JIMP - Jurnal Informatika Merdeka Pasuruan
Vol 5 No 1 Maret 2020
ISSN 2503-1945

Implementasi Monitoring Jaringan Melalui Aplikasi Sosial Media *Telegram* Dengan *Snort*

Danu Kusuma[1], Ucuk Darusalam[2], Deny Hidayatullah[3]
Fakultas Teknologi Komunikasi dan Informatika, Universitas Nasional
Email: **Danukusuma05@gmail.com**[1], ucuk.darusalam5@gmail.com[2], Rafaderi@gmail.com[3]

Abstract

By denying that the internet is developing and advancing at this time, IDS (Intrusion Detection System) is needed which can support external attacks in the form of warnings from Snort. Monitoring network security is one of the efforts of the administrator to keep the security network protected from adverse external attacks. Telegram is a messenger application that will help administrators to monitor networks more easily. Because every attack issued by Snort will give a warning to the Telegram and be received by the administrator. From the Telegram you will see the type of attack and the status of the malicious attack or not for the administrator.
Keywords *- Monitoring, networking, snort, telegram, alert*

Abstrak

Dengan meningkatnya kejahatan internet di era berkembang dan maju saat ini, maka di butuhkan IDS (Intrusion Detection System) yang dimana dapat mendeteksi serangan-serangan dari pihak luar berupa alert dari Snort. Memonitoring keamanan jaringan adalah salah satu upaya dari pihak administrator agar tetap menjaga alur jaringan terhindar serangan-serangan dari pihak luar yang merugikan. Telegram adalah aplikasi messenger yang akan membantu pihak administrator untuk memonitoring jaringan lebih mudah. Karena setiap serangan yang terdeteksi oleh Snort akan memberikan alert ke Telegram dan di terima oleh pihak administrator. Dari Telegram akan terlihat jenis serangan dan status serangan berbahaya atau tidak bagi administrator.
Kata kunci *- Monitoring, jaringan, snort, telegram, alert*

I. PENDAHULUAN

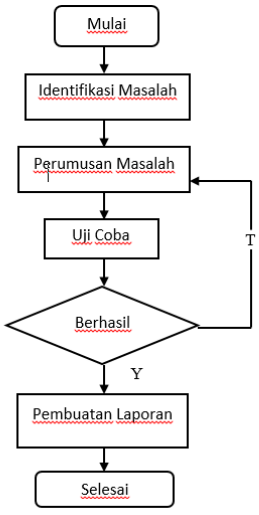
Berkembangnya suatu teknologi yang saat ini sudah di gemari banyak orang tidak mungkin berjalan dengan baik-baik saja. Teruntuk banyaknya kejahatan yang sering kali kerap muncul di lingkungan sekitar. Mengelola keamanan jaringan adalah suatu hal yang harus di persiapkan karena kita harus dapat menjaga keamanan data dengan baik. Terlebih adanya serangan-serangan dari luar yang tidak di ketahui kapan terjadi. *IDS (Instruction Detection System)* adalah suatu aplikasi yang dapat mendeteksi serangan-serangan dari luar. Aplikasi ini bersifat *open source* untuk mendeteksi serangan-serangan dari luar. Dengan adanya *Snort* sebagai perangkat lunak yang mendeteksi serangan mencurigakan. Monitoring adalah hal mendasar jika kita ingin tetap menjaga keamanan suatu data atau jaringan yang kita miliki, dan adanya *Telegram* sebagai aplikasi *messenger* yang mempermudah administrator untuk memonitoring jaringan dari jarak jauh. Hal ini di sebabkan karena di era sekarang sudah banyak yang tak asing dengan *Telegram* messenger, terlebih sudah banyak para administrator yag memiliki kapasitas smart phone untuk men*download telegram* dan memakai dengan baik. Dengan menggabungkan sistem kinerja snort sebagai pendeteksi serangan dan telegram sebagai aplikasi yang akan mengeluarkan sebuah *output* alert adanya bahaya penyusup ini akan memudahkan para administrator untuk memonitoring.

