QUERY: Jurnal Sistem Informasi Volume: 01, Number: 02, October 2017 ISSN 2579-5341 (online)

Pemanfaatan *Telegram* Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan

Jefree Fahana[1], Rusydi Umar[2], Faizin Ridho[3]
Magister Teknik Informatika
Universitas Ahmad Dahlan Yogyakarta, Indonesia
[1]jefree.fahana@tif.uad.ac.id, [2]rusydi.umar@tif.uad.ac.id, [3]faizin1607048009@webmail.uad.ac.id

Abstract

Cyber attacks are a serious threat to network security, especially in routers that result in termination of connections, missing configurations that affect all communications and transactions between networks become impeded by the loss of many parties. The first step to do is to design and build an attack detection system that is Intrusion Detection System (IDS). The use of snort is useful for recording Distributed Danial of Services (DDoS) attacks as well as traffic data stored on the router stored in the log and forwarded to the instant messaging telegram application as a notification to alert the administrator. A telegram can be used not only as a notification but can also be used as a network forensic stage to strengthen evidence of an attack as a process of data collection for the purposes of the trial. The results showed that by utilizing Instant Messaging Telegram by designing wake Application (App) notification using PHP programming language able to detect attacks by using existing rules on snort and can serve as the basis of evidence of an attack.

Keywords: *Telegram, Intrusion Detection System (IDS), Snort, Network Forensics, DDoS.*

1. PENDAHULUAN

Perkembangan teknologi yang telah terbuka bebas, menjadikan *hacker* telah berevolusi dengan mampu menguasai teknik menurunkan kinerja perangkat jaringan anda dengan membanjiri lalu lintas jaringan. Terlepas dari upgrade perangkat keras yang telah anda lakukan untuk meningkatkan kinerja *server* Anda, peretas masih dapat mensimulasikan lebih banyak pengguna dari pada yang dapat ditangani oleh *server*.

Data IDSIRTI yang dikutip Aidil menyatakan jumlah total serangan kedalam jaringan 135,6 juta serangan (2016) kenaikan 50% dibandingkan dengan 2015. Port 53, DNS yang paling banyak mendapatkan serangan dengan sumber serangan majoritas dari AS, China dll. jenis serangan yang berbahaya DDOS dan Serangan paling banyak terjadi bulan April 45.5 juta. Insiden yang paling banyak adalah dari *malware*[1].

Banyak tahapan yang di lakukan seorang pelaku kejahatan *cyber* untuk memuluskan langkahnya mendapatkan informasi sebanyak mungkin pada target salah satunya adalah *DDoS*. Untuk memuluskan langkahnya biasanya seorang pelaku kejahatan *cyber* yaitu dengan menggunakan metode untuk membanjiri *source* pada perangkat jaringan.

Dalam rangka mengurangi ancaman keamanan pada jaringan, administrator harus menggunakan berbagai strategi keamanan yang jitu dengan memanfaatkan *Intrusion Detection System (IDS)* untuk melakukan audit sistem secara berkala dengan mengelola *log*. Umumnya pada setiap sistem memiliki log untuk mencatat peristiwa pada setiap perangkat. Data log mengambil peran penting dalam mengungkap suatu tindak kriminal yang terjadi di dunia *cyber*. Untuk itu perlu adanya *system* yang dapat memberi informasi kepada administrator apabila terjadi serangan yaitu dengan merancang system notifikasi dengan memanfaatkan aplikasi *instan messenger telegram* sebagai tindakan pencegahan sekaligus berguna untuk keperluan forensik terhadap jaringan dalam pengumpulan data.

