Monitoring DDOS Pada Openflow Switch Dengan Alienvault Ossim

Alimuddin Yasin[1]

Program Studi D3 Teknik Informatika, Politeknik Gorontalo.Jln, Muchlis Rahim, Botu Pingge, Bone Bolango, Gorontalo, e-mail: alimuddiny@poligon.ac.id

Ismail Mohidin[2]

Program Studi D3 Teknik Informatika, Politeknik Gorontalo, Jln, Muchlis Rahim, Botu Pingge, Bone Bolango, Gorontalo, e-mail: is.mohidin@poligon.ac.id

Abstrak - DDoS menjadi satu masalah utama dalam keamanan internet dalam dekade terakhir. Intrusion Detection System adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. OSSIM adalah gabungan dari IDS (Intrusion Detection System), vulnerability assessment, anomaly detection, network and availability detection, firewall, dll, yang dikemas dalam bentuk distro linux . Sehingga dalam penelitian ini melakukan uji coba serangan DDoS sekaligus melakukan monitoring DDoS di jaringan SDN dengan Alienvault Ossim.

Kata kunci: DDoS, Alienvault Ossim, Softwaare Defined Network

I. PENDAHULUAN

Seiring dengan berkembangnya teknologi, perangkat elektronik sebagian besar saling terhubunng satu sama lain menggunakan jaringan yang sama dengan perangkat komputer sehingga mengakibatkan kondisi jaringan komputer menjadi kompleks. Akan tetapi perkembangan perangkat jaringan begitu lambat sehinga sulit untuk memenuhi kebutuhab jaringan pada era digital saat ini. Hal ini disebabkan ketergantungan terhadap vendor dengan adanya aturan atau protokol masing masing vendor, sehinga untuk mengkomunikasikan perangkat jaringan yang berbeda vendor butuh upaya tinggi dalam melakukan konfigurasi serta dapat membuat ketergantungan terhadap salah satu vendor. Dengan keterbatasan tersebut diciptakan arsitektur jaringan baru yang dikenal dengan Software Defined Network yang memanfaatkan protokol Openflow [5].

Dalam Arsitektur jaringan SDN ini Data Plane dan Controll Plane terpisah. Dinaba dataplane berada pada sisi perangkat switch Openlow sedangkan Control Plane di pasang pada Komputer Kontrol yang berfungsi mengatur semua alur data pada switch yang memanfaatkan open protokol openflow. Hal ini sangat berbeda dengan arsitektur jaringan biasa dimana control plane dan data plane berada dalam perangkat jaringan computer [4].

Arsitektur jaringan SDN dan Protokol saat ini masih dalam tahap pengembahan sehingga isu keamanan masih terbuka lebar untuk diteliti. Salah satunya adalah serangan DDOS. *DDoS* menjadi satu masalah utama dalam keamanan internet dalam dekade terakhir. Berdasarkan laporan data statistik tentang *DDoS* yang dipublikasikan oleh *Akamai Technologi* dalam *State Of The Internet [Security]* Q1 2015 bahwa infrastruktur layer mengalami serangan *DDoS* dengan presentase 90.68% dan pada aplikasi *layer* hanya mengalami serangan *DDoS* dengan presentase 9.32%. Berdasarkan hasil data statistik tersebut dapat disimpulkan bahwa infrastruktur *layer* lebih rentan terhadap serangan *DDoS* dibandingkan dengan aplikasi *layer* [1].

NetFlow adalah sebuah protokol untuk mengekspor metrics untuk IP traffic flows. Dalam penggunaan NetFlow, dibutuhkan suatu NetFlow collector yang biasanya sebagai digunakan server untuk mengumpulkan NetFlow records yang dikirimkan dari router atau switch (NetFlow exporter). NetFlow records inilah yang nantinya akan dibaca oleh suatu NetFlow analyzer untuk dianalisis [3].

Intrusion Detection System adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

OSSIM adalah singkatan dari *Open Source SIEM*, sedangkan Kata *SIEM* sendiri adalah singkatan *Security Information and Event Management*. *OSSIM* menggabungkan berbagai tool security ke dalam sebuah paket, baik tool yang bersifat aktif maupun pasif. *OSSIM* adalah gabungan dari *IDS (Intrusion Detection System), vulnerability assessment, anomaly detection, network and availability detection, firewall*, dll, yang dikemas dalam bentuk *distro linux* . OSSIM ini juga merupakan sebuah produk *Open Source* dari Alienvault yang berfungsi untuk memonitor sebuah jaringan. OSSIM terdiri dari 4 bagian yaitu Server, Sensor, Database dan Framework yang dimana semuanya sudah mempunyai fungsi tersendiri, dan menyatu [2].

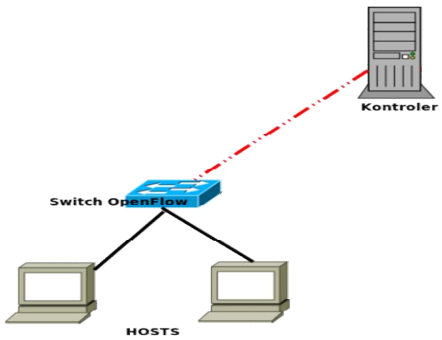
Penelitian ini mngangkat tentang monitoring Serangan DOS Di Jaringan SDN dengan netflow monitoring di Alienvault Ossim.

