebut berasal dari implementasi pengujian tahap sebelumnya. Setelah mendapat data maka langkah selanjutnya adalah menarik kesimpulan.

5. Tahap Penyusunan Laporan Tugas Akhir

Tahap akhir dari penelitian ini adalah pembuatan dokumentasi laporan tugas akhir dan sidang tugas akhir.

1.6 Sistematika Penulisan

Penulisan laporan tugas akhir ini dibagi dalam beberapa bagian. Tiap-tiap bagian menjelaskan langkah demi langkah dalam pengerjaan tugas akhir ini. Berikut ini adalah bagian dari laporan tersebut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang penelitian dari tugas akhir, rumusan masalah, tujuan tugas akhir, batasan masalah dari judul tugas akhir, metodologi penelitian, serta sistematika penulisan yang digunakan dalam tugas akhir ini.

BAB II LANDASAN TEORI

Bab ini terdiri dari teori-teori dan materi dari berbagai sumber-sumber terkait yang digunakan dalam sistem yang dibuat, bersumber dari jurnal, artikel, maupun buku resmi yang ada di internet.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Bab ini membahas mengenai semua hal yang berkaitan dengan proses pemodelan, perancangan, serta implementasi per tiap bagian - bagian sistem seperti yang telah disebutkan dalam metodologi.

BAB IV PENGUJIAN DAN ANALISIS SISTEM

Bab ini berisi hasil implementasi dari perancangan Tugas Akhir serta mengikutsertakan hasil uji coba dari *system* yang dibuat dan telah dicapai dalam Tugas Akhir ini.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan akhir yang dapat diambil dari Tugas Akhir ini beserta saran dan harapan untuk pengembangan penelitian lebih lanjut.