Telegram adalah layanan pesan populer yang berbasis pada *platform open-source* yang dibangun oleh Rusia Pavel Durov pada tahun 2013[2][4].Telegram merupakan aplikasi *cloud based* dan sistem enkripsi yang menyediakan *enkripsi end-to-end, self destruction messages*, dan infrastruktur *multi-data center*. Kemuadahan akses yang diberikan telegram yang dapat berjalan di hampir semua platform memberikan kemudahan bagi administrator untuk membangun system notifikasi dengan

memanfaatkan fasilitas *open Aplication Programing Interface (API)* yang disediakan oleh *telegram* melalui *bot* yang dapat digunakan untuk mengirimkan pesan secara otomatis. *Cloud base* pada *telegram* memungkinkan proses pengiriman jauh lebih cepat serta media penyimpanan yang besar.

Di era teknologi informasi saat ini, Administrator dirasa perlu melakukan tindak antisipasi dengan dengan merancang bangun sistem untuk audit data yang sewaktu-waktu dapat dipergunakan apabila terjadi serangan yang dapat merugikan.Pada sistem keamanan jaringan peneliti memanfaatkan*Intrusion Detection System (IDS)*yang di rancang untuk mencatat segala kejadian yang ada pada sistem.Forensik jeringan dirasa perlu dilakukan dengan tujuan membantu administrator jaringan untuk mempermudah dalam menemukan serangan yang biasanya di lakukan secara manual. Desain dan implementasi forensik *log* perlu dilakukan dengan tujuan untuk menemukan bukti berdasarkan sumber serangan, waktu kejadian, serta dampak dari serangan pada perangkat jaringan.

2. LANDASAN TEORI

2.1 Kajian Peneliti Terdahulu

P.N.V.S.N. Murthy[3]dengan judul *Home Automation using Telegram*, yaitu memanfaatkan telegram sebagai pengendali sistem yang di bangun berdasarkan *Internet of Think(IoT)* untuk memberikan informasi tentang suhu dan kelembapan pada rumah.

Tole Sutikno, dkk[4] pada penelitian yang berjudul *WhatsApp, Viber and Telegram: which is the Best for Instant Messaging?,*menjelaskan bahwa *WhatsApp* adalah yang paling populer di kalangan pengguna smartphone dunia dengan sekitar 60% diikuti oleh dan, di tempat ketiga, *Telegram*. *Viber* adalah utusan yang paling fungsional, namun jika dilihat dari sudut pandang keamanan komunikasi, lebih bijaksana memilih *telegram*. *Telegram* menawarkan kemampuan sinkronisasi, layanan super cepat, *backup* handal dan fitur keamanan yang lebih baik.

Penelitian dengan pemanfaatan notifikasi juga pernah dilakukan oleh Sahid Aris Budiman dkk,[5] dengan memanfaatkan *Intrusion Detection System(IDS)* menggunakan jejaring sosial sebagai media notifikasi serangan terhadap keamanan *webserver* yang menjadikan sosisal media untuk mengirimkan informasi serangan.

Fadhila Nisya Tanjung dan Muhammad Irwan Padli Nasution juga pernah melakukan penelitian[6] dengan judul *Implementasi Pemrograman Java Untuk Alert Intrusion Detection System,*yaitu dengan membangun sistem notifikasi serangan menggunakan bahasa pemrograman java dengan memanfaatkan sms gateway untuk mengirimkan informasi apabila ditemukan serangan.

Imam Riadi pernah meneliti [7] dengan judul *Network Forensics For Detecting Flooding Attack On Web Server* yaitu melakukan Analisa forensik yang terjadi pada web server universitas muhammadiyah magelang yang sebagian besar terejadi serangan flooding.

Vedang Ratan Vatsa dan Gopal Singh telah melakukan penelitian[8] dengan topik *Raspberry Pi based Implementation of Internet of Things using Mobile Messaging Application Telegram,* yaitu memanfaatkan *telegram*yang menggunakan *Cloud base* untuk merespon sebuah intruksi dan mengirimkan pesan balasan pada *Raspberry Pi* yang dikembangkan dengan bahasa pemrograman *phyton* pada otomasi rumah.

