PEMANFAATAN TELEGRAM DAN SMS SEBAGAI NOTIFIKASI SERANGAN UNTUK JARINGAN DI PT.SP2J MENGGUNAKAN TOOL INTRUSION DETECTION SISTEM

Dio Agung Alberiante[1], Fatoni[2]
Fakultas Ilmu Komputer, Universitas Bina Darma
Email: braynt12@gmail.com[1] , Fatoni@binadarma.ac.id [2]

ABSTRACT

The security of data from information is very important, especially on network connections that are connected to the internet. Computer network security in a company can be disrupted by attacks in the form of threats both from within and from outside the company network. The threat of these attacks is in the form of attacks that intend to damage computer networks or steal important data and information on the company through network traffic. It will be a must for network administrators to monitor and carry out security continuously in data traffic on the network. Monitoring internet network traffic is also a necessity and must run in real time. In this study, we will discuss the use of telegram and sms as a medium for notification of attacks on computer networks. The object of this research is the computer network of PT. Palembang Jaya Development Facility (SP2J) using the Intrusion Detection System (IDS) Tool. The method used in this study is the Action Research method which includes diagnosing, action planning, action taking, evaluating and reflection. The results of this study are notification reports of computer network threats or attacks that are conveyed via telegram and sms applications. The notification process where the computer network will be monitored with the Suricata application. Notifications (Alerts) of the dangers of incoming threats will be sent in the form of short messages as information from the data obtained stating a threat or attack. This information will be sent to the Telegram and SMS applications that are already installed on the Smartphone.

Keywords: *Telegram, SMS, Notifications, IDS, Suricata*

ABSTRAK

Keamanan data dari suatu informasi memang sangat penting, terlebih pada koneksi jaringan yang terhubung ke internet. Keamanan jaringan komputer dalam suatu perusahaan dapat terganggu dengan adanya serangan dalam bentuk ancaman baik dari dalam maupun dari luar jaringan perusahaan. Ancaman dari serangan tersebut berupa serangan yang bermaksud merusak jaringan komputer maupun mencuri data dan informasi penting pada perusahaan melalui lalu lintas jaringan. Akan menjadi suatu keharusan bagi administrator jaringan untuk memonitoring dan melakukan keamanan secara terus menerus dalam lalu lintas data di dalam jaringan. Monitoring lalu lintas jaringan internetpun menjadi kebutuhan dan harus berjalan secara *realtime*. Dalam penelitian ini akan membahas pemanfaatan *telegram* dan *sms* sebagai media untuk notifikasi serangan pada jaringan komputer. Objek penelitian ini adalah jaringan komputer PT. Sarana Pembangunan Palembang Jaya (SP2J) dengan menggunakan *Tool Intrusion Detection Sistem (IDS).* Metode yang di gunakan pada penelitian ini yaitu metode *Action Research* yang meliputi *diagnosing, action planing, action taking, evaluating* dan *reflection.* Hasil dari penelitian ini adalah laporan notifikasi terhadapa ancaman atau serangan jaringankomputer yang di sampaikam melalui aplikasi telegram dan sms. Proses notifikasi dimanajaringan komputer akan dipantau dengan aplikasi *Suricata*. Notifikasi (*Alert*) bahaya dari ancaman yang masuk akan dikirimkan berupa pesan singkat sebagai

informasi dari data yang di dapat yang menyatakan adanya ancaman atau serangan. Informasi ini akan di kirimkan pada aplikasi *telegram* dan *sms* yang sudah terpasang pada *Smarthphone.*

Kata Kunci*:* Telegram, SMS, Notifikasi, IDS, Suricata

1. PENDAHULUAN

Keamanan suatu informasi atau data menjadi suatu hal yang sangat penting. keamanan data dari teknologi dan bahaya ancaman informasi pada server sangat beragam mulai dari ancaman serangan *Brute Force, Denial Of Service (DOS) dan Port scanning*. Ancaman tersebut dapat menyebabkan *server* mati dan tidak dapat berfungsi lagi seperti biasanya sehingga tidak dapat memberikan layanan pada pengguna yang mengakses ke *server* tersebut. Serangan dan ancaman yang menyerang *server* dapat di hindari dengan mengidentifikasi celah keamanan semaksimal mungkin.

Salah satu contoh kasus serangan jaringan komputer pada tanggal 16 sampai 17 mei 2008, Serangan *DDoS* yang terjadi adalah serangan yang dilakukan oleh *Yogyafree* terhadap *website* Kaskus di tahun 2008. Serangan yang dilakukan oleh *Yogyafree* ini membuat situs KasKus tidakbisa di akses dan juga *corrupt*. Penyerangan ini bisa menyebabkan *malware* yang telah dibuat harusdi *secure* oleh pihak administrator dari forum KasKus. Dengan kejadian ini yang berlangsung cukuplama maka pihak administrator KasKus dengan berat hati menonaktifkan *server* (Tony Firman 2016).

Contoh kasus lain serangan jaringan komputer pada februari 2000, dari serangan ancaman yang lumayan besar yang dilakukan sampai beberapa situs yang terkenal seperti *Amazon, CNN, eBay, dan Yahoo!* mengalami "*downtime*" selama beberapa waktu. Ancaman serangan yang terbarulagi pernah di lancarkan pada Oktober 2002, ketika 9 dari 13 *root DNS Server* diserang para *hacker*dengan motif penyerangan *DDoS* yang besar disebut *"Ping Flood"*. Pada saat puncak dari serangan.Dari beberapa *server* yang terkena serangan pada tiap detiknya terdapat lebih dari 150.000 *request* paket *Internet Control Message Protocol* (*ICMP*). Akibat yang di timbulkan dari serangan *DDoS* tersebut mengakibatkan sistem yang di serang mengalami gangguan *down* karena *banwitdh* yang digunakan oleh korban akan habis lalu mengakibatkan terputusnya koneksi antar *server*, dan menghabiskan sumber data sistem tersebut sehingga tidak dapat diakses lagi. Jika serangan *DDoS* tidak ditanggulangi maka akan dapat menyebabkan kerusakan permanen pada *hardware* dan *software* korban (Tony Firman 2016).

Mengingat meningkatnya bahaya yang di timbulkan dari serangan jaringan seperti contoh kasus di atas, maka harus dilakukan langkah – langkah pencegahan, pengamanan dan perlindunganpada suatu sistem jaringan komputer dengan. Ini bisa dilakukan dengan membuat suatu sistem keamanan yang dapat menangkal serangan dan usaha penyusupan baik dari *external* maupun *internal* pada jaringan komputer.

Salah satu cara yang dapat digunakan untuk mengatasi hal tersebut adalah dengan memanfaatkan *Telegram* (Hadil Deekshith 2018) dan *SMS* (Maribondang, Wowor, and Karouw 2015) guna untuk mendaptkan notifikasi dari serangan pada jaringan forensik menggunakan *IDS*(Region 2016). Menurut (Ariyanto and Harijanto 2017) *Suricata* merupakan *tools IDS* yang dapat mendeteksi ancaman serangan pada jaringan yang di bantu dengan *rules* yang telah di buat. Cara kerja *suricata* yaitu ketika terjadinya ancaman penyerangan *suricata* akan otomatis melakukan*scanning packets* serangan yang masuk melalui *rules* yang di buat. Ketika serangan itu terdeteksi maka *suricata* akan langsung membuat *log* saat serangan yang di lakukan, *Suricata* juga dapat melakukan pendeteksian otomatis pada layer 7 yaitu aplikasi seperti *ftp, smtp, dns, http dan imap,* sehingga *suricata* akan memberikan solusi untuk meningkatkan keamanan pada *Server*.

Penelitian ini akan membahas pemanfaatan *telegram* dan *sms* sebagai media untuk notifikasi

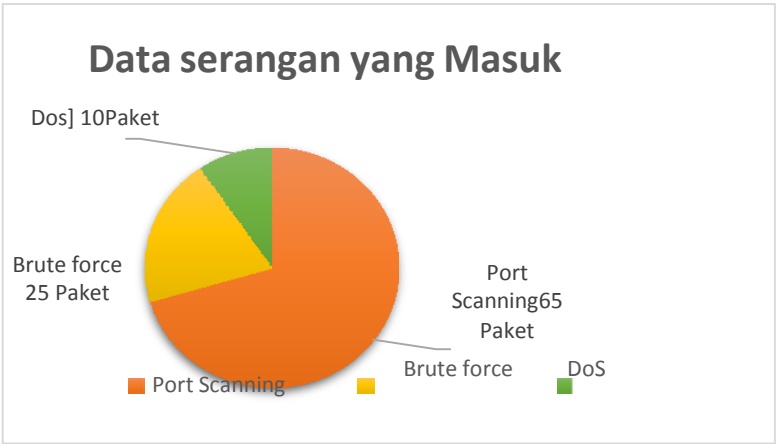
serangan pada jaringan komputer. Objek penelitian adalah jaringan komputer PT. Sarana Pembangunan Palembang Jaya (SP2J).

Metode yang di gunakan pada penelitian ini yaitu Metode *Action Research* Menurut (Davison, Martinsons, and Kock 2017), menyebutkan penelitian tindakan (*Action Research*) sebagai metode penelitian, didirikan atas asumsi bahwa teori dan praktek dapat secara tertutup diintegrasikandengan pembelajaran dari hasil intervensi yang direncanakan setelah mendiagnosis permasalahan yang rinci terhadap konteks masalahnya. Adapun beberapa tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu *diagnosing, action planing, action taking, evaluatting* dan *reflection*.

2. METODOLOGI PENELITIAN

Pada tahap pertama *diagnosis* ini peneliti mengidentifikasi permasalahan mengenai berbagaimacam serangan terhadap jaringan komputer seperti *port scanning*, *brute force* dan *denial of service*, identifikasi dari data yang di dapatkan, identifikasi perangkat keras sampai ke perangkat lunak yangada di PT. SP2J.

Dari data berbagai serangan yamg masuk ke *server* PT. SP2J, Peneliti mendapatkan hasil data yang akan di uji di penelitian ini yaitu *port scanning* yang masuk sebesar 65 paket , *brute force*yang masuk sebesar 25 paket, dan terakhir yaitu *denial of service* masuk sebesar 10 paket seperti pada gambar 1 berikut.



Gambar 1. Data Serangan Jaringan

Dari data yang didapatkan tersebut hasil yang tertinggi yaitu dari serangan *port scanning* karena banyaknya pendeteksian melalui *port scanning* dan di ikuti dengan serangan lain *brute force*dan *denial of service*. Permasalahan ini seringkali menimbulkan ketakutan karena terjadi ancaman bagi perusahaan terutama di PT. SP2J dikarenakan data yang ada didalam *server* tersebut adalah data penting dari perusahaan. Untuk itu perlu dilakukan penanganan untuk mencegah jika terjadi sesuatu yang tidak di inginkan seperti pencurian data ataupun kerusakan pada perangkat *server.*

Adapun identifikasi perangkat keras yang akan digunakan untuk penanganan pencegahan serangan terhadap jaringan adalah seperti pada tabel 1 berikut.

Tabel 1. Perangkat Keras

No	Perangkat	Spesifikasi	Fungsi	Jumlah
1	Server	*Intel Xeon processorE3-1200, 8 GB RAM,HDD (2TB) 2x1TB Bays 3.5" SATA*	Server suricata,dengan sistem operasi ubuntu 16.04 lts	1
2	Laptop Asus A456UR	*Intel Core I5, 12 GB RAM, 1TB HDD, 240 GB SSD, GPU Nvidia Gforce 930MX*	Laptop Penyerang	1
3	*Smartphone*	*Xiaomi Redmi 5+, RAM 3 GB,* Media penyimpanan 32GB	Untuk menerima notifikasi dari smsdan telegram	1
4	*Switch*	*D-link 16 Port10/100 Mbps*	Pembagian jaringan internet	1
5	*Modem*	*Huwaei E1550 USBStick, HSDPA / 3G*	Pengiriman pesansms via *gammu*	1
6	*Routerboard RB450x4*	*Routerboard RB450Gx4 (716MHz Quad Core CPU, 1GB DDR RAM, 512MB NAND* Storage) RouterOS (Level 5) ,5 (lima)buah port gigabit 10/100/1000, dan slot mikro-SD.	Pembagian dan pengaturan jaringan lokal	1

Adapun identifikasi perangkat lunak yang akan digunakan untuk penanganan pencegahan seranganterhadap jaringan adalah seperti pada tabel 2 berikut.

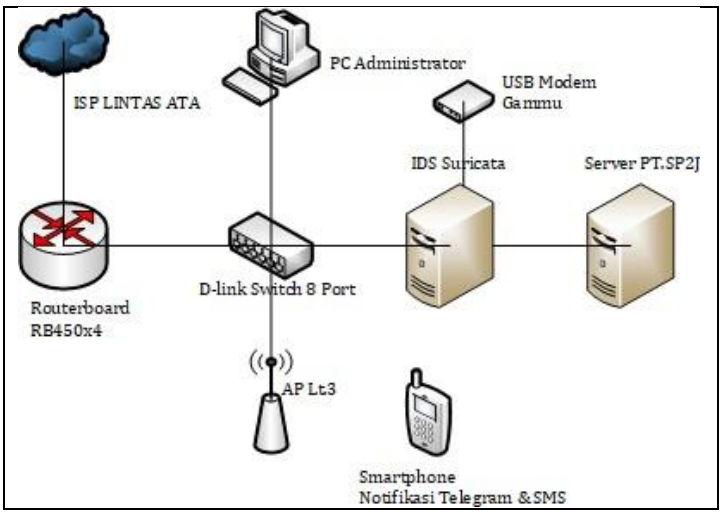
Tabel 2. Perangkat Lunak

No	Perangkat	Penjelasan
1	*Ubuntu 16.04 LTS*	Sistem operasi *server* di *suricata*
2	*Suricata*	*Software intrusion detection system (IDS).*
3	*Snorby*	*Software network security monitoring* antarmuka
4	*Barnyard2*	*Software open source interpreter* untuk suricata *unified2 binary output files*
5	*Kali Linux*	Sistem operasi penyerang
6	*API Telegram*	Mengirimkan *alert suricata* ke pesan telegram administrator
7	*SMS*	Sebuah layanan yang dilaksanakan dengan sebuah telepon genggam untukmengirim atau menerima pesan-pesan pendek
8	*Hydra*	*Software* yang digunakan untuk memasukan *password* secara berkala melalui *word list* yang telah di sediakan
9	*Nmap*	*Tools port scanning*
10	*SYN Flood*	Sebagai *software* serangan.

Dari hasil observasi di PT SP2J, peneliti merancang desain *logical* topologi *IDS suricata* beserta desain penyerangan yang akan di implementasikan untuk melakukan simulasi serangan jaringan nantinya. maka dari itu di dalam penelitian ini peneliti membuat desain topologi jaringan *IDS suricata* (Ardianto and Akbar 2017), dimana nantinya dalam desain tersebut di gunakan untuk mengatasi permasalahan dalam penelitian ini.

Gambar 2 berikut ini adalah desain topologi *logical* jaringan *Intrusin Detection system*

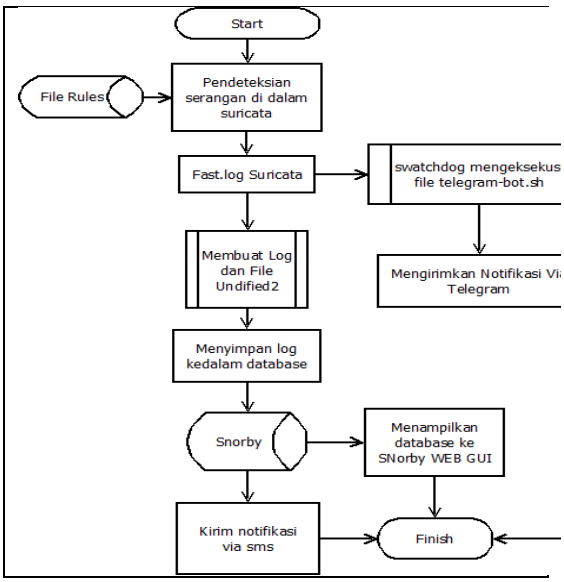
suricata untuk di implementasikan di PT. SP2J.



Gambar 2. Desain Tolologi *IDS*

Alur sistem *IDS Suricata* digunakan untuk melakukan pendeteksian jika terjadinya ancaman serangan ataupun aktivitas yang mencurigakan yang akan masuk ke *server* yang akan menghasilkan *log*, hasil tersebut akan tersimpan dalam bentuk *log* dan tersimpan di *fast.log* untuk menyimpan *log* tersebut membutuhkan *barnyard2* dan *snorby* (Akhyar 2019). Untuk menyimpan data notifikasi tersebut nantinya akan di simpan ke *database*. Data tersebut akan di integrasikan dengan *snorby* melalui *barnyard2* dengan membuat sensor yang akan di konfigurasi oleh peneliti. Sensor tersebut yang akan otomatis mengambil data di dalam *database* yang sudah terhubung dengan koneksi dari *barnyard2* yang nantinya akan di tampilkan pada *web interface snorby*. Selanjutnya *database* yang telah berisi aktivitas *event* atau notifikasi dari penyerangan yang terdapat pada *snorby* akandi ambil dan akan dikirimkan melalui sms dengan menggunakan *gammu*.

Sedangkan dari pendeteksian serangan didalam *IDS suricata* jika terjadi adanya serangan ataupun aktivitas mencurigakan, akan tersimpan ke *fast.log*, dari *fast.log* tersebut peneliti menambahkan *swatchdog* dan membuat *file telegram-bot.sh* untuk mengirimkan notifikasi ke *telegram*. Kemudian *swatchdog* akan mengambil data *log* dari hasil pendeteksian yang berhasil terekam di *IDS suricata* dan di ambil untuk dikirimkan melalui *telegram* secara *realtime*. Gambar 3berikut merupakan alur sistem alur sistem *IDS Suricata*.



Gambar 3. Alur Sistem.

Action Planning adalah serangkaian rencana kegiatan yang di isi dengan aktivitas yangtelah di siapkan oleh peneliti. Pada bagian tahapan ini peneliti melakukan pemahaman dengan *tools* dan bahan untuk penyerangan apa saja yang di butuhkan adalah

1) Melakukan persiapan *server* dengan sistem operasi *ubuntu 16.04 LTS, server* ini nantinya akan di *install software instrusion detection system* (*IDS*) *Suricata*, dan nantinya *server* ini akan melakukan tiga pengujian simulasi serangan *port scanning, bruteforce SSH, dan Denian of service* dari *tools* yang sudah di siapkan oleh peneliti.
2) Persiapan *software suricata* untuk *intrusion detection sistem* dan menyiapkan tiga *rules file suricata* untuk melakukan simulasi serangan dan target nantinya, yaitu *server IDS suricata* yang sudah di *install*.
3) *Rules file suricata* fungsinya untuk dipasangkan ke *software intrusion detection system suricata, fie rules* tersebut nantinya akan berfungsi sesuai dengan yang sudah dikonfigurasi dan dipasang untuk mendeteksi serangan ke *IDS Suricata*.
4) Peneliti menambahkan *hardware* laptop untuk nantinya melakukan simulasi penyerangan ke *server*. Laptop tersebut telah terinstall sistem operasi *Kali linux* dan menggunakan *tools* yang telah disediakan didalam laptop penyerang tersebut.
5) Peneiti menambahkan tiga *tools* serangan yang akan digunakan untuk menyerang ke target server *IDS suricata* yang telah di *install.*
6) *Software suricata* berfungsi untuk mendeteksi aktivitas jaringan lokal maupun luar yang masuk dan apa saja yang mencurigakan yang akan melewati *server* yang telah di sediakan oleh peneliti.

Pada teknik pengujian ini peneliti akan menguji sistem keamanan *server* yang telah dipasang *Intrusion Detection System* (*IDS*) *suricata* dengan skenario serangan yang telah di siapkan sebagai berikut ini :

1) *Port Scanning*
   Skenario pertama peneliti akan melakukan *port scanning* mengguanakan *tools* yang telah di siapkan yaitu *software nmap scan* untuk melihat *port* apa saja yang terbuka di*server IDS Suricata* yang telah di *install* (Hadi 2016).
2) *Brute Force*

Skenario kedua peneliti akan melakukan teknik penyerangan *brute force SSH attack* menggunakan tools *hydra* yang nantinya bertujuan untuk mencoba segala cara dan mengkombinasikan huruf dan karakter untuk mencari akses *login* yang melewati *loginSSH* yang berada di *server IDS suricata* (Pardosi 2015).

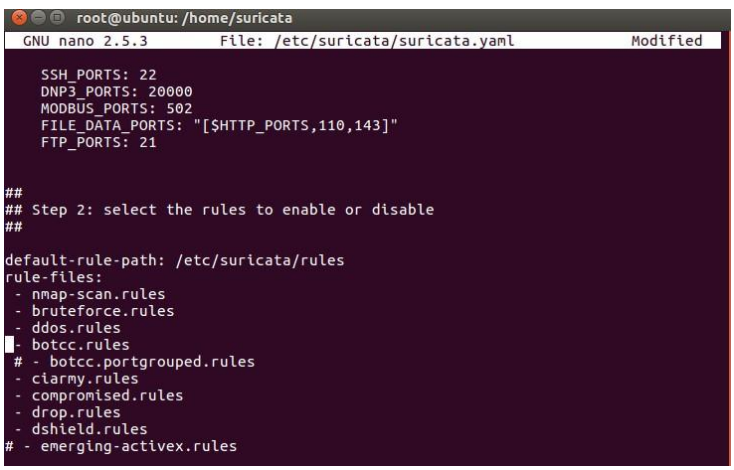
3) *Denial of Service*

Skenario ketiga melakukan teknik penyerangan dengan metode *Denial of Service* dengan *sofware SYN Flood* dimana serangan tersebut nantinya akan berfocus menyerang *IP address Server* IDS *Suricata* dan mengirimkan *packet – packet* yang berlebihan terhadap *server* IDS *suricata* (Nugraha 2016).

Berikut langkah–langkah tiga pengujian sistem serangan *Port scanning, brute forcedan denial of service* :

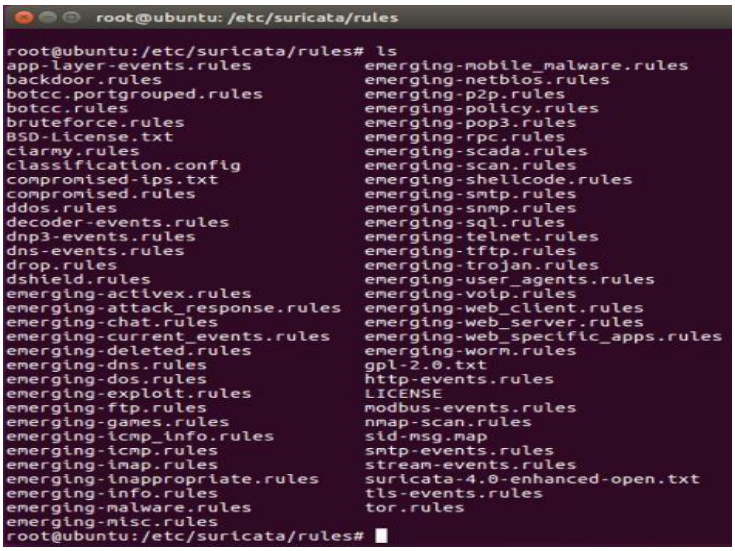
1) Langkah pertama yaitu menggunakan metode *port scanning* dengan *tools nmap scan*, didalam terminal *kali linux* ketik perintah *#nmap -sS -v -A 172.16.1.7*, setelah melakukan eksekusi penyerangan menggunakan metode *scanning port* maka akan terjadi scanning *port* pada *ip address* yang telah di targetkan yaitu *server IDS suricata*
2) Langkah kedua yaitu menggunakan metode *brute force* dengan *tools hydra*, didalam terminal *kali linux* ketik perintah *#hydra -l root -p /home/kali/Download/pass.txt 172.16.1.7 -t 4 ssh***.** Setelah melakukan penyerangan menggunakan metode *brute force*dan menargetkan pada *ip address* yang telah di targetkan yaitu pada *server IDS suricata*
3) Langkah ketiga yaitu menggunakan metode *denial of service* dengan tools *syn flood*, di dalam terminal *kali linux* ketik perintah *#sudo hping3 –flood -V -p 80 172.16.1.7* .
4) Setelah selesai melakukan pengujian sistem dengan tiga metode yang berbeda, *IDS suricata* nantinya akan mendeteksi aktivitas dari ketiga serangan yang mencurigakan tersebut melalui *#tail -f /var/log/suricata/fast.log.*
5) Dalam pengujian sistem ini untuk melakukan penyerangan maka di dalam monitoring *fast.log* akan memberikan pesan sesuai *rules* yang dibuat oleh penulis tadi.

3. HASIL DAN PEMBAHASAN



Gambar 4. File Konfigurasi suricata.yaml

Pada tahapan konfigurasi pengujian dimulai dengan melakukan konfigurasi *IDS Suricata* dan membuat *rules* untuk mengantisipasi dan mencegah serangan yang masuk melalui jaringan lokal ke *server* yang berada di penyimpanan direktori */etc/suricata/rules/*,lalu menambahkan list *rules* ke dalam konfigurasi di dalam *file suricata.yaml*, dapat di lihat pada gambar 5 berikut.



Gambar 5. List file rules serangan.

Pada gambar 6 peneliti melakukan konfigurasi *suricata* di dalam *suricata.yaml* dan melakukan kofigurasi *rules suricata* yang berada dalam direktori */etc/suricata/rules* dan terdapat list *rules files* tersebut ada tiga yaitu *bruteforce.rules, ddos.rules* dan *nmap-scan.rules.* Selanjutnya melakukan pembuatan *alert* di dalam *file rules bruteforce alert* ini akan berfocuske *Secure Shell (SSH)*, ketika terjadi aktivitas serangan yang mencurigakan dan memberikan pesanseperti *bruteforce ssh*. Alert tcp $EXTERNAL_NET any - > $HOME_NET 22 msg: "Possible : Telahterjadi serangan Bruteforce SSH"; fl$ Kemudian membuat *alert* di dalam *file rules denial of service*, *alert* ini akan memberikan peringatan jika terjadi serangan *alert* di *transmission control protocol (TCP)* dan *HypertextTransfer Protocol (HTTP)* , ketika terjadi aktivitas serangan yang mencurigakan dan memberikan pesan seperti telah terjadi serangan *DOS* seperti berikut.

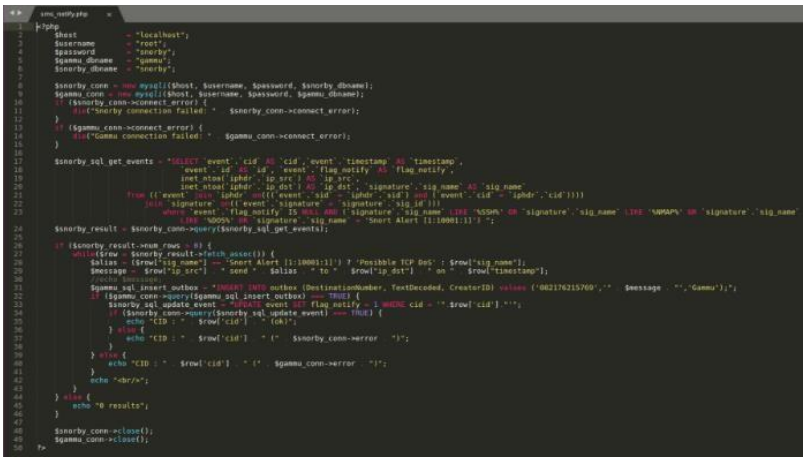
Alert tcp any any - > $HOME_NET 80 (flags: S; msg:"Possible : Telah terjadi serangan DOS"; flow :statels$

Selanjutnya membuat *alert* di dalam *file rules scanning port*, dalam *rules* tersebut akan menampilkan *alert Transmission control protocol (TCP)*, ketika terjadi aktivitas serangan yang mencurigakan dan akan memberikan peringatan pesan ke *log suricata* yang lokasinya di */var/log/suricata/fast.log.*

Alert icmp any any - > $HOME_NET any msg:"Possible : Telah terjadiserangan Nmap Scan"; $

Langkah selanjutnya melakukan konfigurasi *gammu* (Kermite, Winarno, and Rohmani 2017)untuk membuat *sms-gateway*, dari penginstalan *gammu* hingga simulasi pengiriman dan akan di integrasikan melalui *MySQL*. Setelah melakukan konfigurasi gammu langkah selanjutnya meng*import databasegammu* yang berada di *MySQL*, *database gammu* tersebut sudah ada di

dalam direktori */usr/share/doc/gammu/examples/sql*, kemudian di *import* ke *database* yang berada di *databasegammu* dan *import gammu* ke *database*.



Gambar 6. Sms notify.php

Pada bagian ini peneliti membuat *sms_notify.php* menggunakan bahasa pemrograman *php*,dan *sms gateway* ini akan terhubung ke penyimpanan *log* serangan dari *suricata* yang sudah masukke *database* secara *realtime*, gambar 7 berikut. Langkah selanjutnya men-*Trigger sms gateway* dan membuat penjadwalan setiap 10 detik dan akan mengirimkan notifikasi *alert* ke *administrator*, dan *crontab* ini akan mengeksekusi *file sms_notify.php* yang sudah di konfigurasi dan terkoneksi ke *log database* , dapat dilihat pada gambar 8.

Gambar 7. File *config crontab*

Kemudian membuat notifikasi *telegram*, untuk membuat notifikasi *telegram* ini dimulai dengan menginstall *swatchdog* dan membuat *bot telegram* yang menggunakan *cURL* dan di picu perubahan isi *alert log suricata* dengan bantuan *file swatchdog*, seperti pada gambar 9 *bot*

*telegram*sebagai berikut

Gambar 8. Telegram-bot.sh

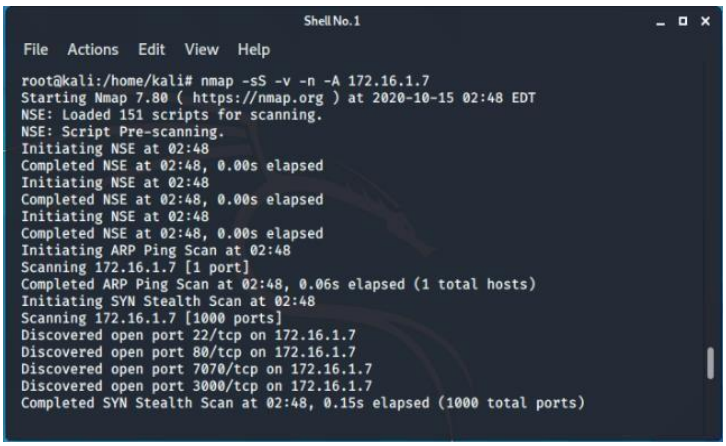
Sedangkan untuk *file* konfigurasi *swatchdog* dibuat untuk melakukan monitoring secara *realtime* untuk mengetahui perubahan yang terjadi pada file */var/log/suricata/fast.log*. adapun konfigurasi *swatchdog* sebagai berikut.

```
Watchfor /Possible: /
Exec bash
     telegram-
     bot.sh "Telah
     terjadi
     serangan"
echo red
throttle 00:01:00
```

Tiga ujicoba atau skenario pengujian simulasi serangan *scanning port, bruteforce ssh* dan *denial of service* untuk melakukan pengujian apakah notifikasi *alert* akan berfungsi dan terkirim melalui *telegram bot* dan *sms gateway* pada *software Intrusion Detection System* (*IDS*) *Suricata* dengan penyerangan di lakukan pada sistem operasi *kali linux* seperti pada gambar 10 berikut ini.

1) Skenario pertama Pada saat melakukan simulasi pengujian serangan menggunakan *software Nmap Scan* terdapat emapt *port* yang aktif dan serangan yang terjadi mendapatkan hasil yaitunotifikasi yang masuk di *telegram* dan *sms.*
2) Skenario kedua saat melakukan simulasi serang terhadap IDS *suricata* menggunakan *SYN Flood*, suricata mendeteksi terjadinya serangan *DoS* dan mengakibatkan *CPU* menjadi berat karena serangan tersebut, aktif dan serangan yang terjadipun mendapatkan hasil yaitu notifikasi yang masuk di *telegram* dan *sms*.
3) Skenario yang terakhir yaitu melakukan simulasi penyerangan ulang menggunakan *software Hydra*, serangan tersebut terdeteksi langsung oleh *IDS suricata* dengan menampilkan pesan terjadinya serangan *Bruteforce SSH* dan serangan yang terjadipun mendapatkan hasil yaitu notifikasi yang masuk di *telegram* dan *sms*.

Dari ujicoba tiga serangan *scanning port, bruteforce ssh* dan *denial of service* didapatkanhasil notifikasi dari *telegram bot* dan *sms* secara *realtime* bila ada serangan yang masuk di *log suricata* dan tersimpan di *fast.log*. Dari hasil notif yang di dapatkan setiap serangan masuk akan berbeda setiap waktunya.



Gambar 9. Skenario Pengujian Serangan

Pada hasil dari notifikasi *sms* yang di integrasi secara *realtime* juga akan berbeda dengan notifikasi *Telegram Bot*, terdapat pengambilan *ip address* dan *waktu penyerangan*, yang tersimpan di database yang sudah di koneksikan bersama *gammu* dan *script alert* yang dikirimkan ke administrator secara *realtime.* Setelah administrator mengetahui ancaman serangan yang masuk terhadap *server* maka administrator akan melakukan tindakan pencegahan dan melakukan penanganan terhadap *ip address* yang di dapatkan yang melalui *IDS suricata*. Administrator melakukan tindakan ke *ip address* tersebut berupa seperti tidak akan bisa mengakses lagi maupun masuk kembali ke dalam ruang lingkup didalam jaringan dan menonaktifkan *port* akses terhadap *ip address* yang meyerang *serverIDS suricata* sehingga serangan yang masuk tersebut telah di tangani dengan cepat dan akurat tanpa ada permasalahan yang lebih parah dari sebelumnya. Setelah melakukan pengujian sistem IDS Suricata dan simulasi pengujian ulang seperti diatas maka dibuatlah tabel hasil dari pengujian. Data yang di dapatkan pada saat pengujian sistem keamanan berupa paket – paket serangan yang masuk seperti serangan scanning port, bruteforce ssh dan denial of service, Tabel 3 dibawah ini adalah tabel hasil dari pengujian.

Tabel 3. Hasil Pengujian Serangan

No	Pengujian Sistem	Tipe Serangan	Status Serangan *Suricata*	Status Pengiriman Notifikasi
1	*Scanning Port*	*Nmap Scan*	Terdeteksi	Terkirim
2	*Scanning Port*	*ET Scan Nmap*	Terdeteksi	Terkirim
3	*DoS*	*DoS TCP*	Terdeteksi	Terkirim
4	*DoS*	*DoS TCP*	Terdeteksi	Terkirim
5	*SSH*	*Brute Force SSH*	Terdeteksi	Terkirim
6	*SSH*	*ET SCAN POTTENTIAN SSH*	Terdeteksi	Terkirim

Dari tabel 3 diatas hasil pengujian serangan yang yang didapatkan, penyerang melakukan tiga pengujian sistem *sanning port, denial of service dan brute force*, untuk penyerangan tersebut mengguanakan satu laptop dengan mengguanakan sistem operasi *kali linux* untuk menyerang *serverIDS suricata*, dengan mendapatkan hasilnya penulis mendapatkan lima tipe serangan yang

berbedamulai dari *Nmap scan*, *ET Scan Nmap*, *Dos TCP*, *Brute force SSH* dan *ET scan pottential ssh*, padastatus monitoring didalam *server IDS suricata* mendeteksi enam serangan yang masuk artinya semua serangan yang masuk itu sukses dan telah terdeteksi oleh *suricata*, setelah mendapatkan serangan yang masuk dengan dilakukan integrasi notifikasi pengiriman melalui *telegram* dan *sms* administrator bisa mendapatkan notifikasi tersebut menggunakan *smartphone*.

Tabel 4. Hasil Pengujian Pengukuran Jumlah Serangan

No	Nama Serangan	Jumlah Serangan	Jumlah Notifikasi	*Delay* PengirimanNotifikasi
1	*ScanningPort*	25	25	1
2	*DoS*	5	5	1
3	*Bruteforce*	12	12	1

Pada tabel 4 didapatkan hasil dari pengujian, dalam pengujian ini peneliti memonitoring serangan dari penyerang yang menggunakan sistem operasi *kali linux* untuk menyerang *server IDSsuricata*, dalam kasus ini didapatkan serangan yang masuk dengan jumlah 45 serangan pada hari terakhir melakukan pengujian. *IDS suricata* menangkap serangan *Scanning port* dengan jumlah serangan 25, *IDS suricata* menangkap serangan *denial of service* berjumlah 5 serangan, dan *IDS suricata* menangkap serangan *brute force* berjumlah 12, dan untuk pengiriman notifikasi ke *telegram* dan *sms* sama dengan masuknya serangan yang terjadi ke target *IDS suicata*.

Tabel 5. Analisis Hasil Pengujian

No	Jenis Pengujian	Tools	Hasil
1	*Scanning Port*	*Nmap*	Suricata berhasil mendeteksi serangandan mampu memberikan *alert*
2	*DoS*	*Hping3*	Suricata berhasil mendeteksi serangan dan mampu memberikan *alert*
3	*Bruteforce*	*Hydra*	Suricata berhasil mendeteksi serangandan mampu memberikan *alert*
4	*Koneksi*	*Terminal*	Penyerang dapat terhubung ke servertarget
5	*Gammu*	*Gammu*	Notifikasi dapat dikirimvia sms
6	*Telegram*	*Telegram*	Notifikasi dapat dikirimvia Telegram

Pada tabel 5 diatas hasil pengujian dari jenis pengujian *scanning port* menggunakan *toolsnmap* dan *server IDS suricata* berhasil mendeteksi ancaman dan memberikan *alert*. Jenis pengujian *Denial of service* menggunakan *tools Hping3* dan *IDS suricata* mampu mendeteksi ancaman dari serangan tersebut sehingga berhasil memberikan *alert* pada *administrator*. Jenis pengujian *brute force* menggunakan *tools hydra* dan *IDS suricata* berhasil dan mampu mendeteksi keberadaan dari ancaman serangan tersebut sehingga memberikan *alert* secara *realtime*.

Tabel 6. Hasil Pengujian Pada Serangan

Hari/ Tanggal	Waktu Awal	Waktu	Jenis Serangan	SeranganMasuk

	Penyerangan WIB	Terdeteksi		
Senin, 12-10-2020	13.30	13.10	*Scanning port, DoS, Bruteforce*	50
Selasa 13-10-2020	10.15	10.15	*Scanning port, DoS, Bruteforce*	33
Rabu 14-10-2020	11.30	11.30	*Scanning port, DoS, Bruteforce*	65
Kamis 15-10-2020	12.44	12.44	*Scanning port, DoS, Bruteforce*	39
Jumat 16-10-2020	14.12	14.12	*Scanning port, DoS, Bruteforce*	42

Dari hasil memonitoring selama 5 hari pengujian penyerangan menggunakan laptop dengan sistem *operasi kali* linux untuk menyerang *server* yang telah di pasang mengguanakan *IDS suricata* berdasarkan tabel 6 diatas dapat disimpulkan pada hari rabu penyerang melakukan serangan pada jam siang 11.30 wib dan *IDS suricata* mampu mendeteksi serangan secara *realtime* dan hasil yang di dapatkan berjumlah 65 serangan yang masuk lebih banyak daripada hari lainnya dan dengan terdeteksinya 3 serangan yang masuk yaitu *scanning port, denial of service* dan *brute force*.

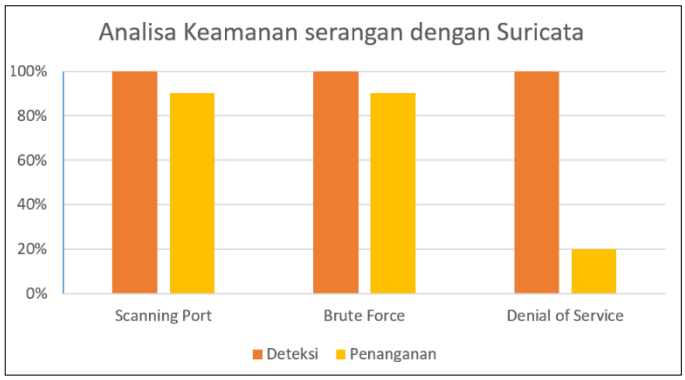
Faktor penyebab terjadinya serangan masuk dapat terjadi karena *hacker* atau *cracker* mampu masuk melalui celah yang terbuka seperti *port* yang sealalu terbuka untuk *public, server* hanya digunakan untuk keperluan data perusahaan saja, rentan akan terjadinya serangan seperti *scanning port, bruteforce ssh* dan *denial of service* dan hanya satu orang administrator untuk memonitoring. Maka dalam kasus ini sering kali berdampak sehingga terjadinya *down*nya *server* ataupun tidak bisa terkoneksi ke *server* tersebut, hal inilah yang menyebabkan terjadinya *server* menjadi gangguan atau *down* pada waktu tertentu.

Dari simulasi pengujian sistem keamanan *IDS suricata* dapat di ambil kesimpulan, sistem akan menunjukan adanya serangan yang akan dideteksi oleh *IDS suricata* jika terjadinya penyerangan terhadap *server IDS suricata* secara otomatis akan megirim notifikasi melalui *software*telegram dan sms, pendeteksian serangan yang telah dilakukan sesuai dengan aturan yang di buat mulai dari *scanning port, bruteforce ssh* dan *denial of service*.

Tabel 7. Hasil Pengujian Sistem

No	Pengujian Sistem	Tipe Serangan	Hasil Serangan	Kesimpulan
1	*Scanning Port*	*Nmap Scan*	Terdeteksi	Berhasil
2	*SSH*	*Bruteforce*	Terdeteksi	Berhasil
3	*DoS*	*SYN Flood*	Terdeteksi	Berhasil

Berdasarkan data yang di peroleh dari pengujian bahwa adanya faktor yang mempengaruhi mengapa serangan itu bisa terjadi. seperti *port* yang selalu terbuka, *server* hanya digunakan untuk keperluan data perusahaan saja, rentan akan terjadinya serangan seperti *scanning port, bruteforce ssh* dan *denial of service*, belum terpasangnya sistem keamanan jaringan server. Berikut grafik hasil analisis keamanan serangan menggunakan *suricata*, pada gambar 10.



Gambar 10. Grafik Keamanan Serangan

Pada gambar diatas grafik menunjukan persentase keberhasilan pendetksian dan penanganan dari keamanan *suricata*, persentase keamanan serangan 100% mampu di deteksi oleh suricata dan 90% mampu di tangani oleh administrator, persentase keamanan*brute force* yaitu 100% dapat dideteksi oleh suricata dan 90% dapat di tangani oleh administrator, dan keamanan serangan dari *denial of service* 100% dapat di deteksi dengan suricata dan 20% dapat di tangani oleh administrator.

Solusi yang dapat dilakukan dari permasalahan ini agar terhindar dari ancaman *hacker*ataupun *cracker* yang bisa mengakibatkan kerusakan atau pencurian data yang tidak di inginkan.

a. Setiap terjadi adanya aktivitas serangan masuk, administrator dapat melihat dan memonitoring langsung melalui:
   #tail -f /var/log/suricata/fast.log
   dan jika terjadi aktivitas mencurigakan seperti adanya serangan yang masuk, notifikasi*telegram* dan *sms* akan mengirimkan ke administrator secara *realtime.* Jika administrator tidak sedang berada di ruangan *server* maka notifikasi telegram dan smsakan tetap dikirim secara *realtime* jika terjadi adanya serangan ataupun aktivitas yangmencurigakan yang akan masuk ke *server IDS suricata*.
b. Administrator yang telah mengetahui adanya ancaman tersebut, bisa melakukan tindakan secara *offline* dengan melakukan pemblokiran *ip address* yang di dapat danmenonaktifkan jalur *port* yang telah di deteksi oleh *suricata* dikarenakan adanya serangan yang masuk melewati celah *port* tersebut.
c. Administrator jaringan melakukan monitoring pada sistem keamanan suricata secaraberkala baik melalui *offline* dan *online*.

4. KESIMPULAN

Telegram dan sms sebagai media notifikasi serangan jaringan, dapat diambil kesimpulan sebagai berikut : Langkah pendeteksian *intrusion detection system IDS suricata* dilakukan melalui limatahapan, yaitu mengkonfigurasi *suricata*, membuat *file rules suricata*, konfigurasi *gammu*, membuat*triger* ke notifikasi *telegram* dan pembuatan *script php* kirim pesan sehingga menghasilkan *alert* berupa *sms* dengan tiga jenis informasi, yaitu : *Ip address* sumber, *ip address* tujuan, jenis serangandan waktu penyerangan. Menambahkan *alert* pada notifikasi *telegram* dan *sms* untuk mengetahui bila ada terjadinyaaktivitas serangan yang mencurigakan masuk kedalam *log suricata* yang tersimpan di direktori */var/log/suricata/fast.log.* Untuk pengembangan sistem deteksi menggunakan *intrusion detection system* (*IDS*) *Suricata*dalam mendeteksi jenis serangan lain seperti : SQL *Injection*, *Cross-site Scripting* (XSS), *Man in the Middle* dan lain-lain. Perlu

dilakukan analisa *suricata* versi terbaru dan mengimplementasikan *intrusion detection system* (*IDS*) *suricata* ini menjadi secara luas dengan media nirkabel dan sistem jaringan *workstation* yang lebih besar seperti multi *WAN*, sehingga bisa membuat penggunaannya tersebut secara tidak terbatas. Saran untuk menggunakan *tools* pengujian *Intrusion detection system* (IDS) lainnya guna melakukan perbandingan analisis dengan *IDS suricata* dengan *tools* yang belum pernah digunakan seperti *OSSEC, Zeek, Sagan* dan lain-lain.

DAFTAR PUSTAKA

Akhyar, Zaki. 2019. "Rancang Bangun Sistem Pengiriman Alert Instrusion Detection System Suricata Melalui Telegram." in *Prosiding Seminar Nasional Politeknik Negeri Lhokseumawe*. Vol. 2.

Ardianto, Feby, and Tri Akbar. 2017. "Perancangan Sistem Monitoring Keamanan Jaringan Jarak Jauh Menggunakan Mikrotik Operational System Melalui Virtual Private Network." *Jurnal Surya Energy*.

Ariyanto, Yuri, and Budi Harijanto. 2017. "Yuri Ariyanto 1) , Budi Harijanto 2) , Dan Yan Watequlis S. 3)." 3:178–89.

Davison, Robert M., Maris G. Martinsons, and Ned Kock. 2017. "Principles of Canonical Action Research." *Information Systems Journal*.

Hadi, Sofyan. 2016. "Implementasi Network Intrusion Detection System Pada Sistem Smart Identification." *EProceedings of Applied Science* 2(3):1171–76.

Hadil Deekshith. 2018. "Get Server Notification on Telegram App." Retrieved (https://www.assistanz.com/get-server-notificationtelegram-%0Aapp/).

Kermite, Reynaldi Yosfino, Agus Winarno, and Asih Rohmani. 2017. "Perancangan Sistem Administrasi Sekolah Dengan SMS Gateway Berbasis Web Menggunakan Gammu Pada SMK LPI Semarang." *JOINS (Journal of Information System)* 2(1):15–27.

Maribondang, Arifializevic Marthen, Hans Wowor, and Stanley Karouw. 2015. "PERANCANGAN SISTEM INFORMASI PEMETAAN DAN PEMANTAUAN DAERAH ALIRAN SUNGAI (DAS) TONDANO DI KOTA MANADO BERBASIS SMS-GATEWAY." *Jurnal Teknik Informatika*.

Nugraha, Beny. 2016. "Analisis Teknik-Teknik Keamanan Pada Cloud Computing Dan NEBULA (Future Cloud): Survey Paper." *TEKNOSI,*.

Pardosi, Rudy Samuel. 2015. *Kali Linux : Top Hacking*. Jasakom.

Region, Security BM. 2016. "Pengertian IDS (Intrusion Detection System)." Retrieved (https://satpambmregion2.wordpress.com/2016/11/01/pengertian-ids-intrusion-detection-system/).

Tony Firman. 2016. "Serangan Internet Terbesar Membikin Situs-Situs Top Tumbang." 1. Retrieved (https://tirto.id/serangan-internet-terbesar-membikin-situs-situs-top-tumbang- b9ZA).