II. MASALAH

Pada penelitian ini di tententukan beberapa batasan masalah, yaitu sebagai berikut:

1. Sistem ini dibuat untuk mempermudah pihak administrator jaringan.
2. Telegram mampu menerima notifikasi yang dikirim snort dari beberapa serangan
3. Notifikasi yang diterima oleh telegram dari snort berkisar 1-3 menit

III. METODE PELAKSANAAN



Gambar 1. Flowchart Perancangan

Mengidentifikasi traffic-trafic jaringan yang mencurigakan dengan monitoring adalah salah satu hal yang dapat meminimalisir kejadian yang tidak kita inginkan, dengan adanya snort sebagai *IDS (Instruction Detection Sysytem)* yang membantu.

A. *IDS (Instruction Detection System)*

Intrusion Detection System(IDS) merupakan sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan pada sebuah sistem atau jaringan. Jika ditemukan aktivitas yang mencurigakan pada traffic jaringan maka IDS akan memberikan sebuah peringatan terhadap sistem atau administrator jaringan dan melakukan analisis dan mencari bukti dari percobaan penyusupan. Jenis-jenis *Intrusion Detection System(IDS).*

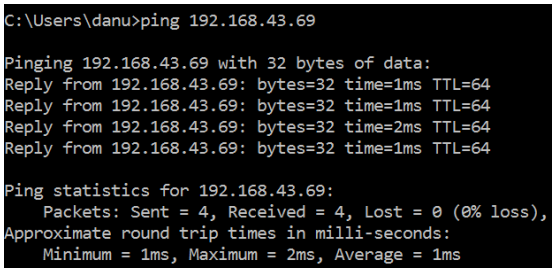
a. ***NIDS (Network Instrucion Detection System)*** berbasis jaringan ini akan ditempatkan pada suatu titik strategis dalam jaringan untuk melakukan pengawasan jalur lintasan traffic dan menganalisis apakah ada percobaan penyerangan atau penyusupan ke dalam sistem jaringan.

b. ***HIDS (Host Intrusion Detection System)*** IDS jenis ini akan menganalisis aktivitas sebuah host jaringan individual apakah terdapat percobaan penyerangan atau pengusupan ke dalam jaringan dan melakukan pengawasan terhadap paket-paket yang berasal dari dalam maupun luar hanya pada satu alat saja dan kemudian memberikan peringatan terhadap sistem atau administrator jaringan.

c. ***Anomaly Based IDS***

Metode ini ini melibatkan pola lalu lintas yang mungkin sebuah serangan yang sedang dilakukan oleh penyerang. Umumnya metode ini menggunakan teknik statistik untuk membandingkan lalu lintas yang sedang dianalisis dengan lalu lintas normal yang biasa terjadi. Metode ini menawarkan kelebihan dibandingkan dengan signature-based IDS yakni dapat mendeteksi bentuk serangan yang baru dan belum terdapat didalam basis data signature-based IDS. Kelemahannya, jenis ini sering mengeluarkan pesan false positive. Sehingga tugas administrator lebih rumit, dengan harus memilah-milah mana yang merupakan serangan yang sebenarnya dari banyaknya pesan false positive yang muncul.

III. HASIL DAN PEMBAHASAN



Gambar 2. *Ping/icmp attack* dari cmd ke ubuntu

Gambar di atas menunjukkan *snort* dapat mendeteksi serangan jaringan yang tidak biasanya melalui trafic jaringan tersebut. Ada bebrapa jenis serangan yang terdeteksi oleh snort dan di tampilkan oleh *telegram*. *Icmp attack*, si penyerang akan memulai serangan dengan membuat paket-paket "*icmp-event request*" dengan alamat IP sumber berisi alamat IP *host* target yang akan diserang.

Gambar 3. Hasil Notifikasi T*elegram*

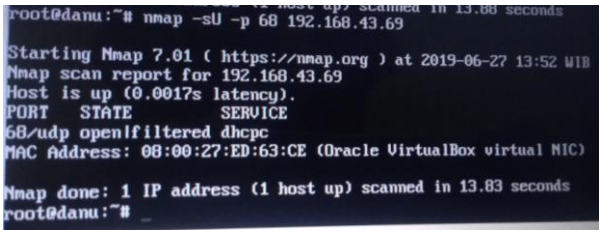
Hasil di atas menunjukkan ip 20 menyerang ip 69 dengan status serangan safe (aman). Namun ip 69 yang di serang tidak terdaftar di sebuah company/perusahaan.

