BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan dunia internet membuat penyedia layanan harus mempertimbangkan banyaknya pengguna yang terus bertambah. Sebuah server pasti memiliki keterbatasan dalam kemampuan menangani pengguna internet. Salah satu cara untuk mengatasi hal tersebut adalah mengganti server dengan yang lebih canggih yang mungkin dapat memakan biaya yang cukup banyak. Namun penambahan server-server yang tidak terlalu canggih bisa menjadi alternatif. Dengan penambahan server, layanan yang sudah ada tetap berjalan ketika proses konfigurasi sedang dilakukan. Sehingga tidak akan sampai mematikan layanan..

Meskipun begitu penambahan server saja akan cukup merepotkan apabila tidak diatur dengan baik. Penambahan server tentu harus dilakukan dalam waktu yang cepat dan sebisa mungkin tidak diketahui oleh user. Dengan bertambahnya jumlah server, harus dipikirkan pula pengaturan saat salah satu server mati. Tidak mungkin seorang administrator harus mengaturnya secara manual. Untuk mengatasi hal-hal tersebut bisa digunakan Linux Virtual Server (LVS) [1]

Dengan LVS, beberapa buah server dapat memiliki 1 buah IP. Dan IP itulah yang nantinya akan diakses oleh klien. Ketika klien mengakses salah satu layanan yang ada, misalkan sebuah web, maka akan diatur agar klien itu mendapat layanan dari server yang mana. Apabila ternyata salah

satu server ada yang mati, maka layanan yang ada pada server tersebut dapat dipindah ke server yang lain secara otomatis

Efek lain dari berkembangnya penggunaan internet adalah munculnya gangguan-gangguan yang menyulitkan pengguna. Salah satu diantara gangguan tersebut adalah Denial of Services (DOS). DOS ini adalah sebuah serangan yang menyebabkan satu atau beberapa server tidak dapat melayani pengguna yang sesungguhnya atau dapat mengalami downtime [2]

LVS, sebagai salah satu bentuk kumpulan server, tentunya dapat juga terkena serangan DDOS. Untuk itu diperlukan sistem yang dapat mendeteksi serangan serta menjebak penyerang yang akan melakukan penyerangan dengan metode serangan yang disebutkan sebelumnya.

Untuk mendeteksi serangan digunakan Intrusion Detection System atau Snort IDS. Snort IDS adalah sebuah sistem untuk mendeteksi serangan atau intrusi pada suatu jaringan atau sistem komputer, dimana pendeteksian dilakukan dengan mencocokkan pola traffic jaringan dengan pola serangan yang telah diketahui Selain itu, berbagai rules khusus dapat dibuat untuk segala macam situasi. [3].

Untuk menjebak penyerang yang masuk digunakan Honeypot. honeypot, merupakan mekanisme baru dalam keamanan, membantu dalam memonitor dan mempelajari serangan. Honeypot adalah alat yang digunakan menjebak Attacker. Honeypot, dapat memikat pengguna jahat dengan cara bertindak sebagai sistem yang mengandung data yang

berharga atau layanan yang menarik. Honeypot memungkinkan untuk dieksploitasi oleh Attacker. Hal inilah yang kemudian dapat membantu pakar keamanan profesional dan peneliti dalam proses pembelajaran terhadap teknik dan metode yang dilakukan oleh para attacker. Honeypots tidak bisa mencegah serangan cyber terhadap jaringan sendiri, tetapi mereka dapat membantu dalam mengidentifikasi dan melakukan deteksi terhadap serangan ketika mereka digunakan bersama dengan perangkat pertahanan lainnya seperti firewall. Honeypot dapat menghasilkan sejumlah data yang memiliki nilai yang tinggi dan dapat juga menjadi tantangan bagi para pakar keamanan profesional.[4]

Tujuan dari penelitian ini adalah untuk mereduksi dampak yang ditimbulkan terhadap serangan DDoS pada Linux Virtual Server. Sehingga diharapkan administrator jaringan yang menggunakan Linux Virtual Server sebagai arsitektur server-nya dapat memberikan layanan yang lebih baik kepada para pengguna meskipun sedang diserang menggunakan DoS maupun DDoS.

1.2 Rumusan Masalah

Berdasarkan masalah yang telah diuraikan pada latar belakang, maka permasalahan pada penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana mengimplementasikan teknik pengalihan penyerangan menggunakan Honeypot dan deteksi serangan menggunakan Snort IDS?