S.T.Shenbagavalli telah melakukan penelitian dengan judul "*Router Interface Based Ip Traceback Method For DDoS Attack In Ipv6 Networks"*. Pada penelitian ini, penulis menggunakan metode *IP Traceback* untuk menemukan pelaku serangan DDoS yang mampu menyembunyikan identitasnya menggunakan teknik *Spoofing* pada perangkat router dengan IPv6[9].

2.2 *Intrusion Detection System (IDS)*

Intrusion Detection System atau disingkat IDS[10] 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).Terdapat dua jenis IDS, yaitu :

1. *Host-Based Intrusion Detection System (HIDS)*

Host-Based IDS memperoleh informasi dari data yang dihasilkan oleh system pada sebuah komputer yang diamati. Data Host-Based IDS biasanya berupa log yang dihasilkan dengan memonitor system file, event, dan keamanan pada Windows NT dan syslog pada lingkungan system operasi UNIX. Saat terjadi perubahan pada log tersebut, dilakukan analisis untuk mengetahui apakah sama dengan pola yang ada pada database IDS.

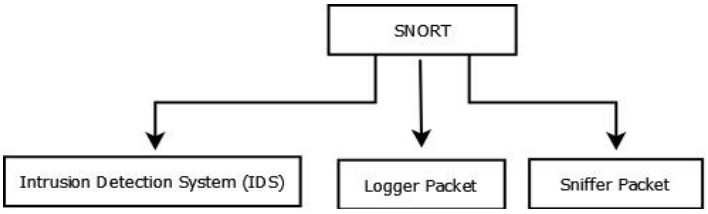
2. *Network-Based Intrusion Detection System (NIDS)*
   Network IDS menempati jaringan secara langsung dan melihat semua aliran yang melewati jaringan. Network-Based IDS merupakan strategi yang efektif untuk melihat traffic masuk / keluar maupun traffic diantara host ataupun diantara segmen jaringan lokal.

2.3 Snort

Snort adalah *software open source* yang berguna untuk mendeteksi intruksi pada sistem, mampu menganalisa lalu lintas data secara real-time pada IP Address[6][7]. Mampu mendeteksi serangan berdasarkan anomaly detection maupun misuse detection untuk menemukan segala ancaman serangan. Cara kerja Snort dibedakan berdasarkan berdasarkan Gambar 1. ada tiga mode paket Yaitu :

- Sniffer Packet
  Mode ini bertugas untuk memonitoring atau melihat lalu lintas data yang ada pada jaringan komputer.
- Logger Packet
  untuk mencatat semua paket yang lewat di jaringan untuk di Analisa untuk menemukan bukti dalam proses forensic jaringan.
- Intrusion Detection Mode

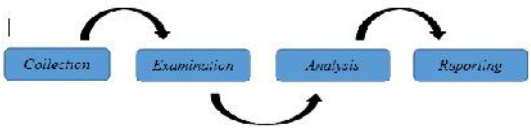
Pada mode ini snort akan berfungsi untuk mendeteksiserangan yang dilakukan melalui jaringan komputer. Untuk menggunakan mode IDS ini di perlukan setup dari berbagai rules / aturan yang akan membedakan sebuah paket normal dengan paket yang membawa serangan seperti yang di jelaskan pada gambar 2. berikut:



Gambar 1. Snort Mode

2.4 Network Forensics

Forensik jaringan (Network Forensics) adalah kegiatan untuk merekam dan menganalisa peristiwa yang terjadi dalam jaringan untuk menemukan sumber serangan dan peristiwa lainnya[11][12]. Dengan kata lain, tahapan forensik dilakukan dengan merekam dan menganalisa lalu lintas data yang tercatat pada *intrusion detection system*. Jaringan data berasal dari peralatan jaringan seperti *router, firewall, snort,* dilakukan proses analisa pada *log* untuk menemukan karakteristik serangan serta melacak pelaku serangan. Umumnya Network Forensics dilakukan berdasarkan empat tahap seperti Gambar 2.berikut :



Gambar 2. Metode Network Forensics

2.5 Ancaman Keamanan

Serangan terhadap kemanan sistem informasi dapat dilihat dari sudut peranan komputer yang fungsinya adalah sebagai penyedia informasi[6][13]. Ada beberapa kemungkinan serangan yaitu:

1. *Interruption*
   Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan pada ketersediaan dari sistem sehingga informasi dan data yang ada dalam sistem komputer dirusak dan dihapus, hal ini berdampak saat informasi dan data dibutuhkan maka data dan informasi tersebut tidak ada lagi. Contoh serangan adalah " Distributed Denial of Service Attack".

