OPEN ACCESS
J. OF ICT, VOL. 1, NO. 2, PP.045-053, MAY 2019

ISSN : 2686-1089 (ONLINE)
DOI: XXXXXX

Journal of Informatics and Communications Technology (JICT)

MONITORING SISTEM KEAMANAN JARINGAN BERBASIS TELEGRAM BOT PADA LOCAL AREA NETWORK

Roni Reza Abdullah [#1], Ade Nurhayati [*2]

Teknik Telekomunikasi, *Akademi Teknik Telekomunikasi Sandhy Putra Jakarta*
JL Daan Mogot KM 11 Jakarta Barat Indonesia

[1] Ronireza520@gmail.com
[2] adenurhayati@akademitelkom.ac.id

Received on dd-mm-yyyy, revised on dd-mm-yyyy, accepted on dd-mm-yyyy

Abstract

Menerapkan sistem keamanan dalam jaringan LAN adalah suatu keharusan agar mendapatkan kenyamanan dalam penggunaan, salah satunya adalah keamanan server. Dengan menggunakan snort untuk mendeteksi serangan menuju ICMP, TCP dan UDP secara real time akan dikirim menuju bot telegram yang sudah di integrasikan dengan shell-bot agar bot telegram tidak hanya berguna sebagai notifikasi dari snort tetapi bisa digunakan sebagai pemblok ip saat terdeteksi adanya serangan, maka admin dapat mengetahui apa yang di lakukan attacker di dalam sebuah server. Selain itu menerapkan honeypot dapat berguna untuk mengalihkan attacker menuju server palsu yang sudah di buat menyerupai dengan server asli akan merekam semua tindakan yang di mulai dari cara masuk hingga perubahan yang di lakukan di dalam server palsu tersebut, semua rekaman yang di lakukan honeypot dapat di lihat oleh administrator melalui terminal linux di kippo.log.

Kata Kunci : Shell-Bot, Bot Telegram, Snort, Honeypot, IDS, IPS

I. PENDAHULUAN

Sistem Keamanan jaringan komputer merupakan suatu sistem untuk mencegah dan mengidentifikasi pengguna yang tidak sah dari jaringan komputer. Dengan menggunakan sistem keamanan Intrustion Detection System (IDS) dan Intrusion Prevention System (IPS) yang di gunakan sebagai pelengkap teknologi keamanan dimana sistem pertahanan akan dapat mengambil tindakan sesuai dengan data pengaplikasian yang jelas dan dapat menindak lanjuti laporan dari data yang sudah valid. Tools (Intrustion Detection System) IDS yang akan digunakan salah satunya adalah snort yang diintegrasikan dengan Bot Telegram agar bisa memonitoring jaringan secara realtime. Bot Telegram akan mengirimkan notifikasi ke admin ketika terjadi serangan yang terindentifikasi oleh tools Snort.

A. *Tujuan Penelitian*

Tujuan penelitian ini adalah sebagai berikut :

1. Memanfaatkan Bot Telegram sebagai notifikasi untuk system keamanan jaringan
2. Meminimalkan serangan attacker ke jaringan Local Area Network(LAN).

B. *Rumusan Masalah*

Masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Sistem Intrustion Detection System (IDS) pada tools Snort dan Honeypots
2. Sistem Intrusion Prevention System (IPS)
3. Perancangan Boot Telegram menjadi notifikasi dari tools Snort
4. Implementasi keamanan jaringan di Local Area Network (LAN)

C. *Metodologi Penelitian*

Adapun metode penelitian dalam proyek akhir ini adalah sebagai berikut :

1. Studi Literatur
   Perancangan dan pengumpulan kajian – kajian yang berkaitan dengan masalah – masalah yang ada dalam Proyek Akhir , baik dari internet, buku referensi , jurnal dan lain lainnya
2. Riset dan Implementasi
   Metode ini di lakukan dengan meriset sebuah keamanan jaringan yang penulis pelajari dari jurnal atau buku yang penulis ambil sebagai referensi.

II. STUDI LITERATURE

2.1 Keamanan Jaringan

Kemanan jaringan komputer adalah komputer yang terhubung dengan jaringan yang mempunyai keamanan yang lebih tinggi dari pada komputer yang tidak terhubung ke jaringan. Dengan pengendalian yang teliti resiko tersebut dapat di kurangi[3]. Namun keamanan jaringan biasanya bertentengan dengan jaringan akses , dimana bila jaringan akses semakin mudah, maka keamanan jaringan akan semakin rawan. Beberapa ancaman yang umum pada jaringan LAN, antara lain[2] :

1. Man In The Midle Attack :
   Metode serangan ini biasanya di dahului dengan ARP Spoffing kemudian penyerang menempatkan perangkat yang di milikinya sebagai komputer fiktif yang terlihat resmi dari sisi accsess point.
2. Brute Force
   Serangan brute-force adalah sebuah serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemprosesan komputer di bandingkan kecerdasaan manusia.
3. Snipper
   Suatu serangan kemananan jaringan dalam bentuk sniffer (atau di kenal sebagai snooping attack) merupakan kegiatan user peruskan yang ingin mendapatkan informasi tentang jaringan atau traffic lewat jaringan tersebut. Suatu Sniffer sering menemukan program penangkapan paket yang bisa menduplikasikan isi paket yang lewat media jaringan kedalam. Serangan Sniffer sering di fokuskan pada koneksi awal antara client dan server untuk mendapatkan logon credensial, kunci rahasia, password dan lainnya.
4. Denial Of Service
   Metode dengan mengirimkan paket data dalam jumlah yang sangat besar terhadap jaringan yang menjadi targetnya secara terus menerus . Hal ini dapat menggangu lalulintas data bahkan kerusakan sistem jaringan pada jaringan LAN semua data di lewatkan dalam suatu medium gelombang radio (udara) , bukan dalam medium lebih aman seperti kabel pada jaringan kabel. Hal ini berarti aliran data pada jaringan nirkabel dapat dengan mudah di sadap oleh orang-orang yang tidak berhak.

2.2 Sistem Keamanan Jaringan

1. Intrusion Prevention System (IPS)

IPS (Intrusion Prevention System) adalah sebuah perangkat jaringan atau perangkat lunak yang berjalan di belakang firewall untuk mengidentifikasi dan memblokir ancaman terhadap jaringan dengan menilai setiap paket yang melintas berdasarkan protokol jaringan dalam aplikasi dan melakukan pelacakan ancaman terhadap keamanan jaringan. IPS membuat akses kontrol dengan cara melihat konten aplikasi, daripada melihat IP address atau ports yang biasanya digunakan oleh Firewall. Sistem IPS sama dengan sistem setup IDS, IPS mampu mencegah serangan yang datang dengan sedikit bantuan dari administrator atau bahkan tidak sama sekali. Serangan biasanya datang dalam bentuk input data berbahaya ke aplikasi target atau melalui layanan yang digunakan penyerang untuk mengganggu dan menguasai aplikasi atau jaringan target, setelah penyerang atau penyusup berhasil masuk dan menguasai jaringan maka penyerang dapat menonaktifkan

Gambar 2. Topologi Sistem IDS dan IPs

jaringan target atau bahkan bisa mengakses semua izin dari aplikasi atau jaringan target. Oleh karena itu IPS akan menghalangi suatu serangan sebelum terjadi eksekusi dalam memori dan IPS akan membandingkan file checksum yang tidak semestinya mendapatkan izin untuk dieksekusi dan juga menginterupsi sistem telfon.
Macam-macam IPS :
1.a Host-based Intruction Prevention System (HIPS)
Sebuah sistem pencegahan yang terdiri dari banyak lapisan, menggunakan packet filtering, inspeksi status dan metode pencegahan yang bersifat real-time untuk menjaga host berada dibawah keadaan dari efisiensi performansi yang layak. Mekanisme kerjanya yaitu dengan mencegah kodekode berbahaya yang memasuki host agar tidak dieksekusi tanpa perlu mengecek threat signature.
1.b Network-based Intruction Prevention System (NIPS)
IPS jenis ini dapat menahan semua traffic jaringan dan memeriksa kelakuan dan kode yang mencurigakan. IPS jenis ini menggunakan in-line model, sehingga performansi tinggi merupakan sebuah elemen krusial dari perangkat IPS untuk mencegah bottleneck pada jaringan. Oleh karena itu, NIPS biasanya didesain menggunakan 3 komponen untuk mengakselerasi performa bandwidth. NIPS melakukan pantauan dan proteksi dalam satu jaringan secara global. NIPS menggabungkan fitur IPS dengan firewall dan kadang disebut sebagai In-Line IDS atau Gateway Intrusion Detection System (GIDS).
2.a Intrusion Detection System (IDS)
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.
Macam-macam IDS adalag sebagai berikut :
2.b Network Intrusion Detection System (NIDS)
IDS 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. 2. Host Intrusion Detection System (HIDS) 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
2.3 Snort
Snort merupakan sebuah aplikasi ataupun software yang bersifat opensource GNU General Public License [GNU89], sehingga boleh digunakan dengan bebas secara gratis, dan kode sumber (source code) untuk Snort juga bisa didapatkan dan dimodifikasi sendiri .Snort dikembangkan oleh Marty Roesch, bisa dilihat pada (www.sourcefire.com). Awalnya dikembangkan di akhir 1998-an sebagai sniffer dengan konsistensi output[9].
2.4 Honeyspot
Honeypot merupakan sebuah sistem yang di bangun menyerupai atau persis dengan sistem yang sesungguhnya, dengan tujuan agar para attacker teralih perhatiannya dari sistem utama yang akan di serang, dan beralih menyerang ke sistem palsu tersebut. Saat ini honeypot tidak hanya berfungsi atau bertujuan untuk bertujuan menjebak attacker untuk melakukan serangan ke server asli, namun honeypot juga bermanfaat untuk para system administrator atau security analyst, untuk menganalisa aktifitas apa saja yang dilakukan oleh atacker / malware yang terdapat di dalam sistem honeypot tersebut[2].
2.5 Telegram Bot
Aplikasi instan messaging Telegram memiliki Application programing Interface (API) yang dapat di gunakan oleh publik. Berbeda dengan instan messaging lainya seperti Whatsapp dan LINE. Pada instant messaing Whatsapp tidak menyediakan API bagi publik, tetapi aplikasi LINE menyediakan API dengan versi trial atau terbatas. API yang di sediakan oleh Telegram dapat gunakan oleh siapapun dan tanpa batas. Telegram juga memiliki Bot API yang memungkinkan untuk dengan mudah membuat program yang menggunakan pesan Telgram sebagai antarmuka. API ini memungkinkan pengembang untuk menghubungkan Bot pada sistem Telegram. Telegram Bot merupakan cara khusu yang tidak memerlukan nomor telepon tambahan sebagi syarat khususnya. Akun Bot tersebut berfungsi sebagai antar muka untuk kode yang dapat di jalankan pada server pengembang[6].

III. METODE PENELITIAN

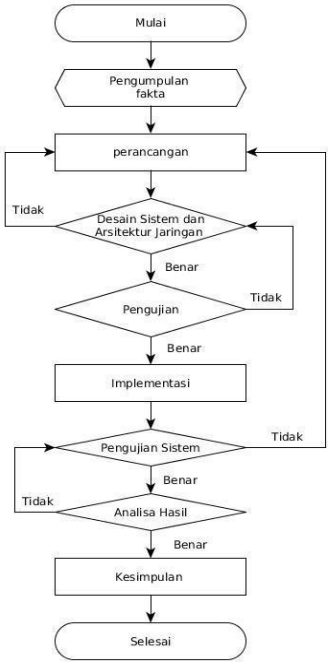
Gambar 2. Topologi Sistem IDS dan IPs

Penelitian ini dilakukan dengan merancang suatu sistem telegram bot sebagai bantuan monitoring untuk sistem keamanan. Dalam penelitian ini diperlukan beberapa komponen antara lain :

A. Kebutuhan Perangkat Keras
   1. Komputer *Server* (IPS dan IDS)
   2. Komputer *Attacker*

B. Kebutuhan Perangkat Lunak
   1. *Snort 2.9.9.0*
   2. *Honeypot*
   3. *Zenmap*
   4. *Cmd*
   5. *Bot Telegram*
   6. *Putty*

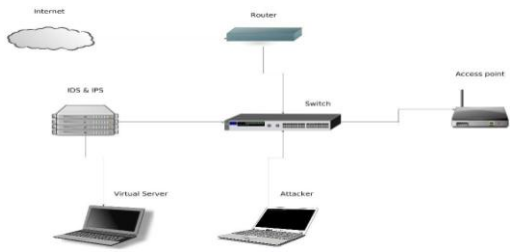
C. Diagram alir Penelitian



Gambar 1. Diagram Alir penelitian

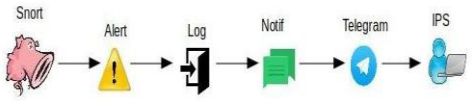
D. Sistem IDS dan IP

Untuk mengirimkan serangan kepada aplikasi *instant messaging telgram*, memanfaatkan API yang memungkinkan *software* dapat berkomunikasi dengan program lainnya *APP* di bangun mengunakan bahasa *bash script* yang bertujuan untuk menghubungkan aplikasi *telegram* dengan App untuk memeriksa informasi terbaru pada *log* yang tersedia di kirimkan ke telegram sebagai notifikasi



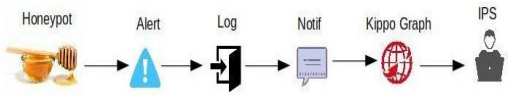
Gambar 3. Desain Sistem

Gambar 2. Topologi Sistem IDS dan IPs



Gambar 4. Alur informasi pengiriman serangan ke *Telegram*

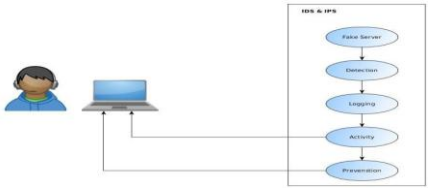
Untuk merekam aktivitas serangan dari *attacker*, seperti *brute force* dan yang paling penting adalah melakukan interaksi pada attacker dengan cara meniru service ssh.



Gambar 5. Alur informasi pengiriman serangan ke kippo graph

Gambar 6. Diagram Honeypot & IPS User Use Case Sistem

Use case tersebut mempresentasikan sebuah interaksi antara aktor dengan sistem. Terdapat satu aktor yaitu



administrator dimana memiliki peran untuk mendapatkan notifikasi mengenai deteksi. Selain mendapatkan notifikasi/rekaman serangan dengan *boot telegram* dan *kippo graph*, *Administrator* juga melihat *log* di server IDS tersebut, berikut proses kerja dari mendeteksi serangan hingga mengamankan serangan.

E. Implementasi Jaringan

Sebelum melakukan pengujian, VPS (Virtual Private Server) yang terinstall snort dan honeypot perlu di rancang terlebih dahulu arsitektur jaringannya sesuai dengan gambaran umum sistem. Implementasi ini menjelaskan pengalamatan serta menkonfigurasi vps sebagai server IDS.

1. Konfigurasi IP Address IDS

Pada IDS terdapat satu buah nic yaitu enp2s0. Konfigurasi ip address ids sebagai berikut:

Tabel 1. IP Address IDS

Network Adapter	enp2s0
IP address	192.168.10.253
Netmask	255.255.255.0
Gateway	192.168.10.1

2. Konfigurasi IP Address Attacker

Komputer attacker memiliki sebauh nic, yaitu eth. Konfigurasi ip addresss pada attacker adalah sebagai berikut:

Tabel 2. IP Address Attacker

Network Adapter	Eth
IP Address	192.168.10.254
Netmask	255.255.255.0
Gateway	192.168.10.1

3. Implementasi Perangkat Lunak Snort

Gambar 2. Topologi Sistem IDS dan IPs

a. Membuat folder bernama snort_src untuk menyimpan semuanya di satu tempat
b. Download dan install library DAQ (Data AcQuisition library)
c. Download dan install zlibg
d. Download dan install snort
e. menempatkan symblink ke snort di /usr/sbin/snort
f. Uji Snort
g. Membuat pengguna dan grup snort
h. Buat direktori Snort
i. Membuat beberapa file yang menyimpan aturan dan daftar ip
j. Membuat direktori logging
k. Memberi hak akses
l. Ubah kepemilikan pada folder
m. Menyalin file konfigurasi

4. Menambah Peringatan Serangan Local

Local rules adalah sebuah lokasi yang di peruntukan sebagai lokasi konfigurasi rules yang di bisa di sesuaikan kebutuhan dari administrator. Dilakukan dengan cara sebagai berikut :

a. Masuk ke dalam local.rules root@ror24:~# nano /etc/snort/local/local.rules
b. Tambahan peringatan serangan dalam local.rules alert icmp any any -> $HOME_NET any(msg:"ICMP test detected"; GID:1; sid:10000001; rev:001;classtype:icmp-event;) alert tcp any any -> $HOME_NET 21(msg:"ICMP test detected"; GID:1; sid:10000002; rev:002;classtype:icmp-event;) alert udp any any -> $HOME_NET 68(msg:"ICMP test detected"; GID:1; sid:10000003; rev:003;classtype:icmp-event;)

5. Implementasi Telegram Bot

Artinya menjadikan Bot telegram sebagai tempat penerimaan notifikasi yang terdapat pada database snort.Telegram bot disini akan berfungsi sebagai jembatan antara sistem dan user. Dalam implementasi user harus memiliki akun telegram kemudian melakukan request kepada @BotFather untuk mendapatkan usernamebot, token, id chat user, maupun id chat grup. Berikut langkah langkahnya:

a. Melakukan pencarian id @BotFather kemudian ketikan /star

Gambar 7. Proses Pembuatan Telegram Bot

b. /newbot untuk membuat bot, setelah itu akan di minta untuk menentukan nama bot yang di inginkan, menulis nama bot, contohnya ror24_
c. Setiap Bot akan mendapatkan token
d. Implementasi Shell-Bot

Peneran Shell-bot di dalam Bot telegeram adalah agar Bot telegram bisa menyerupai terminal linux/ komunikasi dua arah.

- Download dan install shell-bot
- Install nmp
- Konfigurasi node server
- Jalankan shell-bot

Gambar 2. Topologi Sistem IDS dan IPs

IV. RESULTS AND DISCUSSION

Pengujian sistem merupakan proses terakhir untuk melakukan evaluasi atau uji coba dari penelitian yang telah di lakukan berdasarkan implementasi. Pada tahap pengujian terdiri dari beberapa skenario pengujian yang di lakukan dalam beberapa kondisi, seperti;

1. Pengujian kinerja IDS dan IPS

Pengujian ini di lakukan secara bergantian untuk mengetahui efektifitas notifikasi dan data aktivitas yang dikirimkan ke Administrator melalui Aplikasi messaging Telegram dan Kippo Graph.

Dari aktifitas pengujian terhadap server, didapatkan waktu masing masing aktifitas mulai dari penyerangan hingga terkirimnya notifikasi dan akan melakukan perbandingan waktu yang terdapat pada hasil sebelum pengembangan dari penelitian sebelumnya Hasil catatan waktu tersebut berguna untuk mengukur tingkat ke akurasian kecepatan deketeksi hingga terkirimnya alert. Berikut adalah table akurasi waktu

Tabel 3. Akurasi Waktu Terdeteksi

No	Aktifitas	Jenis serangan	Awal serangan	Diterima
1	SISTEM PENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT BERBASIS BOT TELEGRAM DI STT STIKMA INTERNATIONAL MALANG	DDOS	06.35	06.36
		Port Scan	06.20	06.21
2	IMPLEMENTASI INTRUSION PREVENTION SYSTEM PADA LOCAL AREA NETWORK	DDOS	13.54	19.35
		Port Scan	19.43	19.43
		Brute Fource	13.54	13.54

Berdasarkan table tersebut dapat disimpulkan sebagai berikut :

a. Perbandingan tingkat akurasi waktu penerimaaan yang di dapat untuk serangan DDOS masih sama tidak ada perubahan yang cukup terlihat dalam perhitungan waktu.
b. Perbandingan tingkat akurasi waktu penerimaan yang di dapat untuk serangan Port Scan mengalami peningkatan kecepatan dalam hitungan detik tidak mencapai 1menit yang di hitung dari waktu awal penyerangan hingga waktu peenerimaan deteksi.
c. Tingkat akurasi waktu yang di dapat saat terjadinya login pada ssh dengan melakukan Brute Fource tidak melebihi 1 menit dalam penerimaan.

2. Pengujian Kinerja Bot Telegram

Pengujian ini dilakukan dengan dua parameter yaitu pengujian parameter akurasi waktu dan pengujian asal serangan sesuai yang telah disetting.

a. Pengujian Akurasi Waktu Notifikasi Bot Telegram

Tabel 4. Pengujian Notifikasi Bot Telegram

No	Aktifitas	Jenis Serangan	Awal Serangan	Di Terima
1	SISTEM PENDETEKSI SERANGAN SERVER MENGGUNAKAN SNORT BERBASIS BOT TELEGRAM DI STT STIKMA INTERNATIONAL MALANG	DDOS	01.48	01.49
2	IMPLEMENTASI INTRUSION PREVENTION SYSTEM PADA LOCAL AREA NETWORK	DDOS	19.36	19.37
		Port Scan	19.43	19.43

- Perbandingan Akurasi waktu di Bot telegram sebagai notifikasi serangan DDOS tidak ada perubahan karna pengiriman menuju bot telegram sangat tergantung pada koneksi internet yang di dapat pada server dan telegram itu sendiri.

Gambar 2. Topologi Sistem IDS dan IPs

- Akurasi waktu yang yang di mulai dari awal terjadinya serangan hingga diterimanya notifikasi adalah -+ 1 menit dalam pengiriman yang di terima oleh Bot telegram.

b. Pengujian Asak Attacker

Table 5. Informasi Serangan yang Terdeteksi

No	Waktu	Asal serangan	Layanan
1	19.36.06	192.168.10.254	ICMP
2	19.43.46	192.168.10.254	TCP
3	19.47.58	192.168.10.254	UDP

Dari Hasil Pengujian di dapatkan informasi yang terdeteksi. Snort mendeteksi adanya attacker dari 192.168.10.254 melakukan serangan server yang di lindungi oleh ids. Attacker melakukan uji coba serangan pada 3 layanan yaitu ICMP,TCP, UDP.

Dari pengujian tersebut dapat dilihat pengujian keseluruhan sebagai berikut :

Tabel 6. Pengujian Sistem

No	Skenario Pengujian Sistem	Uji Coba	Hasil Yang Diinginkan	Hasil Dari Pengujian	Hasil
1	DDOS	DDOS	Terdeteksi	Terdeteksi	Berhasil
2	Scan Port TCP	Port TCP Terbuka	Terdeteksi	Terdeteksi	Berhasil
3	Scan Port UDP	Port UDP Terbuka	Terdeteksi	Terdeteksi	Berhasil
4	Brute Fource	Login SSH	Terdeteksi	Terdeteksi	Berhasil

Hasil pengujian sistem yang terjadi sudah mendapatkan hasil yang di harapkan bahwa sistem telah mendeteksi pengujian yang sudah di lakukan. Pendeteksian sudah sesuai dengan aturan yang telah di terapkan

V. Conclusion

Berdasarkan hasil perancangan, implementasi dan pengujian dari Honeypot yang berfungsi sebagai pengalihan serangan menuju server, snort sebagai pendeteksi adanya serangan menuju ICMP, TCP dan UDP di intregasikan dengan Bot telegram sebagai notifikasi dan pemblokir ip, maka dapat di ambil beberapa kesimpulan sebagai berikut:

1. Snort bekerja sesuai dengan rules yang di buat administrator sebagai pendeteksi serangan menuju ICMP, TCP dan UDP
2. Honeypot berhasil mengalihkan attacker menuju ke server palsu dan membaca tindakan attacker di dalam server honeypot
3. Bot telegram berhasil menjadi *notifikasi* dari *snort*
4. *Bot telegram* berhasil melakukan perintah *iptables* untuk melakukan pemblokiran

REFERENCES

[1] Funda Denoya Yendra Putra.(2018) Sistem Pendeteksi Serangan Server Menggunakan Snort Berbasis Bot Telegram Di STT STIKMA International Malang.Malang. (diakses pada 4 september 2018)
[2] Fauzi, Yusuf. (2017). Mengenal berbagai jenis serangan pada jaringan komputer https://netsec.id/jenis-serangan-jaringan-komputer/ (diakses pada 11 maret 2019).
[3] Syafrizal, Melvin. (2005). Pengantar Jaringan Komputer. Yogyakarta: ANDI
[4] Setiawan, Deris. (2005). Sistem Kemananan Komputer. Jakarta: PT Elex Media Komputindo.
[5] Hermawan.(2019). Pengertian server https://www.nesabamedia.com/pengertian- server- dan-fungsi-server/ (diakses pada 2 maret 2019)
[6] Pengertian Telegram https://pengertianahli.id/2014/04/pengertian-telegram-apa-itu-telegram.html (diakses pada 2 maret 2019).

Gambar 2. Topologi Sistem IDS dan IPs

[7] Dwi Santoso, Joko. (2017) Keamanan jaringan mengunakan IDS/IPS Straguard sebagai layanan keamanan jaringan terpusat. Sain dan Teknologi Informasi. 3(2)
[8] Putri L. 2011. "Implementasi Intrusion Detection System (IDS) Menggunakan Snort Pada Jaringan Wireless". Jakarta: Universitas Islam Negeri Syarif Hidayatullah.
[9] Dietrich, Noah. (2017). Snort 2.9.9.x on Ubuntu 14 and 16 https://www.snort.org/documents (diakses pada 15 maret 2019)
[10] Spitzner, Lance. (2003). Honeypot: Tracking Hackers.Addison-Wesley
[11] Efvy Zam, Efvy (2011). Buku Sakti Hacker. Jakarta: MediaKita.
[12] Masyarakat Digital Gotong Royong.(2003-2008) Pengantar Sistem Operasi Komputer https://rms46.vlsm.org/2/213.pdf (diakses pada 3 maret 2019)
[13] Wahono, Romi Satria. (2003). Cepat Mahir linux.Ilmu Kompuer.com
[14] Wahana Komputer. (2010). Belajar Hacking dari NOL.Semarang : ANDI

Gambar 2. Topologi Sistem IDS dan IPs