SATIN – Sains dan Teknologi Informasi

journal homepage : http://jurnal.stmik-amik-riau.ac.id

Monitoring pada *Server* STMIK Amik Riau dengan Menggunakan *Suricata* Melalui *Notifikasi Bot Telegram*

Asril Efrando
Teknik Informatika
asrilefrando@gmail.com

Herwin
Manajemen Informatika
herwin@sar.ac.id

Dwi Haryono
Sistem Informasi
dwiharyono@sar.ac.id

Abstract

The act of cybercrime (cybercrime) is currently developing rapidly in accordance with the development of information technology, some models of cybercrime actions are also based on these developments. One form of cyber crime is caused such as attacks on server systems on agencies or companies that can damage confidentiality, authenticity and availability of information. It becomes a demand for network administrators to monitor the network conditions they manage in realtime as well as at STMIK Amik Riau, a college which has several servers that are managed to support academic needs. Therefore we need a network security method that can detect, monitor, and identify activities on a host or network, one of them using Suricata. Suricata is an Intrusion Detection and Prevention System (IDPS) that able to detect a network activity and identify threats based on integrated rules. Rules in suricata play a role in identifying attacks that occur on a host. So that alerts on the network can be monitored in realtime. a link is needed between suricata notification to the network administrator, one of which uses a Telegram bot which acts to automatically send notifications when an attack occurs on the server, with the botTelegram it is expected that it will facilitate network administrators to monitor attack activities from anywhere without having to open the suricata log network administrators can take precautions earlier.

Keyword: Cybercrime, Intrusion Detection and Prevention System,Suricata,Telegram

Abstrak

Tindakan kejahatan dunia maya (cybercrime)saat ini berkembang cepatsesuai dengan perkembangan teknologi informasi, beberapa model tindakan cybercrime didasari juga oleh perkembangan tersebut. Salah satu bentuk kejahatan cyber yang ditimbulkan seperti serangan pada sistem server pada instansi atau perusahaan yang dapat merusak kerahasiaan, keaslian dan ketersediaan informasi.Menjadi sebuah tuntutan bagi administrator jaringan untuk memantau kondisi jaringan yang dikelolanya secara realtime begitu juga pada STMIK Amik Riau, sebuah perguruan tinggi yang memiliki beberapa server yang dikelola untuk menunjang keperluan akademik.Oleh karena itu dibutuhkan sebuah metode keamanan jaringan yang dapat melakukan pendeteksian, monitoring, dan mengidentifikasi aktifitas pada suatu host atau network salah satunya menggunakan Suricata.Suricata adalah Intrusion Detection and Prevention System (IDPS) yang mampu mendeteksi suatu aktifitas jaringan dan mengidentifikasi ancaman berdasarkan rules yang ter-integrasi. Rules pada suricata berperan dalam mengidentifikasi serangan yang terjadi pada sebuah host. Agar alert serangan pada jaringan dapat di monitoring secara realtime. diperlukan sebuah penghubung antara notifikasi suricata ke administrator jaringan, salah satunya memanfaatkan bot Telegram yang berperan secara otomatis mengirimkan notifikasi ketika terjadi serangan pada server, dengan adanya botTelegram tersebut diharapkan akan memudahkan administrator jaringan dalam memantau aktifitas serangan dari mana saja tanpa harus membuka log suricata, sehingga administrator jaringan dapat megambil tindakan pencegahan lebih dini.

Kata Kunci : Cybercrime, Intrusion Detection and Prevention System,Suricata,Telegram

1. Pendahuluan

Perkembangan teknologi di era global saat ini sangatlah pesat, terutama di bidang Teknologi Informasi (TI).Pengaksesan suatu informasi dari jaringan komputer sangat mudah dilakukan dimana saja, sehingga menimbulkan dampak baik positif maupun negatif.*Cybercrime* merupakan salah satu dampak negatif yang timbul dari hal ini.Salah satu tindakan *cyebercrime* yang umum terjadi pada server adalah pencurian/perusakan informasi dan penghapusan data, sehingga apabila hal ini tidak dapat diidentifikasi sejak dini akan menimbulkan kerusakan yang merugikan pihak yang menyediakan sumber layanan tersebut dalam hal ini kampus STMIK Amik Riau.