II. METODE PENELITIAN

Langkah langkah yang digunakan dalam penelitian ini: (1) Perancangan Topologi, (2) Skenario Serangan DDoS (3) Instalasi dan Konfigurasi Alienvault Ossim, (4) Konfigurasi Netflow Monitoring pada Alienvault Ossim, (5) Konfigurasi Netflow pada Switch Openflow , (6) Simulasi serangan DDoS, (7) Pengamatan Trafik jaringan dengan Netflow Monnitoring.

2.1. Perancangan Topologi

Topologi yang digunakan dalam penelitian ini adalah topologi star yang menghubungkan Huawei HG553 sebagai Software based Switch Openflow dengan controller dan 2 buah host computer seperti gambar berikut



Gambar 1. Topologi yang Digunakan dalam Penelitian

Keterangan Topologi yang digunakan pada Gambar 1 sebagai berikut:

Kontroller : Sebagai server yang mengontrol Switch Openflow
Switch Openflow : Menunjukan Posisi Perangkat HG553 sebagai Software Based Switch Openflow
Host : Host yang terhubung pada Switch Openflow
_____ : Link yang menghubungkan Kontroller dengan Switch Openflow
---------- : Link yang menghubungkan Host dengan Switch Openflow

2.2. Modifikaasi Firmware Huwaei HG553

Jenis serangan DDoS yang digunakan dalam penelitian ini UDP Flooding attack. Yakni jaringan SDN yang berjalan dengan perangkat HG553 akan dibanjiri paket UDP. Saat terjadi serangan di jaringan SDN, dan akan diamati lalulintas data dari jaringan SDN pada netflow yang berada pada Alienvault Ossim

2.3. Instalasi dan Konfigurasi Alienvault Ossim

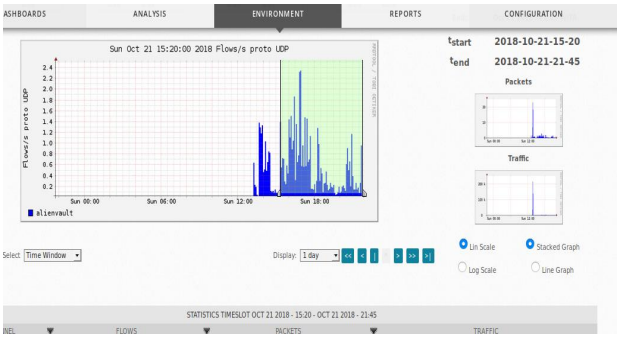
Instalasi Alienvault OSSIM sama dengan melakukan instalasi sistem operasi turunan debian pada umumnya. Yakni meliputi setting wilayah, bahasa, serta konfigurasi jaringan. Dan konfigurasi yang diperlukan meliputi konfigurasi sensor, konfigurasi netflow, serta konfiugrasi Asset.

2.4. Skenario Serangan DDoS

Langkah-langkah konfigurasi netflow OSSIM meliputi konfigurasi sensor netflo serta konfigurasi

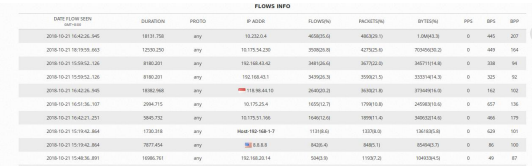
III. HASIL DAN PEMBAHASAN

Serangan DDoS yang terjadi di jaringan SDN Menyebabkan komunikasi antara switch Openflow dan Kontroller terputus. Sehingga menyebabkan terganggunya komunikasi antar perangkat yang berada di jaringan SDN.



Gambar 2. Peningkatan Trafict pada Netflow Monitoring Saat terjadi Serangan DoS

Hasil pengamatan lalulintas data pada Netfow di Alienvault Ossim saat terjadi serangan DOS terlihat ada peningkatan lalulintas data seperti yang berada pada gambar 2. Pada saat serangan berlangsung, pada sisi netflow di alienvault ossim dapat langsung menangkap peningkatan data yang digambarkan dengan diagram.



Gambar 3. Detail serangan DDoS di Jaringan SDN

Hasil dari monitoring Netflow dapat dilihat detail dari paket paket yang berada dalam jaringan seperti yang terdapat pada gambar 3. Pada gambar 3 terlihat bahwa asal paket-paket UDP yang membanjiri seolah olah berasal dari banyak host padahal paket tersebut hanya berasal dari 1 host saja. Hal ini dikarenakan pada saat melakukan simulasi serangan DDoS, karena pada saat itu perintah yang dipakai dalam menjalankan serangan DoS adalah serangan yang berasal dari banyak komputer juga.

IV. KESIMPULAN

Dari hasil penelitian dapat disimpulkan bahwa Alienvault OSSIM dapat dijadikan sebagai tool monitoring network SDN yang memanfaatkan protokol netflow. Saat terjadi serangan DoS, secara realtime serangan DoS tersebut dapat diamati secara realtime

PUSTAKA

[1] Akamai, diakses tanggal 4 Januari 2016, Q1 2015 State of the Internet – Security Report. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/ 2015-q1-internet-security-report.pdf

[2] alienvault. (n.d.). AlienVault Unified Security

Management & Threat Intelligence. Diambil 24 Oktober 2018, dari https://www.alienvault.com/#

[3] Cisco Meraki, diakses tanggal 20 mei 2016, NetFlow Overview, https://documentation.meraki.com/MX-Z/monitoring_and_reporting/netflow_ overview

[4] Fattah, F., & Hasnawi, M. (2018). Simulasi Jaringan Virtual Berbasis SDN Pada Topologi Tree, 8–9.

[5] O.N.F. (2012). Software-defined networking: The new norm for networks. *ONF White Paper*, *2*, 2–6. Diambil dari https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf