Pemodelan Sistem Keamanan Snort Intrusion Detection System (IDS) pada Jaringan yang Berbasis Software Defined Network (SDN)

Yosef Asido Manalu[1)], Linna Oktaviana Sari[2)]
[1)]Mahasiswa Program Studi Teknik Elektro, [2)]Dosen Teknik Lingkungan
Laboratorium Telekomunikasi
Program Studi Teknik Elektro S1, Fakultas Teknik Universitas Riau
Kampus Bina Widya Jl. HR Soebrantas Km 12,5 Simpang Baru
Panam, Pekanbaru 28293
Jurusan Teknik Elektro Universitas Riau
Email: yosef.asido@student.unri.ac.id

ABSTRACT

Software Defined Network (SDN) is a centralized network where control plane and data plane embedded in different systems. However, controller is an indivual threat to the security of data packet that passes OpenFlow Network. Security on a computer network is the top priority in designing a network. This research is performed by designing a tree network topology in SDN from and simulated on the mininet software. Then, snort activation is done on protected Host with snort detection system. Attack test is done on Host 8 as an Attacker and Host 1 becomes the Target of attack using hping3 application. Test results of Ddos attack by Host 8 uses IP Address 192.168.10.14 and Host 1 uses IP Address 192.168.10.7. Attack priority level is done on Level 1 (high attack category). After detection by snort, notification is displayed on BASE with intrusion that processed by IDS with UDP messages

Keywords : SDN, Ddos, Security Network, Snort

1. PENDAHULUAN

Seiring perkembangan teknologi jaringan juga disertai munculnya berbagai permasalahan keamanan. Teknologi SDN mempunyai beberapa metode yang digunakan untuk mengontrol data antar komunikasi pada jaringan. Salah satu teknologi SDN yang sedang berkembang saat ini adalah *protocol OpenFlow*.

Protocol OpenFlow merupakan sebuah arsitektur jaringan komputer pada perangkat *switch*, yang berfungsi untuk melakukan komunikasi data, dimana diantara perangkat *data plane* dengan *control plane* saling dipisahkan. *Controller* menjadi *device* pertama yang mengetahui apabila terjadi hal-hal yang tidak sesuai dengan harapan awal dibuatnya jaringan SDN tersebut. Beberapa isu ancaman yang sering terjadi pada jaringan *OpenFlow* diantaranya adalah dos (*deniel of services*) *attacks*, Ddos (*Distributed-deniel of services*) *ping flood*, *packet sniffing* serta ancaman-ancaman lainnya.

Penelitian mengenai Analisis performa *Centralized Firewall* pada *Multi Domain Controller* di Arsitektur *Software-Defined Networking* (SDN) oleh Rifki Pinto Hidayat tahun 2017. Pada penelitian ini, Rifki Pinto Hidayat menggunakan *software Mininet* dengan pengujian untuk mengetahui kinerja dari *system centralized firewall* di jaringan SDN.

Penelitian yang dilakukan Guntoro pada tahun 2015 mengenai Keamanan Jaringan *OpenFlow* menggunakan *Intrusion Detection System* (IDS) berbasis *Backpropagation Neural Network*. Penelitian ini menerapkan IDS berbasis *backpropagation neural network* kedalam jaringan *OpenFlow* yang berfungsi untuk mengenali pola-pola

serangan serta mengklasifikasikan jenis paket data yang ada pada jaringan *OpenFlow*, baik dalam kategori serangan maupun bukan serangan.

Berdasarkan latar belakang dan penelitian yang sudah ada, maka penelitian ini bertujuan untuk Perancangan Sistem Keamanan *Snort* IDS pada Jaringan Universitas Riau yang berbasis *Software-Defined Network* yang disimulasikan dengan *software MiniNet* dengan membahas tentang penerapan IDS menggunakan *Snort* kedalam jaringan *OpenFlow*.

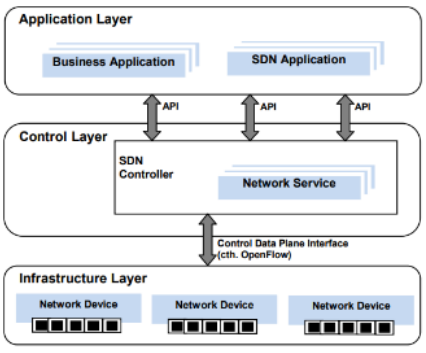
2. LANDASAN TEORI

2.1. Pengenalan SDN

Software Defined Network (SDN) adalah istilah yang merujuk pada konsep/paradigma baru dalam mendesain, mengelola dan mengimplementasikan jaringan, terutama untuk mendukung kebutuhan dan inovasi di bidang ini yang semakin lama semakin kompleks. Konsep dasar SDN adalah dengan melakukan pemisahan eksplisit antara *control* dan *forwarding plane*, serta kemudian melakukan abstraksi sistem dan meng-isolasi kompleksitas yang ada pada komponen atau sub-sistem dengan mendefinisikan antar-muka (*interface*) yang standar.

Arsitektur SDN dapat dilihat sebagai 3 lapis/bidang:

1. Infrastruktur (*data-plane / infrastructure layer*).
2. Kontrol (*control plane / layer*).
3. Aplikasi (*application plane / layer*).



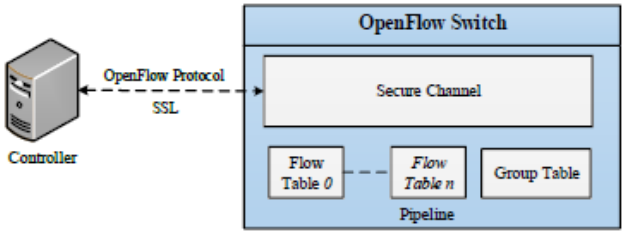
Gambar 1. Arsitektur jaringan SDN

2.2. Perbandingan Jaringan Tradisional dengan Jaringan SDN

Konsep *software-defined networking* adalah melakukan pemisahan antara *control plane* dengan *data plane*, dimana pada bagian *data plane* berada pada perangkat jaringan, sedangkan *control plane* terpisah dari perangkat jaringan yang disebut *controller*. Sedangkan konsep didalam jaringan tradisional, yaitu *control plane* dengan *data plane* berada pada perangkat jaringan yang sama dan tidak saling dipisahkan.

2.3. Jaringan OpenFlow

Sebuah *controller* menentukan setiap paket data yang ada di dalam jaringan, kemana paket data harus dikirimkan. Setiap paket data yang melewati jaringan *OpenFlow* harus diverifikasi oleh *controller* pada gambar 2.



Gambar 2. Arsitektur protokol *OpenFlow*

OpenFlow protocol berfungsi untuk menyediakan layanan yang terbuka untuk komunikasi antara *controller* dengan *OpenFlow switch*.

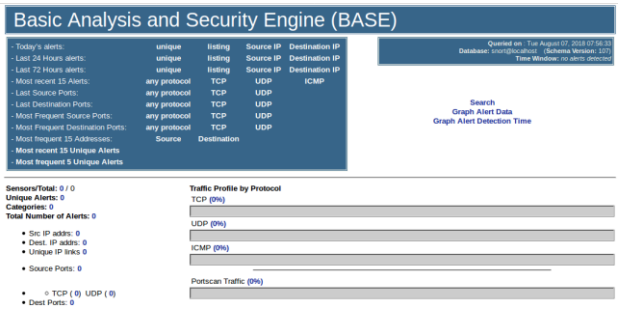
2.4. Intrusion Detection System

Intrusion detection system (IDS) merupakan suatu sistem yang akan menghambat semua serangan yang mengganggu sebuah jaringan. Selain memberikan peringatan, IDS juga mampu melacak jenis aktivitas yang merugikan sebuah sistem. IDS akan melakukan pemantauan terhadap paket-paket yang melewati jaringan dan berusaha menemukan jika terjadi paket-paket yang berisi aktivitas yang menyimpang dan selanjutnya melakukan proses pencegahan.

2.5. Snort

Snort adalah sebuah metode untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan pemindaian, dan berbagai bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Ada tiga tingkat prioritas secara *default*: *low* (3), *medium* (2), dan *high* (1).

Tampilan notifikasi snort dapat berupa tampilan di terminal snort atau berupa bentuk lain, salah satunya berupa tampilan *web*. BASE merupakan perangkat notifikasi snort berbasis *web*. BASE terhubung ke *database* untuk telah dihubungkan pada snort *log*. Setelah dilakukan konfigurasi BASE (*Basic Analysis and Security Engine*), maka masuk ke halaman tampilan antarmuka BASE untuk mendapatkan notifikasi dengan terjadinya serangan seperti pada gambar 3.



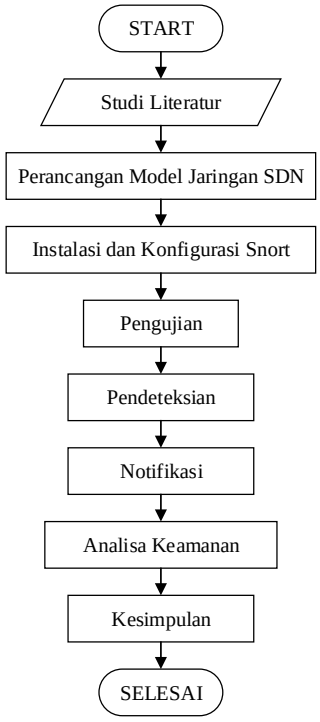
Gambar 3. Tampilan Antarmuka BASE

3. METODOLOGI PENELITIAN

3.1. Flowchart Penelitian

Berikutnya adalah memulai perencanaan simulasi sistem keamanan snort model jaringan SDN di *software* mininet. Hal-hal yang perlu di rencanakan adalah jenis *routing protocol*, pendistribusian IP, dan jenis *switch* dan *controller* yang digunakan pada perangkat jaringan serta bentuk topologi jaringan yang akan di modelkan dalam *software* simulasi. Setelah itu hasil perancangan akan di uji coba dan di analisa apakah hasilnya sudah sesuai dengan yang diinginkan. Diagram alir penelitian pemodelan sistem keamanan snort IDS pada jaringan yang berbasis SDN dapat dilihat pada gambar 4.

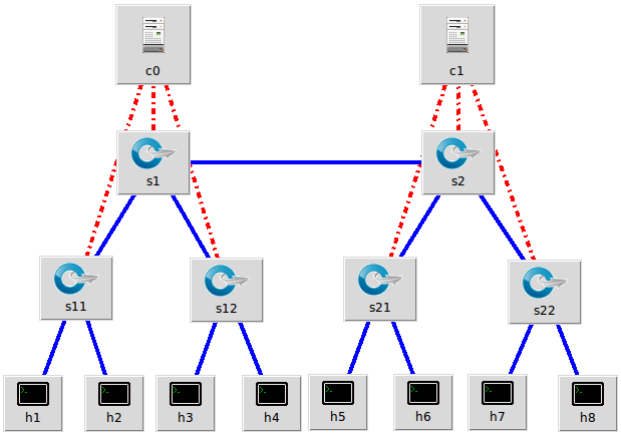
.



Gambar 4. Diagram Alir Penelitian

3.2. Perencanaan Model Jaringan

Perencanaan model jaringan pada penelitian ini yaitu pemodelan jaringan berbasis SDN dengan sistem keamanan IDS. Jaringan yang digunakan yaitu model topologi jaringan *tree*. Pada topologi jaringan terhubung masing-masing 4 *switch* dan setiap *switch* terhubung pada *OpenFlow Controller*. Pada *Host* telah diinstalasi IDS snort yang dapat mendeteksi adanya penyusup dari dalam jaringan.



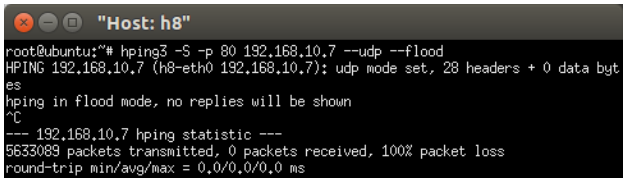
Gambar 5. Desain Topologi *Tree* di *software mininet*

Pada gambar 5 terdapat desain topologi tree pada *software* mininet yang terdiri dari 2 buah *OpenFlow Switch* dan terdapat 2 *switch* yang terhubung pada *controller*. Untuk memeriksa *link* yang terhubung pada jaringan dapat menggunakan perintah *pingall* pada CLI *controller*.