2. *Interception*
   Merupakan ancaman terhadap kerahsiaan. Pihak yang tidak berwenang berhasil mengakses aset dan informasi dimana informasi tersebut disimpan. Contoh dari serangan ini adalah penyadapan (wiretapping).
3. *Modification*
   Merupakan ancaman terhadap integritas. Pihak yang tidak berwenang tidak saja berhasil mengakses, tetapi dapat juga mengubah data. Contoh dari serangan ini adalah mengubah pesan dari website dengan pesan yang merugikan pemilik website
4. *Fabrication*
   Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil memalsukan suatu informasi yang ada sehingga orang lain yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh penerima pesan tersebut.

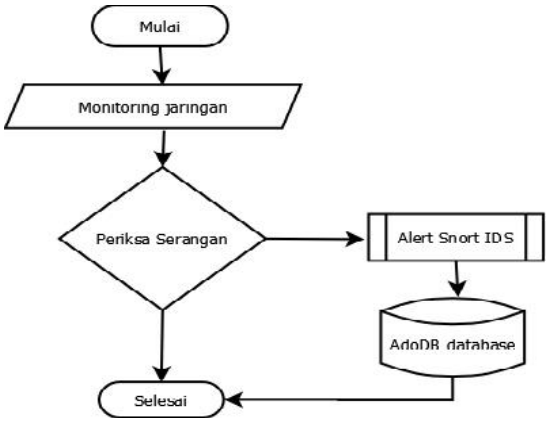
3. METODE PENELITIAN

Metode penelitian dilakukan dengan beberapa tahapan diantaranya :

3.1 Desain Sistem

a. Deteksi Serangan

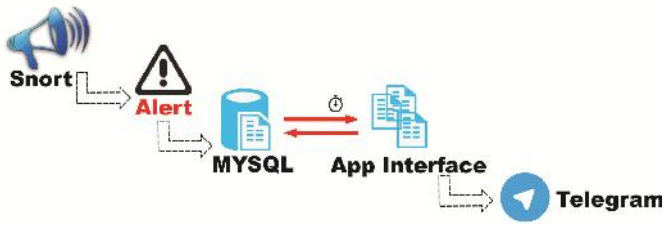
   Deteksi serangan di lakukan dengan memanfanfaatkan aplikasi *snort* pada *Intrusion Detection System* (IDS) yang dipasang pada router digunakan untuk memonitoring dan mendeteksi serangan yang terjadi pada router.Pemeriksaan serangan di lakukan dengan menentukan rule yang di set pada snort untuk menyatakan apakah sebuah paket data dianggap sebagai serangan atau bukan, selanjudnya akan di periksa dan di cocokkan dengan rule yang sudah di atur pada snort. Apabila ditemukan sebuah intrusi maka alert snort akan mengirimkan data menuju database yang telah disediakan seperti yang dipaparkan pada alur Gambar 3. berikut:



Gambar 3. Alur Deteksi Serangan

b. Desain App

Untuk dapat mengirimkan informasi serangan kepada aplikasi *instant messanging telegram*, perlu adanya sebuah aplikasi yang bertugas sebagai *triger* dengan memanfaatkan *API (Aplication Programming Interface)* yang memungkinkan software untuk dapat berkomunikasi dengan program lainnya. App dibangun menggunakan bahasa pemrograman *PHP* yang bertujuan untuk menghubungkan aplikasi *telegram* dengan *App* guna memeriksa informasi terbaru pada database yang tersedia lalu dikirimkan ke *telegram* sebagai notifikasi seperti yang tertera pada Gambar 4. Berikut :

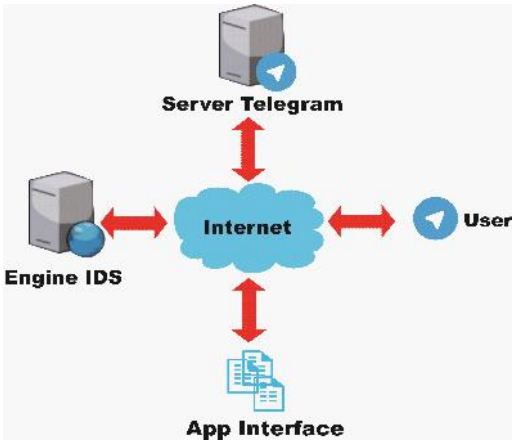


Gambar 4. Alur Pengiriman Informasi Serangan

Aplikasi*interface* dirancang khusus untuk mendapatkan informasi terbaru dari*database* melalui waktu yang ditetapkan setiap 1/10 detik untuk dapat bekerja secara *realtime*. Selanjudnya, apabila ditemukan data terbaru yang merupakan sebuah serangan maka *App*akan langsung mengirimkan informasi kepada telegram. Informasi yang dikirimkan kepada telegram berdasarkan jenis serangan *Sig_Name, IP Source, IP Destination and Timestamp.*

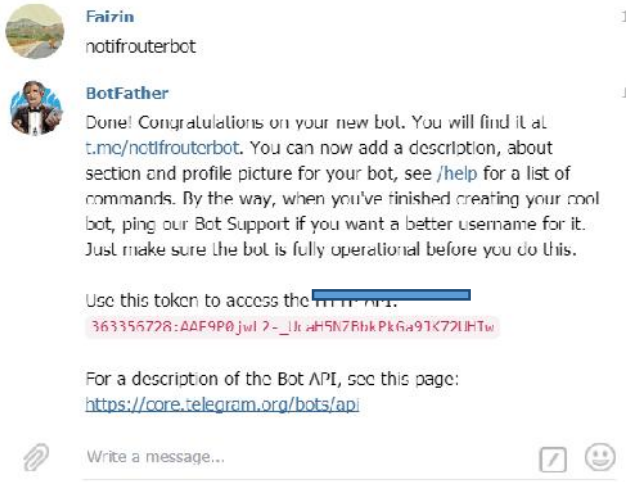
c. Desain *Bot Telegram*

Biasanya, untuk dapat menerima informasi, layaknya seperti aplikasi instant messanger seperti bbm, whatsapp,line, dll, telegram juga memiliki *bot* yang dapat digunakan untuk menjalankan perintah secara otomatis.*Bot* merupakan program yang berjalan disisi server dan untuk mendapatkan informasi dengan cara menggunakan *Telegram Client* yang telah terpasang pada perangkat mobile admin *serve*r. Penggunaan *Telegram Client* berfungsi sebagai antarmuka yang menampilkan informasi tertentu. Agar *bot* dapat bekerja dengan maksimal diperlukan akses internet yang baik untuk menghubungkan semua komponen sampai pada *server telegram*. Proses pengiriman dan penerimaan informasi menggunakan *telegram* dapat dilihat pada Gambar 5.



Gambar 5. Alur Pengiriman dan Penerimaan informasi

Dalam hal ini, peneliti memanfaatkan *"BotFather"* yang tersedia pada *telegram* untuk menciptakan bot sendiri yang dijadikan sebagai akun penerima informasi. Proses tersebut dapat dilihat pada Gambar 6. berikut:



Gambar 6. Pembuatan Akun *Bot* Notifikasi

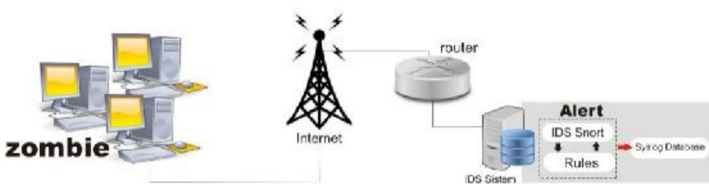
Jika *bot* telah berhasil dipasang, maka *bot*akan mengirimkan *token API* pada telegram. Token dimanfaatkan untuk menghubungkan *telegram* dengan *App Interface* untuk dapat menerima informasi apabila terjadi instruksi. *Token* akan dihubungkan menggunakan pemrograman PHP seperti pada gambar berikut :

```php
<?php
require_once('config.php');
require_once('functions.php');

$query = mysqli_query($conn, "SELECT sig_name, timestamp,
ip_src, inet_ntoa(ip_src) vip_src, ip_dst, inet_ntoa(ip_dst)
vip_dst, status FROM acid_event ORDER BY timestamp DESC");
$count = mysqli_num_rows($query);
$token = "bot363356728:AAF9P0jwL2-_U[redacted]72UHIw";
$chatid = "290192635";

if(!empty($count)) {
      while($row = mysqli_fetch_array($query, MYSQLI_ASSOC)) {
            if($row['status'] == 0) {
                  $content = "Notified " . $row['sig_name'] . "
from " . $row['vip_src'] . " to " . $row['vip_dst'] . " at " .
$row['timestamp'];
                  sendMessage($chatid, $content, $token);

                  $update = mysqli_query($conn, "UPDATE acid_event
SET status = '1' WHERE sig_name = '$row[sig_name]' AND timestamp
= '$row[timestamp]' AND ip_src = '$row[ip_src]' AND ip_dst
'$row[ip_dst]'");
            }
      }
}
```

Gambar 7. Code koneksi ke API Telegram

3.2 Simulasi Serangan

Simulasi serangan dilakukan berdasarkan skerion dengan mengirimkan paket *ICMPsyn flooding* guna menguji apakah konfigurasi *Intrusion Detection System (IDS)* pada *router* sudah berjalan sesuai dengan yang diharapkan. Simulasi serangan dilakukan dengan menggunakan *tools Nmap,hping3 dan loic* untu mengirim serangan *syn flooding* kepada router.



Gambar 8. Skenario Serangan Pada Router

Pada gambar 3. Dilakukan skenario dengan mengirimkan paket syn kepada router melalui komputer yang terhubung dengan internet dengan menggunakan alat hping3 dan nmap yang di analogikan sebagai zombie. Pengujian menggunakan skenario tersebut bertujuan untuk mengetahui *alert* pada IDS yang telah di pasang pada router.

3.3*Reporting*

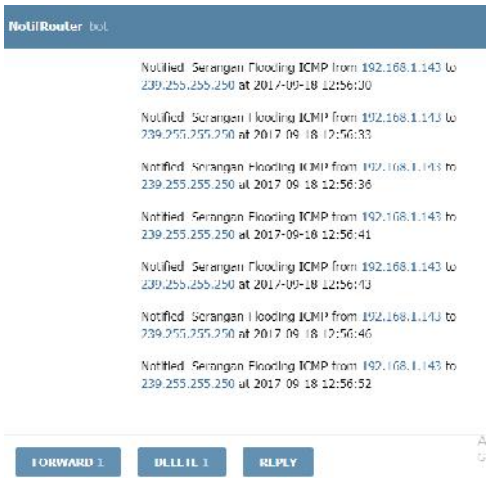
Reporting data dilakukan sebagai dasar untuk mengumpulakan data berupa informasi yang masuk pada aplikasi *instant messanging telegram* yang dapat digunakan sebagai data untuk memperkuat bukti yang dapat digunakan di persidangan.

4. HASIL PENELITIAN

4.1 Penerimaan Informasi

Berdasarkan perancangan sistem dan simulasi yang telah dibuat menunjukan bahwa *IDS* bekerja dengan baik. Serangan *syn flooding* yang dikirim routermampu di deteksi oleh *alert IDS* berdasarkan *anomaly* yang terdapat pada *rule alert*. *Rule* tersebut bekerja untuk menentukan apakah paket dianggap sebagai serangan atau bukan.*Alert* berfungsi dengan baik terbukti data serangan tersimpan di *database*. *App* dibangun dengan bahasa pemrograman PHP yang bekerja sangant baik menangkap serangan pada lalu lintas berdasarkan*rule* dan *alert* pada *IDS* yang kemudian di kirim ke*database snort*.*App Interface* yang bertugas untuk terus menerus memeriksa *database* dan memproses *alert snort* untuk dapat mengirimkan informasi serangan menggunakan *instant messanger telegram* secara *realtime*. Informasi yang akan diterima administrator dengan

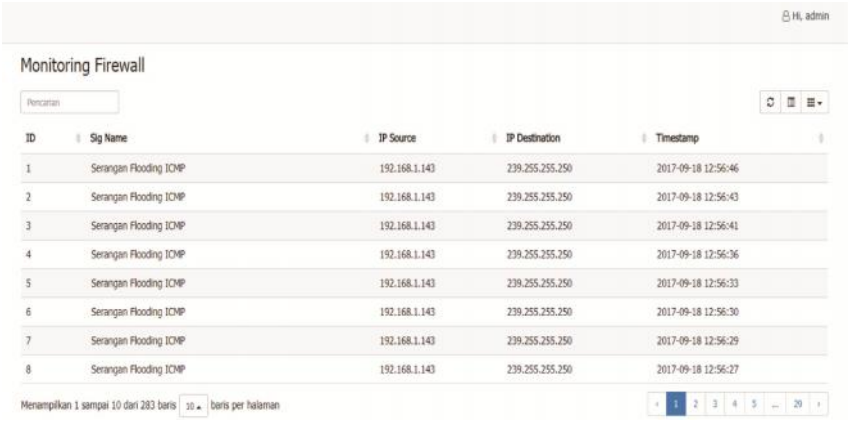
memanfaatkan telegram yaitu:*Sig_name, IP Source, IP Destination dan Timestamp*. Hasil notifikasi yang ditemukan dapat dilihat pada gambar 9. Berikut:



Gambar 9. Tampilan Notifikasi Serangan

4.2 Tahap Reporting Sebagai Keperluan Forensik

Tahapan ini merupakan bagian dari alur network forensics yaitu mengumpulkan semua informasi yang ada berdasarkan informasi yang tersimpan pada sistem. Pengumpulan data dapat dilakukan dengan melihat informasi yang berada pada app yang di bangun yang ditampikan pada Gambar 10.serta data yang ada pada notifikasi telegram seperti yang tertera pada Gambar 9. Yang selanjudnya data akan di jadikan sebagai dasar informasi yang akan dipergunakan dalam persidangan jika sewaktu-waktu diperlukan.



Gambar 10. Informasi Serangan pada App

Berdasarkan Gambar 10. Dapat di lihat informasi yaitu :*Sig_Name, IP_Source, IP_Destination, Timestamp*. Dalam hal ini, data yang disimpan oleh Aplikasi dan *database* yang akan digunakan sebagai informasi tambahan selain dengan asil analisa yang dilakukan pada tahapan forensik.

5. KESIMPULAN

Berdasarkan Analisa yang telah dilakukan menunjukkan bahwa IDS yang dirancang telah berhasil mendeteksi serangan dengan memanfaatkan Snort. Alert berkerja dengan sangat baik dan mampu

mengirimkan informasi ke database yang selanjutnya informasi diteruskan dengan menggunakan aplikasi *instant messenger telegram* secara *real time*. Hasil menunjukkan bahwa telah terjadi serangan ddos melalui ICMP berdasarkan analisa log yang dilakukan. Hasil dari rancang bangun sistem yang dilakukan dapat membantu administrator dan pihak terkait dalam mengumpulkan data dan menemukan bukti serangan untuk keperluan persidangan.

BAHAN REFERENSI

[1] ICION 2017. Teknologi Keamanan Fokus Konferensi Indonesia CIO Network di bali. Diakses 15 April 2017, dengan alamat https://komite.id/category/cyber/

[2] Mohammad Nizam Bin Ibrahim , Emilia Binti Norsaal, Mohd Hanapiah Bin Abdullah, Teaching and Learning Enhancement Based on Telegram Social Media Tool, *Jurnal Intelek*, 2016 Vol 11(1): 7-11, ISSN 2231-7716

[3] P.N.V.S.N. Murthy, S. Tejeswara Rao, G. Mohana Rao3, Home Automation using Telegram, *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, Vol. 6, Issue 6, June 2017, ISSN (Online) 2278-1021

[4] Tole Sutikno, Lina Handayani, Deris Stiawan, Munawar Agus Riyadi, Imam Much Ibnu Subroto, WhatsApp, Viber and Telegram: which is the Best for Instant Messaging?, *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 6, No. 3, June 2016, pp. 909~914, ISSN: 2088-8708, DOI: 10.11591/ijece.v6i3.10271

[5] Sahid Aris Budiman, Catur Iswahyudi, Muhammad Sholeh, 2014, Implementasi Intrusion Detection System (IDS) Menggunakan Jejaring Sosial Sebagai Media Notifikasi, Yogyakarta, 15 November 2014, ISSN: 1979-911X

[6] Fadhila Nisya Tanjung, Muhammad Irwan Padli Nasution, 2012, Implementasi Pemrograman Java Untuk Alert Intrusion Detection System, pematang siantar, 31 agustus – 2 september 2012, ISBN 978-602-18749-0-5, https://www.researchgate.net/publication/307973619 diakses 29 September 2016

[7] Imam Riadi, Muamalah, D.,2017, Network Forensics For Detecting Flooding Attack On Web Server, *International Journal of Computer Science and Information Security*, Vol.15, No. 2

[8] Vedang Ratan Vatsa., Gopal Singh., *2016*, Raspberry Pi based Implementation of Internet of Things using Mobile Messaging Application - 'Telegram'., *International Journal of Computer Applications (0975 – 8887).,Volume 145 – No.14*

[9] S.T.Shenbagavalli., 2016, Router Interface Based Ip Traceback Method For Ddos Attack In Ipv6 Networks, *Journal of Recent Research in Engineering and Technology*, ISSN (Online): 2349 – 2252, Volume 2 Issue 3

[10] I Wayan Bevin Waranugraha, Ary Mazharuddin S. , dan Baskoro Adi Pratomo (2012), *Aplikasi Forensik Jaringan Terdistribusi Menggunakan JADE*, Jurnal Teknik Pomits Vol. 1, No. 1, (2012) 1-6.

[11] Riadi imam, 2012, Log Analysis Techniques using Clustering in Network Forensics, *International Journal of Computer Science and Information Security (IJCSIS)* , Vol. 10, No.7

[12] Yogi Surya Nugroho, 2015, Investigasi Forensik Jaringan Dari serangan DDoS menggunakan metode Naïve Bayes, *skripsi*, Fakultas Sains dan Teknologi, UIN Sunan kalijaga, Yogyakarta.

[13] Ariyus Doni, 2006, Computer Security, Andi, Yogyakarta

[14] Valentina dan Mirjana, (2014). "Applcation of Forensic Analisys for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks". Latest Trends in Information Technology, ISBN : 978-1-61804-134-0

[15] Cartealy I. (2013). "Linux Networking", Jasakom, ISBN : 978-979-1090-73-5

[16] Nasution, Muhammad Irwan Padli, 2008, Urgensi Keamanan Pada Sistem Informasi, *Jurnal Iqra' Volume 02 Nomor 02*.