Gambar 4. Serangan tcp dengan port 21

Gambar di atas menunjukkan cara penyerangan *tcp* dengan menggunakan nmap yang di install dalam snort dan dengan port 21 untuk penyerangan tersebut. *Tcp detection scan,* menunjukkan serangan terhadap pihak administrator bahwa adanya serangan yang terdeteksi.

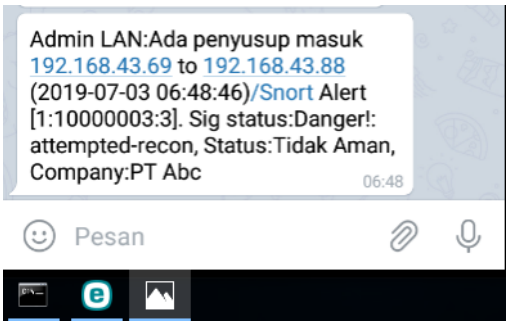
Gambar 5. Hasil Notifikasi *Telegram*

Hasil di atas menunjukkan ip 69 menyerang ip 88 dengan status serangan safe (aman). Ip 88 terdaftar dalam company/perusahaan PT Abc sehingga serangan ini tidak menimbulkan bahaya.



Gambar 6. Serangan udp dengan port 68

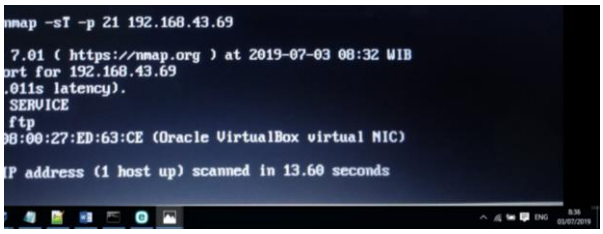
Gambar di atas menunjukkan cara penyerangan *udp* dengan menggunakan nmap yang di install dalam snort dan dengan port 68 untuk penyerangan tersebut. *Udp detection scan* menunjukkan serangan terhadap pihak administrator bahwa adanyan serangan yang terdeteksi.



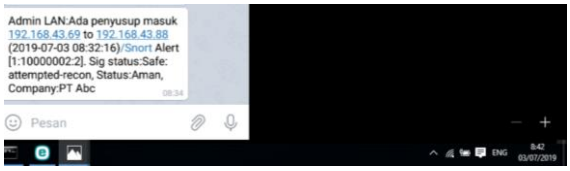
Gambar 7. Hasil Notifikasi T*elegram*

Hasil di atas menunjukan ip 69 menyerang ip 88 dengan serangan berbeda dengan status serangan danger (tidak aman). Ip 88 terdaftar dalam company/perusahaan PT Abc sehingga pihak administrator akan menanggapi pesan tersebut dengan baik.

Beberapa percobaan menunjukkan ketepatan dan kecepatan telegram dalam memberi informasi.

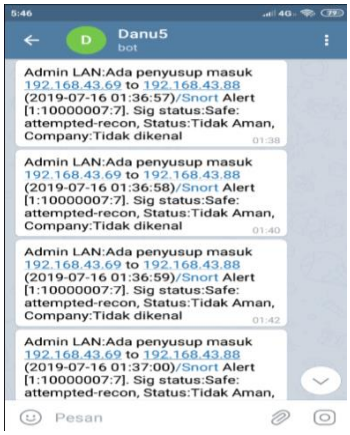


Gambar 8. Serangan pkul 08.32 dengan port 21

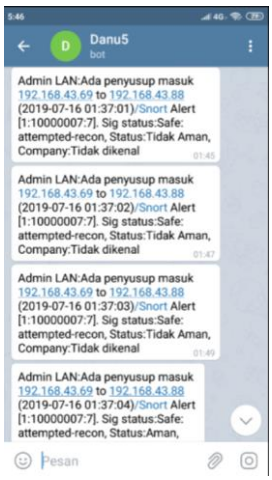


Gambar 9. Hasil Notifikasi *Telegram*

Salah satu contoh pada pukul 08.32 mencoba menyerang dengan menggunakan port 21 dan hasil yang di terima telegram pukul 08.34



