Analisis Sistem Keamanan *Web Server* Dan *Database Server* Menggunakan *Suricata*

Nazwita[1], Siti Ramadhani[2]
SMK N 4 Payakumbuh, UIN Sultan Syarif Kasim
Alamat: Jl. Koto Kociak Kecamatan Latina Payakumbuh Sumatera Barat,
Jl. HR. Soebrantas Kelurahan Simpang Baru No. 155 KM 15,5 Kecamatan Tampan
e-mail: nazwita77@gmail.com, siti.ramadhani@uin-suska.ac.id

Abstrak

Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Suatu serangan ke dalam server jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam server itu sendiri yang mampu mendeteksi langsung. Suricata merupakan perangkat lunak pendeteksi dan sekaligus pencegah gangguan atau Intrusion Detection and Prevention System (IDPS) open source yang merupakan generasi lanjutan dari IDS/IPS. Suricata di bangun untuk alternatif multi-threaded untuk Snort , sistem multi-threaded yang dapat memberikan kinerja yang lebih tinggi dan skalabilitas yang lebih baik., Suricata dapat mendeteksi dan mencegah gangguan seperti Port Scanning atau *aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status* port *(biasanya* port *TCP) pada sebuah* host*, dan Brute force atau metode untuk mendapatkan password dari user yang menjadi target. Rule yang dirumuskan dalam suricata telah bekerja dengan baik dan pada gilirannya bisa membantu tugas network admin untuk melakukan tindakan prefentif terhadap serangan.*

Kata Kunci : *Keamanan Jaringan, Suricata IDS, Suricata Rule*

Abstract

Computer network security as part of a system becomes very important to maintain the validity and integrity of data and ensure the availability of services for its users. An attack on a computer network server can occur at any time. Whether the administrator is working or not. Thus required security system within the server itself is able to detect directly. Suricata is an open source detection and prevention software or Intrusion Detection and Prevention System (IDPS) which is an advanced generation of IDS / IPS. Suricata is built for a multi-threaded alternative for Snort, a multi-threaded system that can provide higher performance and better scalability. Suricata can detect and prevent interruptions such as Port Scanning or activity to get thorough information about port status (usually Port TCP) on a host, and Brute force or method to get the password of the target user. The rules formulated in suricata work well and in turn can help the network admin task to perform prefentive actions against attacks

Keywords: *Network Security, Suricata IDS, Suricata Rule*

1. Pendahuluan

Keamanan jaringan tergantung pada kecepatan pengaturan jaringan dalam menindak lanjuti system saat terjadi ganguan[1]. Untuk memperkuat keamanan jaringan komputer dapat diterapkan sistem pendeteksi serangan dalam jaringan komputer.*Server* sebagai sarana vital untuk menyimpan *database*, aplikasi dan layanan penting sangat diperlukan sisi keamanannya. Baik dari segi infrastruktur sendiri maupun aplikasi pendukungnya. Diharapkan *server* terhindar dari hal-hal yang menggangu kinerjanya sehingga pelayanan terhadap *client* berfungsi secara maksimal.

Keamanan jaringan komputer sebagai bagian dari sebuah sistem menjadi sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya[2]. Suatu serangan ke dalam *server* jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam *server* itu sendiri yang mampu mendeteksi langsung.

Namun tanpa meninggalkan aspek keamanan bagi *server* untuk sebuah *web*, sistem keamanan yang digunakan adalah salah satu IDS *engine open source* yang dirilis oleh OISF (*Open Information System Foudation*) organisasi non-profit yang didanai oleh pemerintah

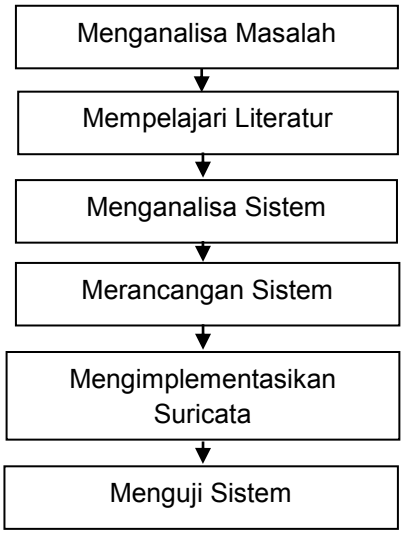
Amerika Serikat. Suricata merupakan perangkat lunak pendeteksi dan sekaligus pencegah gangguan atau *Intrusion Detection and Prevention System* (IDPS) open source yang merupakan generasi lanjutan dari IDS/IPS[3].