2. Bagaimana performa serangan dan performa system keamanan yang di bangun?

1.3 Batasan Masalah

Batasan masalah yang digunakan dalam penelitian ini lebih mengarah dan tidak menyimpang dari permasalahan yang ada antara lain :

1. Jaringan yang di uji berupa Local Area Network (LAN)
2. Terdapat 6 user yang terdiri dari 3 server, 1 client, 1 penyerang, 1 sebagai firewall
3. Menggunakan system operasi linux ubuntu dan kali linux
4. Membuat serangan Ddos dengan serangan ke Linux Virtual Server
5. Melakukan simulasi pengujian kombinasi keamanan Honeypot sebagai pengalihan penyerangan dan Snort IDS sebagai pendeteksi juga analisis terhadap serangan terhadap Linux Virtual Server
6. Ddos tool yang digunakan adalah Hping3

1.4 Maksud dan Tujuan Penelitian

Maksud dan tujuan penelitian ini adalah

1. Menghasilkan sistem keamanan jaringan dengan menggunakan Honeypot dan Snort IDS yang berfungsi untuk mendeteksi dan menaglihankan serangan atau intrusi pada jaringan yang sengaja dibuat untuk menjadi umpan atau target para attacker dan penyusup yang dapat merugikan dan tidak bertanggung jawab, dengan menggunakan serangan Ddos.

2. Mengimplementasikan system scanning dan reduksi serangan terhadap Linux Virtual Server sehingga real server tetap berjalan normal dan tidak mengalami downtime

1.5 Manfaat Penelitian

1.5.1 Manfaat Bagi Mahasiswa

Menambah ilmu pengetahuan serta wawasan mengenai keamanan jaringan menggunakan honeypot dan Snort IDS dalam menghadapi serangan Distributed Denial of Service (Ddos)

1.5.2 Manfaat Bagi Akademik

Penelitian ini dapat menjadi refrensi untuk membantu para peneliti dan pengembang dalam membuat sistem keamanan jaringan di masa yang akan datang.

1.6 Metode Penelitian

1.6.1 Metode Pengumpulan Data

Adapun metode pengunpulan yang di gunakan penulis dapat dijelaskan sebagai berikut :

1.6.1.1 Metode Analisis

Data yang telah dikumpulkan dan didapatkan kemudian dipelajari dan dianalisa. Analisa ini berguna untuk proses implementasi ke objek dan serta menganalisa bagaimana cara kerja program terhadap objek.

1.6.2 Metode Perancangan

Metode ini berisi tentang pemaparan deskriptif tentang langkah langkah proses perancangan aplikasi. Proses identifikasi suatu objek dan

memberikan gamabaran umum tentang alur perancangan media pembelajaran

1.6.3 Metode Implementasi an Pengembangan Sistem

Metodologi ini bertujuan menggambarkan kegiatan yang akan dilaksanakan selama penelitian. Pada penelitian ini juga digunakan metode Security Policy Development Lifecycle untuk pengembangan sistem nya

1.6.4 Metode Testing

Melakukan proses pengujian untuk memastikan dan mengetahui semua system berfungsi dengan baik.

1.7 Sistematika Penulisan

Sistematika penulisan yang di buat agar saling berhubungan dengan antar bab lainnya dan merupakan satu kesatuan dari suatu laporan, sistematika penulisan, yaitu sebagai berikut :

BAB I : PENDAHULUAN

Bab ini berisikan tentang perkembangan teknologi, penjelasan tentang latar belakang masalah, indentifikasi masalah, tujuan dari penelitian, lalu metodologi dan sistematika

BAB II : LANDASAN TEORI

Bab ini berisi tentang berbagai landasan teori yang mendukung dari buku-buku teks ataupun makalah jurnal-jurnal ilmiah yang terkait dengan topik dalam pembuatan tugas akhir

BAB III : ANALISIS DAN PERANCANGAN

Bab ini mencakup analisis masalah, kebutuhan perangkat lunak yang digunakan. Selain itu dijelaskan beberapa perancangan yang akan diimplementasikan, perancangan tersebut meliputi rancangan sistem dan skenario pengujian

BAB IV : HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai hasil uji pengamatan terhadap perancangan yang telah dibuat dengan skenario yang berbeda-beda dan membandingkan dengan hasil uji pengamatan sebelum dilakukan perancangan

BAB V : PENUTUP

Bab ini berisi tentang kesimpulan dari hasil data yang telah di dapati dan memberikan saran terhadap pelaku objek penelitian agar mendapatkan kualitas yang diharapkan bisa lebih baik lagi