Gambar 10. Hasil udp flood



Gambar 11. udp flood membanjiri notifikasi telegram

Udp flood adalah suatu serangan yang sifatnya mengirim dan membanjiri lalu lintas server agar terjadi kelambatan untuk beraktifitas yang jumlah serangan/paketnya bisa sampai ribuan.

IV. KESIMPULAN

Berdasarkan kesimpulan di atas, dan bebrapa uji coba yang di lakukan.

1. Setelah uji coba berhasil, pihak administrator dapat menerima pesan dari telegram.
2. Berdasarkan hasil pendeteksian dari snort, aplikasi telegram dapat menerima notifikasi 1-3 menit. Tergantung koneksi dan keberadaan administrator.
3. Di satu sisi telegram hanya akan menerima satu notifikasi dari satu serangan yang sama di menit yang sama di karenakan guna meminimalisir terjadinya handphone administrator lemot karena adanya banyak notif dan agar penyimpanan riwat chat administrator tidak penuh.

DAFTAR PUSTAKA

[1] Asep Fauzi Mutaqin, Rancang Bangun Sistem Monitoring Keamanan Jaringan Prodi Teknik Informatika Melalui SMS Alert dengan Snort. Jurnal Sistem dan Teknologi Informasi (JUSTIN) (2016).
[2] Lidia Putri, Implementasi Instruction Detection SystemMenggunakan Snort Pada Jaringan Wireless (Studi Kasus: SMK Triguna Ciputat) (2011).
[3] Rizki Triandini, IMPLEMENTASI INTRUSION DETECTION SYSTEM MENGGUNAKAN SNORT, BARNYARD2 DAN BASE PADA SISTEM OPERASI LINUX. (2016).
[4] Ery Setiyawan Jullev Atmaji, Bekti Maryuni Susanto, Monitoring Keamanan Jaringan Komputer Menggunakan Network Intrussion Detection System (NIDS) (2016).
[5] Dias Utomo, Muchammad Sholeh, Arry Avorizano, Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram (2017).
[6] Zaki Akhyar, Hendrawaty , Azhar, Rancang Bangun Sistem Pengiriman Alert Instrusion Detection System Suricata Melalui Telegram (2018).
[7] Khairulanam, Sistem Pendeteksi Serangan Pada Jaringan Komputer Menggunakan Snort Berbasis Sms Gateway (Studi Kasus: Taman Pintar Yogyakarta) (2011).
[8] Rico Ronaldo, Implementasi Sistem Monitoring Jaringan Menggunakan Mikrotik Router OS di Universitas Islam Batik Surakarta.
[9] Rishabh Upadhyay, Chatbot Platform As Command & Control Channel In Botnet (2017).
[10] Mohamad Hanif Md Saad#, Rabiah Adawiyah Shahad*, Mohamad Zaki Sarnon*, Muhammad Faiz Mohd Shukri*, Aini Hussain, Smart Pump Operation Monitoring and Notification (PuMa) Via Telegram Social Messaging Application (2017).
[11] Arpenta L.T. Ginting, Junika Napitupulu, Jamaluddin Jamaluddin, Sistem Monitoring Pendeteksian Penyusup Menggunakan Snort pada Jaringan Komputer Fakultas Ekonomi Universitas Methodist Indonesia (2015).
[12] Yohanes Priyo Atmojo, Bot Alert Snort dengan Telegram Bot API pada Intrusion Detection System: Studi Kasus IDS pada Server Web (2018).
[13] Arief Prasetyo, Luqman Affandi , Dedi Arpandi ,IMPLEMENTASI METODE NAIVE BAYES UNTUK INTRUSION DETECTION SYSTEM (IDS) (2018)