Database server merupakan suatu perangkat lunak yang mampu mengelola data dengan baik, sehingga data yang tersimpan dapat digunakan kembali. *Database server* menyediakan fleksibilitas untuk konfigurasi *database* service yang kita inginkan. *Client-server* model dapat diartikan sebagai model dari suatu sistem yang membagi proses sistem antara *server* yang mengolah *database* dan *client* yang menjalankan aplikasi. *Database server* mengurangi beban akses data oleh *client* pada *server*. *Database* dapat diakses oleh beberapa *client* secara bersamaan dimana data yang diakses hanya diubah berasal dari satu sumber yaitu *database* pada *server*[4].

Keamanan adalah suatu proses, bukan hasil dari sebuah produk. Keamanan bukan merupakan suatu sistem yang terletak pada hardware atau software yang digunkan, seperti *Firewall* atau *Intruder Detection.* Kerena memamng keamanan bukanlah hasil dari suatu produk, keamanan lebih kepada proses yang dilewati untuk mendapatkan aman itu sendiri[5].

2. Metodologi Penelitian

Tujuan penelitian adalah memasang sistem keamanan pada *server*, karena serangan ke dalam *server* pada jaringan komputer dapat terjadi kapan saja. Tahapan penelitian ini dimulai dengan menganalisa masalah, mempelajari literatur, menganalisa system, merancang system, mengimplementasikan system dan menguji sistem.



Gambar 1 Kerangka Kerja Penelitian

2.1 Menganalisa Masalah

Langkah analisis masalah merupakan langkah untuk dapat memahami masalah yang telah ditentukan ruang lingkup atau batasannya. Dengan menganalisis masalah yang telah ditentukan tersebut, maka diharapkan masalah dapat dipahami dengan baik.

2.2 Mempelajari Literatur

Studi literatur dilakukan dengan mempelajari buku-buku beberapa sumber jurnal, diktat ilmiah, *web*site resmi, majalah dan informasi lain yang ada kaitannya dengan implementasi keamanan *web server* dan *database server* menggunakan Suricata pada Linux Debian 6.0.

2.3 Menganalisa Sistem

Tahap ini akan dilakukan proses perancangan dan metode analisis terhadap keamanan jaringan komputer serta metode yang digunakan dalam mengatasinya. Pada tahap ini melakukan konfigurasi pada *Suricata* yang merupakan gambaran dari solusi yang akan

dihasilkan, dengan konfigurasi dan *rule* nya dapat menghasilkan output yang diinginkan yaitu *host* (komputer) aman dari serangan atau penyusup lainnya.

2.4 Mengimplementasikan Sistem

Setelah tahapan pengujian dilakukan, maka langkah selanjutnya adalah menerapkan sistem yang dibuat yaitu penerapan Suricata IDS sebagai sistem keamanan *web server* dan *database server.* Adapun perangkat yang digunakan dalam penyusunan penelitian ini adalah :

a) Perangkat keras, perangkat ini terdiri dari :
   1. Satu unit computer *server*, dengan spesifikasi sebagai berikut :
      a. Processor Xeon
      b. Motherboard DELL
      c. Hardisk SATA 320 Giga Byte
      d. Memory RAM 2 Giga Byte
      e. CD ROM DVD RW
      f. Ethernet Card RTL 8111/8168B PCI Express Gigabit
   2. Switch, menggunakan Dlink DES-1016D
   3. Router, menggunakan Mikrotik Router Board 750
   4. Wireless, menggunakan TP-LINK 3G/3.75 Wireless Lite N Router
   5. 1 unit computer sebagai *client,* dengan spesifikasi sebagai berikut :
      a. Processor Pentium Dual core
      b. Hardisk ATA 160 Giga Byte
      c. Memory RAM 2 Giga Byte
      d. CD ROM DVD RW

b) Perangkat lunak, perangkat ini terdiri dari:
   1. Linux Debian 6.0
   2. PuTTY Versi 0.62
   3. FileZilla Client Versi 3.6.0.2
   4. Suricata 2.03
   5. Nmap 5.62
   6. Brutus AET2

2.5 Menguji Sistem

Tahap berikutnya setelah perancangan dan pembangunan sistem adalah pengujian sistem. Hal ini dilakukan untuk melihat sejauh mana Suricata ini mampu memecahkan permasalahan. Pengujian dilakukan dengan *metode port scaning* menggunakan aplikasi NMAP dan *brute force* menggunakan Brutus. Pengujian dilakukan sebelum suricata diaktifkan dan setelah suricata diaktifkan, Hasilnya kemudian dievaluasi apakah sudah sesuai dengan hasil yang dicapai dalam keamanan jaringan komputer[6].