Oleh karena itu dalam penelitian ini akan dibuat system keamanan jaringan yang dapat meminimalisir tindakan *cybercrime* dengan melakukan pendeteksian, *monitoring*, dan mengidentifikasi aktifitas pada suatu *host* atau *network.*salah satu metode yang dapat diterapkan dalam hal ini adalah menggunakan *Suricata*. *Suricata* adalah *Intrusion Detection and Prevention System* (IDPS) yang mampu mendeteksi suatu aktifitas jaringan dan mengidentifikasi ancaman berdasarkan *rules* yang ter-integrasi. *Rules* pada *suricata* berperan dalam mengidentifikasi serangan yang terjadi pada sebuah *host*.Agar *alert* serangan pada jaringan dapat di monitoring secara *realtime*. diperlukan sebuah penghubung antara notifikasi *suricata* ke *administrator* jaringan, salah satunya memanfaatkan *bot Telegram* yang berperan secara otomatis mengirimkan notifikasi ketika terjadi serangan pada *server*, dengan adanya *botTelegram* tersebut diharapkan akan memudahkan *administrator* jaringan dalam memantau aktifitas serangan dari mana saja tanpa harus membuka *log suricata*, sehingga *administrator* jaringan dapat megambil tindakan pencegahan lebih dini.

Tujuan penelitian ini untuk mempermudah *administrator* jaringan dalam hal memonitoring dan melakukan pengecekan *log* pada *server* STMIK Amik Riau.Dengan adanya monitoring secara realtime *administrator* jaringan dapat mengambil tindakan preventif ketika terjadi serangan pada *server*.

2. Landasan Teori

2.1.Definisi Jaringan Komputer

Menurut Dede Sopandi (Instalasi dan konfigurasi jaringan komputer, 2008) Jaringan komputer merupakan gabungan antara teknologi komputer dan teknologi komunikasi. Gabungan teknologi ini melahirkan pengolahan data yang dapat didistribusikan, mencakup pemakaian *database, software* aplikasi, dan peralatan *hardware* secara bersamaan.

Untuk memudahkan pemahaman mengenai jaringan komputer, para ahli membagi jaringan komputer berdasarkan klasifikasi berdasarkan :

a. Berdasarkan area atau skala
b. Berdasarkan media pengantar
c. Berdasarkan fungsi

Namun ada juga yang meng-klasifikasikan jaringan komputer menjadi empat, yaitu:

a. Berdasarkan skala atau area
b. Berdasarkan media pengantar
c. Berdasarkan fungsi
d. Berdasarkan metode access control

2.2. Protokol Jaringan

Menurut Winarno Sugeng (Jaringan Komputer Dengan *TCP/IP*, 2010:60)[2] Protokol merupakan sebuah standar aturan komputer berkomunikasi dalam jaringan, dikarenakan sebuah komputer diproduksi oleh perusahaan yang berbeda maka diperlukanya sebuah protokol yang dapat digunakan secara umum sehingga komunikasi antar komputer berjalan dengan baik.

2.3 Definisi *Server*

Menurut Dede Sopandi, (2008) *server* adalah sebuah komputer yang berisi program baik sistem operasi maupun program aplikasi yang menyediakan pelayanan kepada komputer atau program lain yang sama atau pun berbeda. adapun jenis server yang paling banyak digunakan adalah *disk server, file server,* dan *terminal server.*

1. *Disk Server*
   Disk server digunakan untuk menyediakan fasilitas pengaksesan ke *harddisk*.*server* ini bersifat transparant terhadap *user*, sehingga setiap pengguna merasa sedang mengakses harddisk nya masing-masing.
2. *File Server*
   File server menyediakan pelayanan yang mirip dengan *disk server* tetapi juga mengelola disk lokal setiap komputer.*File server* bekerja berdasar *softwaredisk held* yang mengelola *file-file* yang disimpan dan memungkinkan beberapa atau seluruh data yang tersimpan untuk dimanfaatkan oleh sejumlah *user* yang berbeda.
3. *Terminal Server*
   Terminal server bertindak seperti sebuah *multiplexer* yang memungkinkan sejumlah komputer kecil, atau terminal-terminal yang lain, untuk mengakses ke sebuah titik LAN yang sama.