4. HASIL DAN PEMBAHASAN

4.1. Pengujian Serangan

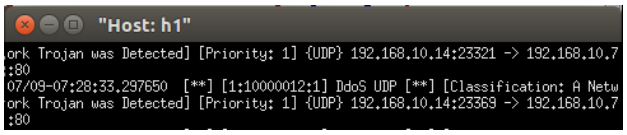
Pada desain topologi jaringan *tree* dilakukan pengujian serangan Ddos. Terdapat *Host* 1 yang akan menjadi target serangan dengan penyerangan pada *Host* yang berbeda. Untuk pengujian serangan pada jenis serangan sebagai berikut.



Gambar 6. Serangan Ddos pada topologi *Tree*

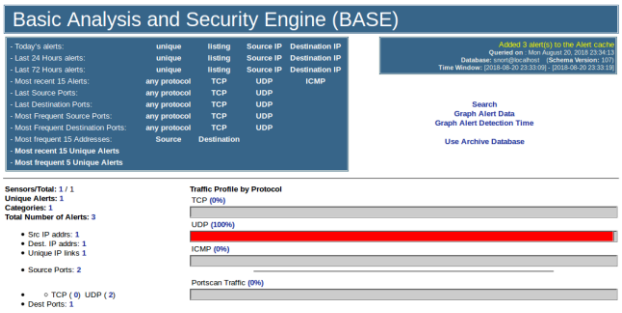
Pada gambar 6 dilakukan pada aplikasi hping3 pada *Host* 8 dan untuk target yang diserang yaitu *Host* 1. Pada pengujian menggunakan aplikasi hping3 seperti pada gambar 6.

Hasil pengujian serangan Ddos oleh *Host* 8 sebagai *attacker* dengan IP *Address* 192.168.10.14 terdapat *host* 1 sebagai target serangan dengan IP *Address* 192.168.10.7. Pada deteksi snort dapat dilihat pada gambar 7.



Gambar 7. Snort mendeteksi serangan Ddos pada topologi *Tree*

Berdasarkan gambar 7 serangan Ddos terdapat target serangan yaitu *Host* 1 dengan IP *Address* 192.168.10.7 dimana snort mendeteksi adanya serangan pada prioritas 1 pada kategori *high*. Setelah terdeteksi pada snort, lalu dikirimkan pada BASE (*Basic Analysis and Security Engine*) dengan intrusi yang diproses oleh IDS yang dapat dilihat pada gambar 8. Notifikasi yang dikirimkan dengan pesan UDP dimana serangan yang terdeteksi merupakan jenis serangan Ddos.



Gambar 8. Notifikasi BASE mendeteksi serangan Ddos pada topologi *Tree*

5. KESIMPULAN

Hasil simulasi sistem keamanan pada deteksi snort IDS dimana adanya aktivitas serangan Ddos pada desain topologi jaringan *tree* yang terdeteksi pada *Host* 1 dimana serangan terdeteksi dilakukan oleh IP *Address* 192.168.10.14, dengan prioritas 1 (*high*). Selanjutnya untuk notifikasi BASE terdapat pesan UDP.

6. SARAN

Penelitian lebih lanjut untuk melakukan pembuatan akun palsu berupa IPS (*Intrusion Prevention System*) atau memblokir alamat yang menyusup pada lalu lintas jaringan.

DAFTAR PUSTAKA

Baker, Andrew R., Esler, Joel. 2007. *Snort IDS and IPS Toolkit*. Syndress.

Guntoro. 2015. Keamanan Jaringan *OpenFlow* menggunakan *Intrusion Detection System* (IDS) berbasis *Backpropagation Neural Network*. Magister Komputer, Program Studi Ilmu Komputer, Institut Pertanian Bogor.

Hidayat, Rifki Pinto., Primananda, Rakhmadhnay., Widasari, Edita Rosana. 2017. Analisis Performa *Centralized Firewall* pada *Multi Domain Controller* di Arsitektur *Software-Defined Networking* (SDN). Program Studi Teknik Informatika,

Fakultas Ilmu Komputer, Universitas Brawijaya.

Kloti, Rowan., Kotronis, Vasileios., Smith, Paul. 2013. *OpenFlow*: *A Security Analysis*. IEEE *International Conference on Network Protocol* (ICNP). 1-6.doi.10.1109/ICNP.2013.6733671 ETH Zurich, Switzerland.

Mulyana, Eueung., 2015. Buku Komunitas SDN – RG. *Published with GitBook*.