BAB 5
PENUTUP

5.1 KESIMPULAN

Beberapa hal yang dapat disimpulkan dari penelitian ini berdasarkan pengujian yang dilakukan antara lain :

1. Performansi *server* pada *container berplatform* Kubernetes terhadap serangan DoS yaitu masih memiliki kinerja yang cukup baik. Hasil yang didapatkan yaitu serangan UDP *flood* mendapatkan hasil pada parameter *response time* sebesar 0,06 s, *throughput* sebesar 5,794 MBps, dan CPU *usage* sebesar 72,13 %. Setelah serangan UDP *flood*, serangan *smurf attack* memiliki hasil pada parameter *response time* 0,06 s dan *throughput* 4,342 MBps. Hasil serangan TCP *flood* dibawah UDP *flood* dan *smurf attack* dengan *response time* 0,05 s, *throughput* 0,08 MBps, CPU *usage* 99,64 % dan *memory* 869,1 MB.
2. Performansi *server* pada *container berplatform* Kubernetes ketika tidak mengalami serangan DoS memiliki hasil yang lebih baik dibanding dengan *server* ketika diserang DoS. Namun saat *server* diserang DoS UDP *flood* dan *smurft attack* juga memiliki hasil yang tidak terlalu jauh nilainya dengan hasil saat *server* yang tidak diserang DoS, dengan penurunan performansi UDP *flood* sebesar 22,22% dan *smurft attack* sebesar 30,78%. Berbeda dengan TCP *flood* yang memiliki perbedaan cukup signifikan, dengan penurunan performansi sebesar 86,72% dibandingkan dengan *server* yang tidak mengalami penyerangan DoS.

5.2 SARAN

Beberapa hal yang dapat menjadi saran untuk penelitian selanjutnya antara lain :

1. Penelitian selanjutnya dapat menggunakan metode penyerangan yang berbeda seperti SQL *Injection*, *Cross-Site Scripting* (XSS), *Spoofing*, dan lainnya.
2. Penelitian lain dapat menggunakan *cluster* Kubernetes *container* yang lebih kompleks.
3. Penelitian lebih lanjut dapat menggunakan infrastruktur yang berbeda seperti *Amazon Web Sevices*, *Microsoft Azure*, *Docker*, atau lainnya.