2.4 *Suricata*

Suricata merupakan *Network* IDS, IPS dan sebuah mesin monitor keamanan jaringan dengan peforma tinggi. Suricata adalah IDS *opensource* dan dimiliki oleh sebuah komunitas non-profit, yaitu *Open Information Security Foundation* (OISF).Suricata di kembangkan oleh OISF dan vendor pendukungnya. *Suricata engine* merupakan *open source nextgeneration intrusion detection and prevention engine*.*Suricata* merupakan *engine* yang memiliki kemampuan (Utomo, Sholeh, & Avorizona, 2017)[3]

2.5 Telegram

Telegram adalah aplikasi messaging dengan fokus pada kecepatan dan keamanan, yang super-cepat, sederhana dan gratis. Kita dapat menggunakan Telegram di semua perangkat pada waktu yang sama (sinkronisasi). Telegram dapat mengirim pesan, foto, video dan file jenis apapun (*doc, zip, mp3*, dll), serta membuat grup hingga 5000 orang.API telegram bersifat terbuka, dan memperbolehkan pengembang untuk membuat aplikasi telegram sendiri.Selain itu telegram memiliki *API Bot*, *platform* untuk pengembang yang memungkinkan siapapun mudah membangun alat khusus untuk telegram. (Sumber: telegram.org)

2.6 *Web Server*

Web server adalah sebuah perangkat lunak *server* yang berfungsi menerima permintaan *HTTP* atau *HTTPS* dari klien yang dikenal dengan *web browser* dan mengirimakan kembali hasilnya dalam bentuk halaman-halaman web yang umumnya berbentuk dokumen *HTML*. *Server web* yang terkenal diantaranya adalah *Apache* dan *Microsoft Internet Information Service* (ISS).*Web server* menunggu permintaan dari *client* yang menggunakan *browser seperti Internet Explorer, Mozilla Firefox, Opera, dan* program *browser* lainnya(Winarno Sugeng, 2010)

2.7 *Penetration Testing*

Berdasarkan definisi dalam modul CEH, *Penetration Testing* merupakan metode evaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya dan merupakan bagian dari *security audit*. Simulasi serangan yang dilakukan dibuat seperti kasus yang bisa dibuat oleh black hat hacker, cracker, dan sebagainya. Tujuannya adalah menentukan dan mengetahui macam – macam serangan yang mungkin dilakukan pada sistem beserta akibat yang bisa terjadi karena kelemahan sistem. Dalam melakukan penetration testing, diperlukan analisa intensif untuk setiap kerentanan yang diakibatkan oleh kelemahan sistem. Nantinya setelah seluruh analisa selesai dilakukan, akan didokumentasikan dan diberikan kepada pemilik beserta solusi dan dampak yang dapat diakibatkan dari celah keamanan yang ada. (Bhaskara,T,M., Kusyanti, Ari.,Yahya, Widhi ,2017).

