BAB 1
PENDAHULUAN

1.1 Latar Belakang

Bidang *Information Technology* (IT) mengalami perkembangan yang signifikan dari waktu ke waktu terutama dalam teknologi kontainerisasi [1]. Kontainer sendiri mempunyai konsep yaitu untuk sebuah sistem memungkinkan untuk membuat layanan dan sumber daya yang berbeda. Kontainer bekerja dengan cara berbagi perangkat keras di dalam sebuah sistem operasi dan berjalan di atas *libraries*, *drivers* dan *binaries* yang berbeda. Berdasarkan konsep ini, dapat mengurangi jumlah sumber daya yang terbuang selama komputasi dikarenakan kontainer hanya menjalankan dan menyediakan kebutuhan *library* yang sesuai dengan aplikasi atau layanan yang dijalankan saja [2].

Kubernetes merupakan sebuah *platform* kontainer yang digunakan untuk melakukan manajemen aplikasi yang di kontainerisasi kan. Kubernetes juga merupakan *platform open-source* yang digunakan untuk melakukan *workloads* aplikasi, serta menyediakan konfigurasi dan otomatisasi secara deklaratif. Kubernetes berada di dalam ekosistem yang besar dan berkembang dengan cepat. Kubernetes sendiri mempunyai kelebihan seperti mekanisme pembuatan aplikasi serta proses *deployment* yang lebih efektif dalam pengalokasian dan penggunaannya jika dibandingkan *virtual machine* [3].

Pada implementasi beberapa teknologi kontainerisasi, masih memerlukan penelitian maupun percobaan lebih lanjut karena beberapa teknologinya masih tergolong baru. Salah satu aspek penelitian yang banyak dikaji adalah mengenai performansi aplikasi di atas teknologi kontainerisasi serta aspek keamanan jaringan. Salah satu contohnya yaitu menggunakan *platform Docker* dengan *software* Ubuntu Server 14.0. Di antara berbagai aspek keamanan jaringan terhadap serangan *server* berbasis kontainer, serangan *Denial of Service* (DoS) adalah yang paling umum dan dikenal sebagai salah satu metode yang paling kuat, salah satu jenisnya yaitu SYN *flooding* dan dengan parameter perhitungan *responsive server* diantaranya CPU, RAM, *IOzone write*, dan *IOzone read* [4]. Untuk uji cobanya yaitu dengan membuat suatu cluster yang terdiri dari tiga nodes dengan container yang saling terhubung,

dimana untuk aplikasi container menggunakan Ngnix [5]. Untuk hasil dari penyerangan akan dihitung dengan *real time*, melalui pengecekan secara berkala menggunakan *tools Apache Benchmarking* sebagai *software* perhitungannya [6]. DoS dapat diartikan sebagai serangan *cyber* yang menargetkan *website*, layanan online, maupun jaringan dengan cara membanjiri laman tersebut dengan *fake traffic* yang sangat banyak [7]. Sehingga menyebabkan *website* tidak bisa mengakomodasi *traffic* yang masuk dan menyebabkan lumpuhnya suatu *server*. Jenis serangan DoS ada tiga, diantaranya UDP *Flood*, TCP *Flood* dan *Smurf Attack* [8].

Berdasarkan latar belakang yang sudah dijabarkan, penelitian ini akan menguji performansi kontainer *berplatform* Kubernetes terhadap serangan *Denial of Service* (DoS). Tujuan penelitian ini untuk menganalisa dan mengetahui dampak yang ditimbulkan oleh serangan DoS. Pengujian yang dilakukan yaitu dengan membandingkan *web server* yang di *install* pada kontainer *berplatform* Kubernetes yang mendapatkan serangan DoS dan *web server* yang di *install* pada kontainer *berplatform* Kubernetes yang tidak mendapatkan serangan DoS. Pengujian ini menggunakan tiga skenario penyerangan DoS yaitu TCP *flood*, UDP *flood*, dan *smurf attack*. Parameter yang akan dianalisis yaitu *response time*, *throughput*, CPU *usage*, dan *memory* dengan menggunakan metode *benchmark*.

1.2 Rumusan Masalah

Rumusan masalah dari penelitian yang dilaksanakan yaitu:

1) Bagaimana performansi dari server kontainer *berplatform* Kubernetes terhadap serangan *Denial of Service* (DoS)?
2) Bagaimana perbandingan performansi server kontainer *berplatform* kubernetes yang mengalami penyerangan DoS dan *server* kontainer *berplatform* Kubernetes yang tidak mengalami penyerangan DoS?

1.3 Batasan Masalah

Batasan masalah dari penelitian yang dilaksanakan yaitu:

1) Penelitian ini membahas mengenai performansi *server* kontainer *berplatform* Kubernetes terhadap serangan DoS diantaranya TCP *flood*, UDP *flood*, dan *smurf attack*.

2) Skenario pengujian dilakukan dari sisi *server* dan juga *client*.
3) Parameter yang diuji yaitu *response time*, *throughput*, CPU *usage*, dan *memory*.
4) Pengujian parameter menggunakan metode *benchmark*.

1.4 Tujuan Penelitian

Tujuan dari penelitian yang dilaksanakan yaitu:

1) Mampu menganalisis performansi *server* kontainer *berplatform* Kubernetes terhadap Serangan *Denial of Service*.
2) Mampu menganalisis perbandingan performansi *server container berplatform* Kubernetes yang mengalami penyerangan DoS dan *server container berplatform* Kubernetes yang tidak mengalami penyerangan DoS.

1.5 Manfaat Penelitian

Manfaat dari penelitian yang dilaksanakan yaitu:

1) Memberikan informasi mengenai kelebihan dari *container berplatform* Kubernetes.
2) Memberikan informasi mengenai pengoperasian dan simulasi *server container berplatform* Kubernetes melalui *software web server*.
3) Mampu melakukan simulasi *server* yang mengalami serangan *Denial of Service* (DoS).
4) Mampu melakukan analisa perhitungan menggunakan *software benchmark*.

1.6 Sistematika Penulisan

Penelitian ini terbagi menjadi beberapa bab. Bab 1 berisi tentang latar belakang, rumusan masalah, manfaat dan tujuan penelitian, batasan masalah dan sistematika penulisan. Bab 2 berisi mengenai kajian pustaka serta dasar teori yang menjadi refrensi penulis untuk menyusun penelitian ini. Cara penelitian seperti alat yang digunakan, topologi yang digunakan, spesifikasi perangkat yang digunakan, diagram alur penelitian akan dibahas pada Bab 3. Bab 4 membahas tentang hasil

simulasi dan analisis sistem berdasarkan hasil dari percobaan. Kesimpulan dan saran pengembangan untuk kedepannya dideskripsikan pada Bab 5.