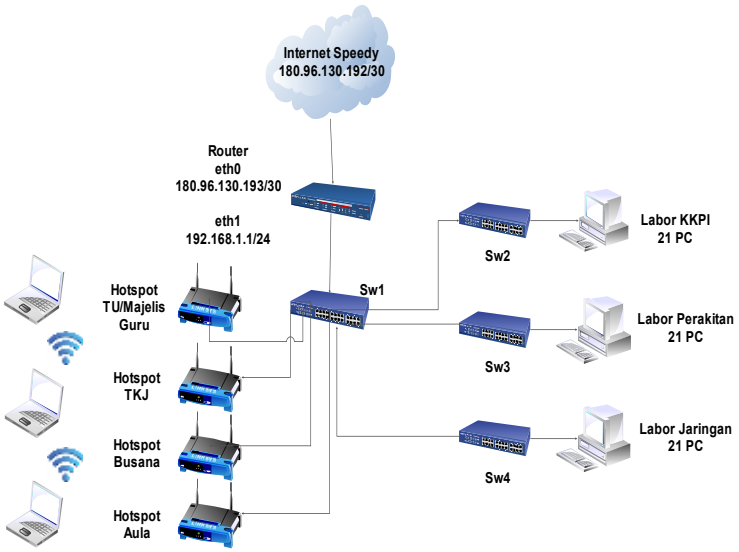
3. Hasil dan Analisa

Sistem keamanan *web server* dan *database server* merupakan hal penting untuk ditingkatkan,apalagi terkoneksi dengan *internet* yang dapat diakses dari berbagai negara atau area dan *user.* Banyak sekali tindakan kejahatan yang dilakukan oleh orang yang tidak bertanggung jawab terhadap sistem dengan berbagai serangan terhadap sistem.

3.1 Analisa sisitem yang sedang Berjalan

Analisis dilakukan dalam upaya untuk mengetahui kelemahan yang ada pada sistem yang digunakan. Pada saat ini sistem jaringan komputer belum menggunakan sistem keamanan *web server* dan *database server* . Sistem jaringan computer yang dianalisa berada pada SMK N 3 Payakumbuh. Jaringan computer yang digunakan di sekolah ini terdapat pada gambar 2.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



Gambar 2 Jaringan Komputer yang biasa digunakan

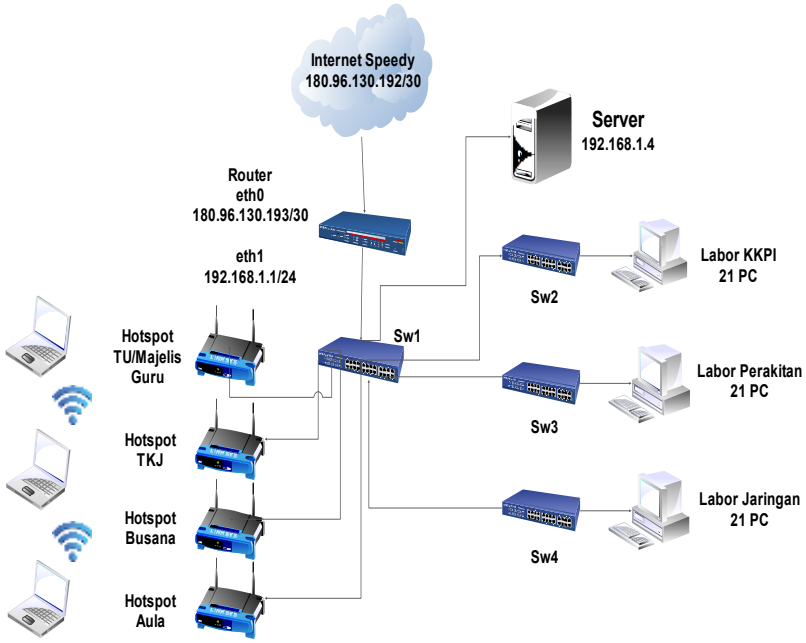
Pada gambar 2 topologi jaringan yang digunakan pada SMK N 3 Payakumbuh adalah topologi star. Dinamakan dengan topologi star karena sistem jaringannya yang terpusat pada satu media penghubung yaitu *router.* Router mempunyai 2 *ethernet card* (eth0 dan eth1), eth0 dihubungkan dengan *speedy* dan eth1 dihubungkan dengan *switch*. Switch akan membagi jaringan ke labor-labor dan ruangan lainnya.