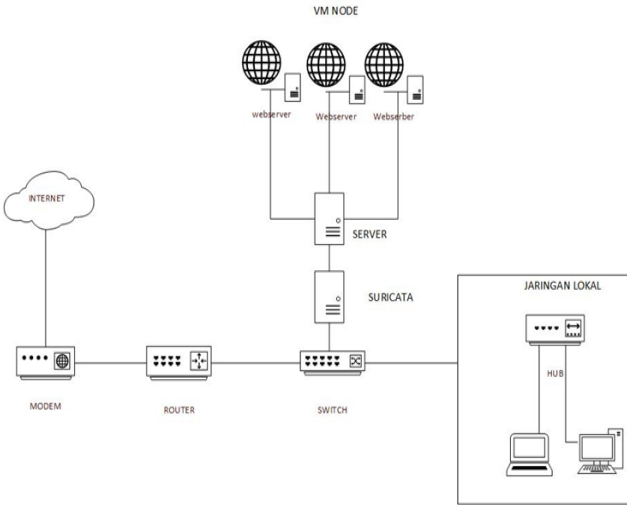
3. Analisa dan Perancangan Sitem

3.1 Analisa

Kampus STMIK Amik Riau memiliki beberapa *server* degan sistem keamanan berupa *firewall* yang digunakan untuk keperluan akademik diantaranya berupa *website* dan aplikasi-aplikasi internal yang menunjang kegiatan perkuliahan, *website* dan aplikasi-aplikasi tersebut diakses oleh berbagai *user* dengan keperluan dan tujuan masing-masing. Tentunya hal ini akan berdapak pada sisi keamanan *server*, semakin luas penggunaan aplikasi/*website* semakin besar ancaman pada sistem tersebut seperti *cybercrime*. Salah satu bentuk kejahatan *cyber* yang ditimbulkan seperti serangan pada sistem *server* di sebuah instansi seperti kampus STMIK Amik Riau yang dapat merusak kerahasiaan, keaslian dan ketersediaan informasi.Untuk itu dibutuhkan sebuah metode keamanan jaringan yang dapat meminimalisir tindakan *cybercrime* dengan melakukan pendeteksian, *monitoring*, dan mengidentifikasi aktifitas pada suatu *host* atau *network*.Salah satu metode yang dapat diterapkan dalam hal ini adalah menggunakan *Suricata.*

3.2 Perancangan

Untuk mencegah dan meminimalisir kemungkinan terjadi serangan terhadap *server* kampus STMIK Amik Riau, maka penulis merancang dan mencoba mengimplementasikan *suricata (IDS)* kedalam arsitektur jaringan *server* kampus STMIK Amik Riau seperti pada gambar dibawah ini:

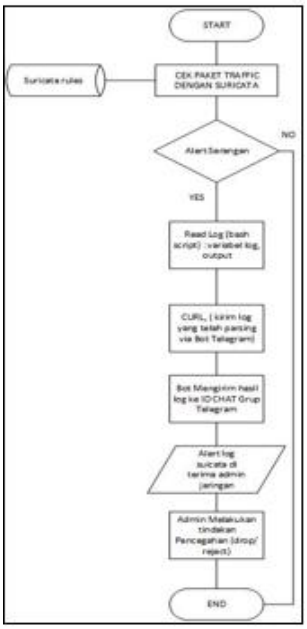


Gambar 1 Usulan Topologi *Server* Menggunakan *Suricata (IDS)*

Dengan menambahkan *serverlogsuricata* pada *server* yang ada, maka *administrator server* dapat memonitoring *log-log* yang teridentifikasi sebagai *traffic* serangan menuju *server*.

Namun hal ini masih terbatas dikarenakan administrator harus login ke *server* dan memeriksa *log* secara manual, maka dari itu penulis mencoba mengintegrasikan *logsuricata* tersebut menggunakan *bot telegram*, sehingga administrator dapat melihat aktivitas-aktivitas *log* secara otomatis dan *realtime*.

3.3 *Flowchart* Integrasi *Telegram* dan *Suricata*



Gambar 2. *Flowchat* Cara Kerja *Suricata (IDS)* dan *Bot*

Penjelasan pada gambar *flowchat* diatas adalah ketika ada *traffic/paket* menuju *server*, *suricara* terlebih dahulu akan melakukan pencocokan dengan rules yang tersedia, apa bila *traffic/packet* yang datang sesuai dengan *rules* milik *suricata* maka suricata akan menampilkan *log alert* pada *file fast.log* di *directory /var/log/suricata/fast.log* dan apabila tidak cocok maka suricata akan mengabaikanya.

Penulis merancang sebua bah *script/hell script* untuk mempermudah dalam melihat *log-log alert suricata*, pada *script* tersebut *log suricata* akan diproses dan dibaca setiap barisnya kemudian *log* tersebut akan dikirim melalui perantara bot telegram ke *administrator* jaringan. *Bot* telegram memiliki API dengan Token ID yang dapat digunakan untuk membuat bot sendiri dan mendukung banyak bahasa pemrograman.

Ketika *administrator* jaringan mendapat notifikasi dari *bot telegram suricata*, maka admin dapat dengan cepat merespon dan mengambil tindakan pencegahan sehingga tindakan *cybercrime* dapat diminimalisir dampaknya. Kelebihan dari integrasi notifikasi tersebut adalah admin jaringan dapat memantau *traffic*/paket berbahaya yang menuju *server* dari mana saja.

