EasyChair Preprint

№ 2912

Implementation of Intrusion Prevention System (IPS) as a Security from DDoS (Distributed Denial of Service) Attacks

Istiana Adesty, Wahyu Adi Prabowo and Muhammad Fajar Sidiq

March 9, 2020

Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service (DDoS)

Istiana Adesty[1], Wahyu Adi Prabowo[2], Muhammad Fajar Sidiq[3]
[1,2,3]Teknik Informatika, Fakultas Informatika, Insitut Tekbologi Telkom Purwokerto
[1,2,3]Jl. D. I. Pandjaitan No.128 Purwokerto Selatan, Jawa Tengah Indonesia 53147

[1]16102125@ittelkom-pwt.ac.id
[2]wahyuadiprabowo@ittelkom-pwt.ac.id,
[3]muhammadfajarsidiq@ittelkom-pwt.ac.id

Abstrak – Pengamanan pada sebuah server dalam suatu jaringan diperlukan untuk menghindari hal-hal yang tidak dinginkan seperti adanya serangan yang dilakukan oleh oknum-oknum yang tidak bertanggung jawab. IPS (*Intrusion Prevention System*) merupakan salah satu metode atau tools yang digunakan sebagai suatu sistem pengamanan pada sebuah server. IPS mampu memberikan pengamanan dari suatu serangan dengan memanfaatkan fitur dari IDS (*Intrusion Detection System)* dan *firewall* sebagai fitur untuk memblokir akses pada lalu lintas jaringan. Serangan *Distributed Denial of Service* (DDoS) merupakan salah satu serangan yang digunakan dengan tujuan untuk membuat server menjadi *down*. Dalam penelitian ini dilakukan penerapan IPS Suricata yang mampu memberikan pengaman dari serangan DDoS. Dan dari hasil penelitian ini bahwa IPS Suricata mampu mendeteksi serangan DDoS dan mampu memblokir akses serangan tersebut dengan memanfaatkan fitur *firewall* yaitu *IPTables*.

Kata kunci – *DDoS, Firewall, IDS, IPS, IPTables, Suricata*

Abstract— *Security on a server in a network is needed to avoid things that are not cold, such as an attack carried out by unscrupulous elements. IPS (Intrusion Prevention System) is one of the methods or tools used as a security system on a server. IPS is able to provide security from an attack by utilizing the features of the IDS (Intrusion Detection System) and firewall as a feature to block access to network traffic. Distributed Denial of Service (DDoS) attack is one of the attacks used in order to make the server go down. In this research, the application of IPS Suricata is able to provide security from DDoS attacks. And from the results of this study that IPS Suricata is able to detect DDoS attacks and is able to block access to these attacks by utilizing the firewall feature, namely IPTables.*

Keywords – *DDoS, Firewall, IDS, IPS, IPTables, Suricata*

I. PENDAHULUAN

Pada Maret 2019 Kasus cybercrime di Indonesia semakin berkembang pesat sejalan dengan adanya perkembangan internet dan teknologi yang ada. Selain karena sistem keamanan yang lemah, salah satu kemungkinan yang menyebabkan Indonesia rawan terkena serangan adalah ketidaktahuan pengguna terhadap bahayanya cybercrime. Saat ini sudah banyak perusahaan di Indonesia yang sudah menerapkan digitalisasi, namun tidak di imbangi dengan peningkatan sistem keamanan yang baik [1]. Dalam menjaga keamanan jaringan, diterapkan konsep atau hukum dasar yang biasa disebut CIA yang merupakan *Confidentiality* (kerahasiaan), *Integrity* (integritas) Availability (ketersediaan). *Confidentiality* adalah seperangkat aturan yang membatasi akses ke informasi. *Integrity* adalah jaminan bahwa informasi itu dapat dipercaya dan akurat, serta *Availability* yang merupakan konsep dimana informasi tersebut selalu tersedia ketika dibutuhkan oleh orang-orang yang memiliki akses atau wewenang.

Perusahaan sekuriti yaitu "*Kaspersky Labs*" memprediksi tren terbaru serangan siber bakal mengemuka pada tahun 2019. Beberapa serangan siber tersebut bisa terjadi kapan saja tanpa mengenal target serta ruang dan waktu. Terutama dengan semakin terbukanya pengetahuan tentang *hacking* dan *cracking* yang didukung oleh tools yang bisa didapatkan dengan mudah dan gratis. Selain itu ancaman keamanan jaringan komputer

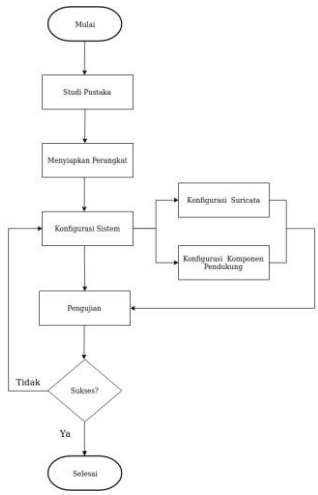
juga datang dari virus, *malicious*, *trojan*, *worm*, DOS, *spoofing*, *sniffing*, *spamming*, dan lainnya [2].

Ancaman berikutnya yang sangat membahayakan adalah *Distributed Denial of Services*, dimana serangan ini memanfaatkan sejumlah besar komputer untuk menjalankan serangan DoS kepada *server, web services*, atau sumber daya jaringan lainnya [3]. Banyak metode yang bisa dilakukan untuk dapat mengamankan sebuah sistem jaringan. Salah satunya adalah dengan menggunakan *Intrusion Prevention System* (IPS). Pada saat bekerja, IPS akan membuat akses control dengan melihat konten aplikasi sehingga IPS mampu mencegah serangan yang datang dengan bantuan administrator dan akan menghalangi suatu serangan. IPS sendiri merupakan kombinasi antara fasilitas *blocking capabilities* dari firewall dan kedalaman inspeksi paket data dari Intrusion Detection System[2]. IPS mengkombinasikan teknik firewall dan metode IDS dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang akan masuk ke jaringan local dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat serangan teridentifikasi [4].

Dengan adanya permasalahan tersebut, maka dilaksanakan penelitian dengan judul "Penerapan Intrusion Prevention System (IPS) Sebagai Pengamanan Dari Serangan DDoS *(Distributed Denial of Service*)" . Sehingga dapat memberikan keamanan jaringan dan mendeteksi dari serangan DDoS menggunakan sistem tersebut.

II. METODE PENELITIAN

Pada tahapan penelitian ini yaitu menguraikan seluruh kegiatan yang akan dilakukan oleh penulis selama penelitian berlangsung. Berikut tahapan yang akan dilakukan adalah sebagai berikut:



Gambar 2.1 Tahapan Penelitian

A. Studi Pustaka

Pada tahap awal ini adalah studi pustaka yang berguna untuk mendukung penelitian yang akan dikerjakan. Teori-teori yang didapat dan bersumber dari buku, jurnal, website dan peneliti sejenis

B. Menyiapkan Perangkat

Tahapan selanjutnya adalah menyiapkan perangkat dari persiapan alat yang dibutuhkan dalam pengkonfigurasian sistem sampai pengujian sistem.

Tabel 1. Spesifikasi Perangkat Keras

No	Perangkat Keras	Spesifikasi	Keterangan
1	1 Buah Laptop	Lenovo G40-45, OS Ubuntu, Prosessor A8-6410 4 Cores 2.0 GHz up to 2.4 GHz, RAM 8GB, Display 14.0 HD	Sebagai Server
2	1 Buah Laptop	Acer Aspire E5-476G-34UX, OS Archlinux, Processor Core i3, RAM 8 GB DDR4, Display 14.0 HD	Sebagai Penyerang
3	1 Buah *Access Point*	TP-Link , TL-WA5110G	Sebagai WLAN

Tabel 2. Spesifikasi Perangkat Lunak

No	Perangkat Lunak	Keterangan
1	Linux Ubuntu	Sistem Operasi yang digunakan server
2	Arch Linux	Sistem Operasi yang digunakan oleh penyerang
3	Suricata	Tools yang digunakan sebagai IPS
4	Hping3	Tools yang digunakan sebagai penyerang
5	LOIC	Tools yang digunakan sebagai penyerang
6	Wireshak	Untuk mengetahui traffic serangan yang masuk

