BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi virtualisasi pada komputasi sekarang menjadi topik yang cukup ramai dalam pembahasan riset teknologi cloud. Virtualisasi dan container merupakan bagian yang sangat penting dalam penerapan cloud computing, karena sangat berpengaruh pada efisiensi pengelolaan sumber daya infrastruktur cloud computing. Server web menjadi bagian penting dari infrastruktur internet saat ini. Sebagian besar server web yang digunakan saat ini masih banyak menggunakan arsitektur *single backend server*. Permasalahan yang dapat muncul adalah apakah mampu *single server* tersebut menangani permintaan data yang sangat banyak maka akan menimbulkan masalah sehingga website lama untuk diakses bahkan tidak bisa diakses. Itulah sebabnya, membangun infrastruktur server web yang andal dan sangat tersedia sangat penting. Untuk itu kita perlu mempertimbangkan menggunakan *clustering web server* untuk meningkatkan kehandalan server.

Namun dalam implementasinya saat ini, beberapa teknologi virtualisasi masih memerlukan penelitian maupun percobaan lebih lanjut karena beberapa teknologinya masih tergolong baru. Salah satu aspek penelitian yang banyak dikaji adalah mengenai jalannya aplikasi di atas teknologi virtualisasi serta aspek keamanan jaringan. Di antara banyak jenis serangan jaringan, yang paling sering digunakan adalah serangan Denial of Service (DoS). DoS adalah jenis serangan terhadap sebuah komputer atau server didalam jaringan internet dengan cara

menghabiskan sumber (resource) yang dimiliki komputer tersebut sampai komputer tersebut tidak dapat menjalakan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut,

Pada analisis performansi antara virtual machine dan container pada penelitian yang telah dilakukan oleh Chrisna Fiddin, Ir. Dr. Rendy Munad, M.T. Ratna Mayasari, S.T, M.T. dalam paper yang berjudul “Analisis Performansi Virtualisasi Container Menggunakan Docker Dibawah Serangan Denial of Service”. mendapatkan kesimpulan bahwa performansi virtualisasi container menggunakan Docker sedikit lebih unggul jika dibandingkan dengan teknik virtualisasi lainnya.

Berdasarkan latar belakang yang sudah dijabarkan dari penelitian sebelumnya maka akan dilakukan penelitian pada performansi Docker Swarm, dengan tujuan untuk menganalisa dan mengetahui dampak yang ditimbulkan oleh serangan Denial of Service (DoS) SYN attack terhadap layanan web yang dijalankan menggunakan virtualisasi Docker Swarm.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah bagaimana melakukan pengujian Denial of Service pada docker swarm.

1.3 Ruang Lingkup

Berdasarkan rumusan masalah di atas, peneliti dapat menyimpulkan untuk ruang lingkup aplikasi yang akan dibuat sebagai berikut :

1. Implementasi virtualisasi Docker Swarm
2. Computer cluster terdiri dari 1 (satu) node manager sebagai controller pada computer cluster dan 2 (dua) node worker sebagai node yang mengeksekusi proses yang telah dibagi oleh node manager.
3. Sistem operasi yang digunakan pada setiap node adalah Ubuntu Server.
4. Website dan Database yang digunakan hanya sebagai implementasi sehingga tidak termasuk dalam pembahasan.
5. Tools yang digunakan dalam pengujian adalah slowloris

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah menghasilkan informasi dari analisis dampak serangan Denial of Service pada Virtualisasi Docker Swarm.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan bermanfaat untuk:

1. Peneliti

   Menambah wawasan ilmu pengetahuan, serta pemahaman mengenai virtualisasi docker swarm dan jenis serangan Dos sehingga nantinya berguna di dunia kerja.

2. STMIK Akakom Yogyakarta

Sebagai arsip dan referensi bagi mahasiswa selanjutnya dalam menyusun tugas kuliah, materi perkuliahan, tugas akhir dan skripsi mengenai performansi docker swarm pada serangan dos.