3.4 Kebutuhan Perangkat Keras

Berikut adalah spesifikasi perangkat keras komputer yang digunakan sebagai Pengujian *Prototype* :

Spesifikasi Komputer/Laptop (Host)

a. *Processor* :*Dual core* 1.8 *GHz*
b. *Memori (RAM)* : 4 *GB*
c. *Harddisk* : 320 *GB*
d. *Ethernet Controller* : *Intel NM10 dan D-link RTL8139*
e. *Monitor* : 14 *inc*

Spesifikasi *Node Suricata*

a. *Processor (Core)* : *1*
b. *Memori (RAM)* : 1.5 *GB*
c. *Harddisk* : 20 *GB*
d. *Ethernet Controller* : *NAT & Custom (Vmnet1)*

Spesifikasi *Node Kali Linux (Attacker)*

e. *Processor (Core)* : *1*
f. *Memori (RAM)* : 2 *GB*
g. *Harddisk* : 20 *GB*
h. *Ethernet Controller* : *NAT & Custom (Vmnet1)*

3.5 Kebutuhan Perangkat Lunak

Berikut adalah kebutuhan *software* dan paket aplikasi yang digunakan untuk mendukung Monitoring *Server* berbasis *Suricata* pada STMIK-AMIK Riau*:*

a. *Linux Ubuntu Server*
b. *Suricata*
c. *curl*
d. *bash*

Sedangkan *software* yang digunakan pada Komputer *Host* adalah sebagai berikut:

a. *Windows*10 *Pro* x64
b. *Vmware Workstation 14*
c. *Putty*
d. *Telegram Messaging*

3.6 Perancangan IP Address

Agar sebuah perangkat saling terkoneksi pada jaringan maka harus memiliki alamat khusus yang biasa di sebut *Internet Protokol(IP Address), ip address* tersebut akan di konfigurasi pada *server suricata* dan juga komputer *attacker* . Ada pun *ip address* untuk *server suricata adalah* sebagai berikut:

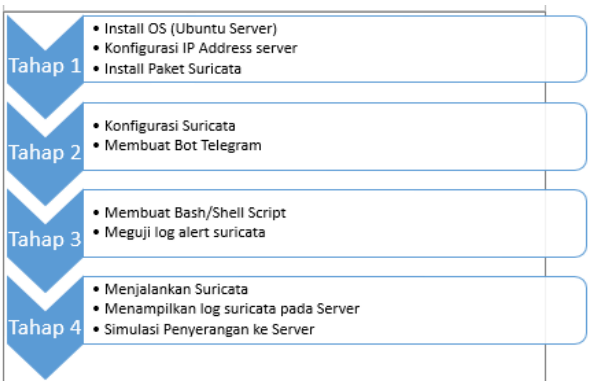
IP Address : *Server Suricata*
Ethet1 : DHCP
Ether2 : 192.168.1.1 /24
Gateway : -

Pada perancangan *ip addressserver* diatas penulis menggunakan 2 buah *Network Adapter* pada ether1 digunakan untuk menghubungkan *server* dengan internet dan ini diperlukan untuk mengirim *log* melalui *bot telegram* dan *Ether2* digunakan untuk menghubungkan dengan komputer (*attacker/tester*). Sedangkan *ip address* yang digunakan pada komputer *attacker* adalah:

IP Addreess : 192.168.1.2/24
SubnetMask : 255.255.255.0
Gateway : -

3.7 Alur Proses Perancangan Monitoring Berbasis Suricata

Untuk mempermudah proses perancangan diperlukan sebuah alur yang terstruktur dari tahapan-tahapan yang akan dilakukan. Sehingga proses perancangan dan implementasi lebih terarah, seperti pada gambar berikut:



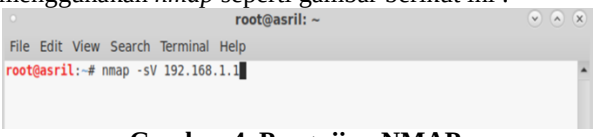
Gambar 3. Proses Perancangan *Suricata*

4. Implementasi dan Pengujian

Pada tahap implementasi dan pengujian, penulis akan menggunakan beberapa *tools penetration testing* diantaranya adalah tool nmap,nikto dan hydra. nmap berfungsi untuk melakukan *scanning port* pada *server* tujuan, sedangkan *nikto* berfungsi melakukan *scanning vulnerbility* pada *webserver* dan *hydra* digunakan untuk melakukan *bruteforce attack password* dalam penelitian ini penulis gunakan untuk *bruteforce attack password ssh*.

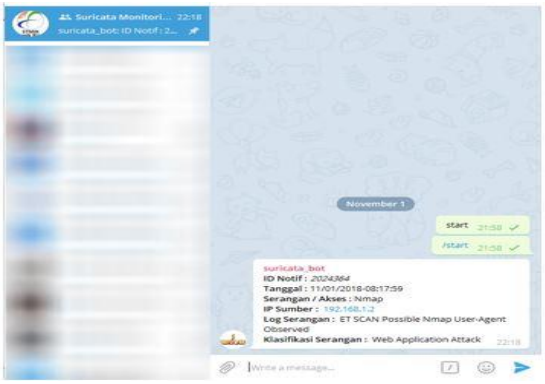
4.1 Pengujian NMAP

Penulis melakukan *scanning port server* menggunakan *nmap* seperti gambar berikut ini :



Gambar 4. Pengujian NMAP

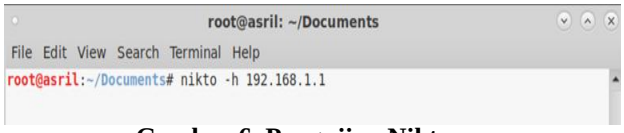
Saat proses *scanning nmap* berjalan, *log suricata* akan mendeteksi hal tersebu lalu akan disimpan pada file *fast.log*. Setelah berhasil tersimpan, kemudian notifikasi tersebut pun akan terkirim ke telegram dalam hal ini penulis mengirim log tersebut ke grup yang sudah penulis siapkan seperti pada gambar.5



Gambar 5. *Log Suricata Nmap* ke *Telegram*

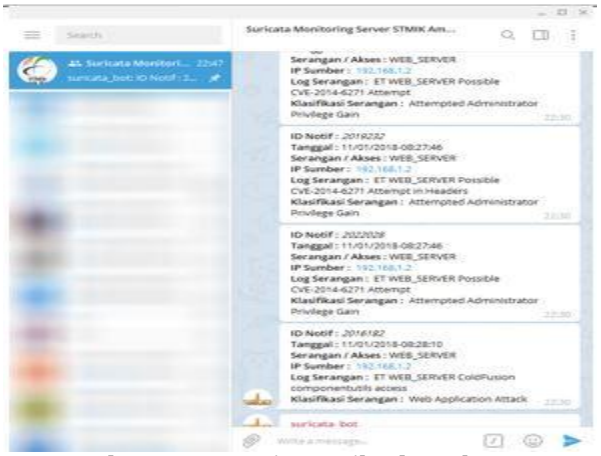
4.2 Pengujian Nikto

Penulis melakukan akan melakukan *scanning webserver* menggunakan *tools* nikto seperti gambar berikut ini :



Gambar 6. Pengujian Nikto

Seperti halnya pada pengujian *nmap*, serangan yang berhasil dideteksi melalui proses scanning *port server* menggunakan nikto akan dikirim ke notifikasi telegram seperti gambar. 7



Gambar 7. *Log Suricata Nikto* ke *Telegram*

4.3 Pengujian Hydra

Selanjutnya adalah pengujian penulis melakukan *bruteforce attack* untuk *service ssh* menggunakan *tool hydra*, dalam hal ini pengujian akan melibatkan
dictionary yang dapat di unduh pada *link* berikut: https://github.com/jeanphorn/wordlist/blob/master/ssh_*passwd.txt.* Selanjutnya membuka terminal kali *linux* dan ketik perintah seperti gambar dibawah ini :

Gambar 8. Pengujian *Bruteforce Hydra*

Penjelasan diatas adalah *root user* pada *server* target kemudian ssh_password.txt adalah *dictionary* dari *ssh password* yang telah di download pada link diatas, kemudian pada akhir perintah terdapat *ip server* target dan nama *service* yang akan di lakukan *bruteforce*. Sama halnya pada pengujian sebelumnya menggunakan *nmap* dan *nikto,log bash script brutoforce hydra* dikirm melalui *notifikasi* ke *telegram* seperti gambar. 9

Gambar 9. *Log Suricata Hydra* ke *Telegram*

Dari beberapa pengujian diatas, dapat dilihat bahwa konfigurasi *suricata* yang di buat berhasil mendeteksi *log* dari serangan *tools* penetst seperti *port scanning* dll. Kemudian *log-log* tersebut tidak hanya sekedar di deteksi akan tetapi juga berhasil di kirimkan secara otomatis ke grup *telegram* ketika terjadi serangan menuju *server*, hal ini tentunya sangat membantu dan memudahkan *administrator* jaringan dalam memonitoring aktivitas dan *log* pada *server*. Dari ketiga pengujian yang telah dilakukan, maka jika dimuat dalam *table*, akan seperti *table*. 1.