C. Koonfigurasi Sistem

Tahap ini merupakan tahapan untuk konfigurasi pada server suricata IPS. Adapun tahap- tahap konfigurasinya yaitu:

Tabel 3. Konfigurasi Suricata

Konfigurasi Suricata :
1. *Install* Suricata
2. Mengkonfigurasi Suricata menjadi mode inline
3. Konfigurasi *rules* Suricata

Tabel 4. Konfigurasi Komponen Pendukung

Konfigurasi Komponen Pendukung
1. Konfigurasi IPTables
2. Konfigurasi ELK Stack
3. Konfigurasi Apache2

D. Pengujian

Pada tahapan pengujian ini, dilakukan pada jaringan lokal. Pengujian dengan melakukan serangan dari attacker untuk menguji sistem Intrusion Prevention System (IPS) Suricata dan firewall IPTables yang sudah diterapkan. Pengujian serangan dilakukan dengan melakukan penyerangan terhadap web uji coba yang sudah penulis buat dengan menggunakan dua tools untuk melakukan serangan request flooding. Tools yang digunakan menggunakan Hping3 dan Loic. Setelah dilakukan serangan, alert/log deteksi dapat langsung masuk kedalam ELK Stack yang sudah dikonfigurasikan oleh penulis.

III. HASIL PENELITIAN

Gambar 3.1 Tahapan Konfigurasi dan Pengujian

Tahapan ini membahas mengenai konfigurasi dan pengujian pada penelitian ini.

A. Instalasi dan Konfigurasi Suricata

Pada tahap ini peneliti melakukan instalasi dan konfigurasi Suricata pada jaringan lokal yang digunakan sebagai sistem penerapan keamanan dari serangan distributed denial of service.

B. Konfigurasi IPTables

Tahapan konfigurasi IPTables merupakan tahapan setelah konfigurasi suricata. IPTables merupakan firewall yang digunakan pada penelitian ini.

C. Konfigurasi Apache2

Tahapan konfigurasi apache2 ini bertujuan sebagai webserver dari web yang akan digunakan sebagai uji coba penyerangan.

D. Konfigurasi ELK Stack

ELK Stack (Elasticsearch, Logstash, Kibana) merupakan tempat log/ alert penyimpanan yang di konfigurasikan untuk menampilkan hasil log serangan yang masuk kedalam ips suricata yang sudah dibuat. ELK Stack memiliki fungsi untuk menyimpan alert yang masuk ke dalam server dan menampilkan atau memvisualisasikannya dalam bentuk web.

E. Melakukan Penyerangan

Pada tahapan ini attacker atau penyerang melakukan pengujian serangan DDoS pada web uji coba serangan yang sudah penulis buat. Penyerangan dilakukan dengan menggunakan dua tools yang berbeda yaitu hping3 dan LOIC dengan mengirimkan request yang berbeda untuk menyerang server ips suricata.

F. IPS melakukan Blok Akses

Setelah pengujian serangan dilakukan, tahapan selanjutnya adalah server ips suricata yang sudah dikonfigurasikan dengan firewall iptables dapat memblokir serangan yang masuk pada server yang dapat dilihat melalui monitoring traffic pada wireshak.

G. Mengirimkan Log serangan ke ELK Stack

Setelah attacker melakukan penyerangan dan sistem IPS suricata dapat melakukan blok akses, maka otomatis alert yang terdeteksi akan masuk ke dalam service ELK Stack yang sudah dikonfigurasi dan di visualisasi kan hasil alert/log tersebut dalam bentuk web.

IV. PEMBAHASAN

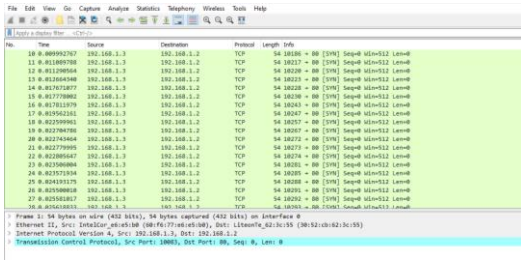
Setelah dilakukannya pengujian serangan *syn flood* maka pada tahap ini akan dijelaskan hasil dari pengujian serangan, deteksi serangan dan penerapan ips suricata.

A. Hasil Deteksi Serangan

Gambar 3.1 Hasil Deteksi Serangan

Pada gambar 3.1 didapatkan bahwa Suricata dapat mendeteksi adanya serangan masuk seperti waktu, tanggal masuknya serangan yaitu “01/22/2020-13:57:58” . Dan juga dapat dilihat bahwa terdeteksi adanya ip penyerang yaitu “192.168.1.3” .

B. Hasil Penerapan IPS Suricata



Gambar 3.2 Hasil penerapan IPS Suricata

Gambar 3.2 menjelaskan bahwa pada kolom “Info” ketika “SYN” atau adanya serangan/packet yang masuk, maka server tidak merespon atau mengirim respon balik kepada *attacker* karena sudah adanya *blok akses* dan sudah dijalankannya *firewall iptables* pada ips Suricata.

C. Hasil Log Serangan

Gambar 3.3 Hasil Log Serangan

Gambar 3.3 diatas adalah hasil dari *log/alert* serangan pada web kibana. Pada gambar tersebut terlihat tanggal, bulan, dan tahun serta waktu masuknya serangan. Pada web tersebut juga terlihat grafik serangan yang masuk pada server IPS Suricata.

V. PENUTUP

A. Kesimpulan

Dari hasil pengujian serangan, dan analisis pada penelitian ini, maka dapat ditarik kesimpulan yaitu sebagai berikut :

a. Dengan menggunakan dua *tools* dalam pengujian serangan DDoS yang dilakukan, serangan DDoS berhasil membuat web uji coba menjadi tidak dapat diakses
b. IPS Suricata mampu mendeteksi adanya serangan masuk dan didapatkan waktu, tanggal, serta IP penyerang yaitu “192.168.1.3”
c. IPS Suricata dengan *fitur inline* dan *firewall* IPTables berhasil dan mampu menolak akses serangan DDoS.
d. Hasil deteksi beserta grafik serangan yang masuk dapat dilihat pada *ELK Stack*

B. Saran

Saran yang dapat peneliti sampaikan untuk pengembangan penelitian selanjutnya adalah:

a. Menguji coba dengan beberapa serangan yang berbeda dan menambahkan rules pada konfigurasi Suricata.
b. Membuat notifikasi adanya serangan yang masuk dalam bentuk web untuk memudahkan admin mengetahui adanya serangan

ACKNOWLEDGMENT

Terimakasih saya ucapkan sebesar- besarnya kepada pembimbing saya Bapak Wahyu Adi Prabowo S.Kom.,M.B.A.,M.Kom dan Bapak Muhamad Fajar Sidiq S.T.,M.T yang telah memberikan ilmu serta saran dan bantuannya dalam menyelesaikan penelitian ini.

DAFTAR PUSTAKA

[1] F. Nkd, “Mengetahui 3 Contoh Kasus Cyber Crime di Indonesia,” 2019. [Online]. Available: https://www.logique.co.id/blog/2019/03/20/kasus-cyber-crime-di-indonesia/.

[2] Y. A. Widya Pradipta, “IMPLEMENTASI INTRUSION PREVENTION SYSTEM

(IPS) MENGGUNAKAN SNORT DAN IP TABLES BERBASIS LINUX," p. 8, 2017.

[3] S. Geges and W. Wibisono, "Pengembangan Pencegahan Serangan Distributed Denial of Service (Ddos) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle," *JUTI J. Ilm. Teknol. Inf.*, vol. 13, no. 1, p. 53, 2015.

[4] D. M. Myzda, "Analisa Dan Konfigurasi Network Intrusion Prevention System (Nips) Pada Linux Ubuntu 10 . 04 Lts," 2011.