Tabel 1 Hasil Pengujian *Monitoring* Berbasis *Suricata* dan *Telegram*

No	Jenis Pengujian	Tools	Log pada Suricata (Ya/Tdk)	Log Bash Script (Ya/Tdk)	Tampil Notifikasi pada Grup Telegram (Ya/Tdk)
1	Scanning PORT	NMAP	(Ya), log berhasil tampil pada file fast.log	(Ya), log tampil pada bash script penulis	(Ya), Notifikasi berhasil dikirim dan tampil pada Grup Telegram
2	Scanning WebServer	NIKTO	(Ya), log berhasil tampil pada file fast.log	(Ya), log tampil pada bash script penulis	(Ya), Notifikasi berhasil dikirim dan tampil pada Grup Telegram
3	Bruteforce	HYDRA	(Ya), log berhasil tampil pada file fast.log	(Ya), log tampil pada bash script penulis	(Ya), Notifikasi berhasil dikirim dan tampil pada Grup Telegram

5. Simpulan

Sesuai dengan pembahasan yang telah diuraikan, maka kesimpulan yang dapat diambil adalah : dengan adanya *Monitoring Server* berbasis *Suricata* akan meminimalisir serangan dan ancaman dari *attacker* yang berpotensi merusak dan menggangu sistem dari *server*, pengujian *Monitoring Server* berbasis *Suricata* menggunakan *tool pentest* seperti *nmap, nikto dan hydra* telah berhasil dalam pengujian dengan mengirimkan notifikasi ke telegram sehingga administrator jaringan dapat mengambil tindakan pencegahan dini ketika mendapatkan laporan dari notifikasi *telegram*, selama berada dalam jangkauan internet.

Untuk kedepannya, sistem *monitoring* berbasis suricata ini dalam updaya pengembangannya dapat ditambahkan fitur *IPS (Intrusion Prevent System)*

sehingga *suricata* dapat langsung memblok aktifitas dari *traffic* yang berbahaya. *Log suricata* dibuatkan *server* sendiri dan dikombinasikan dengan perangkat *firewall* sehingga proses pengiriman *log telegram* tidak terganggu dengan adanya serangan pada *server*. Membangun *bot telegram* yang lebih interaktif sehingga *administrator* jaringan dapat membuat perintah-perintah khusus yang ingin di tampilkan pada *server*. Mengembangkan dengan bahasa pemrograman lain semisal *python* sehingga fitur pada *bot* dapat lebih bervariasi dan dapat dikembangkan lebih jauh.

6. Referensi

Utomo, D., Sholeh, M., & Avorizano, A. (2017). Membangun Sistem Mobile Monitoring Keamanan Web Aplikasi Menggunakan Suricata dan Bot Telegram Channel. Teknoka, 2.

https://telegram.org/

Gunawan,N,L., Anjarwirawan, Justinus., Handojo,Andreas. (2018). Aplikasi Bot Telegram Untuk Media Informasi Perkuliahan Program Studi Informatika-Sistem Informasi Bisnis Universitas Kristen Petra. Jurnal Infra,6(1).

Khairil, Kalsum, U,T.(2014). Implementasi Intrusion Detection System Sebagai Keamanan Web Server Universitas Dehasen Bengkulu. Jurnal Pseudocode,1(2),155-169.

Bhaskara,T,M., Kusyanti, Ari.,Yahya, Widhi (2017). Analisa Perbandingan Penetration Testing Tool Untuk Aplikasi Web. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 1(3), 206–214.

Sopandi, Dede. (2008). *Installasi Dan Konfigurasi Jaringan Komputer*, Informatika, Bandung

Sugeng, Winarno. (2010). *Installasi Dan Konfigurasi Jaringan Komputer* Dengan *TCP/IP*, Modula, Bandung

Fahana,Jefree., Umar,Rusydi., Ridho,Faizin (2017). Pemanfaatan Telegram Sebagai Notifikasi Serangan untuk Keperluan Forensik Jaringan. Jurnal Sistem Informasi, 1(2).6-14.