Berdasarkan peninjauan langsung SMKN 3 Payakumbuh permasalahan yang dihadapi adalah tidak adanya sistem keamanan, karena pada sistem yang yang berjalan sekarang lama tidak dapat mendeteksi adanya serangan pada sistem. Kejadian seperti ini dapat menimbulkan ancaman bagi sistem SMK N 3 Payakumbuh. Hal ini menjadikan landasan untuk menjadikan sistem jaringan computer yang lebih aman.

3.2 Alternatif Pemecahan Masalah

Peningkatan keamanan jaringan komputer dari ancaman penyerang, SMKN 3 Payakumbuh memerlukan suatu sistem perlindungan untuk keamanan jaringan komputer. Perlingungan untuk sistem keamanan *web server* dan *database server* yang akan digunakan terlihat pada gambar 4.2 .

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406



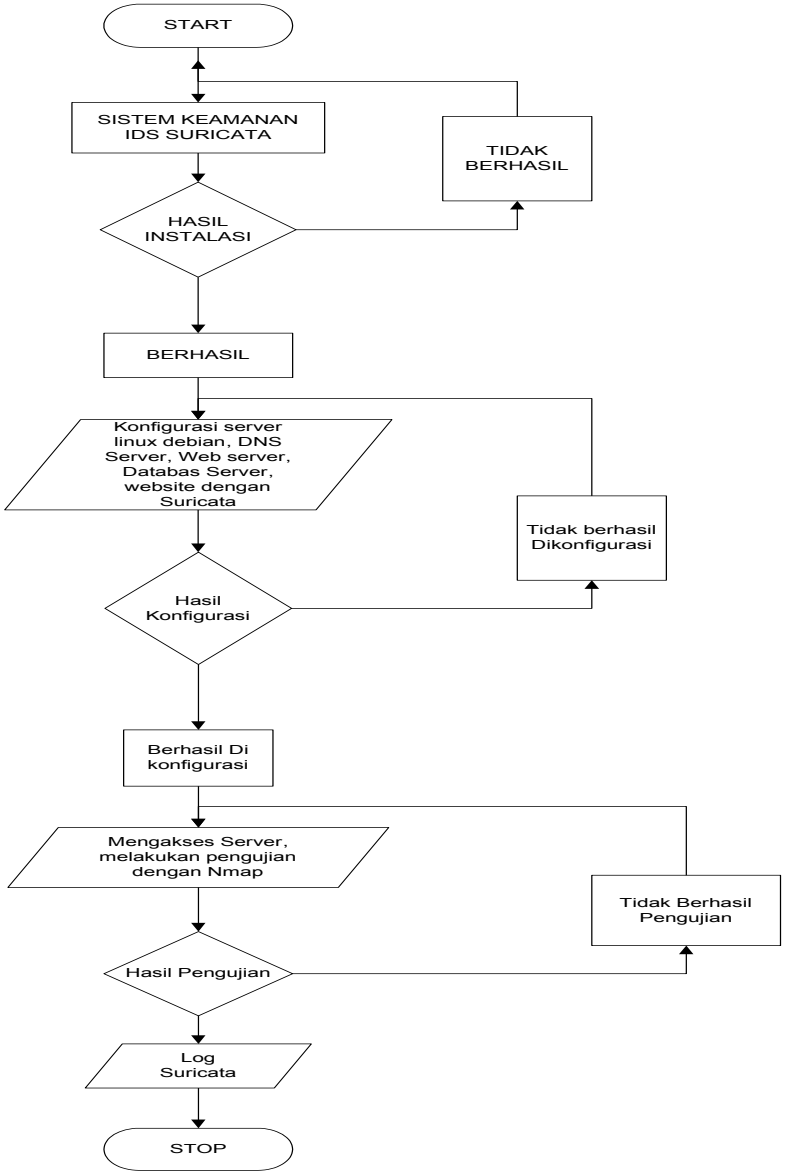
Gambar 3 Topologi Jaringan komputer yang Akan dibangun

Dari analisis yang dilakukan pada topologi jaringan di SMK N 3 Payakumbuh, maka akan dibangun sebuah server sebagai penempatan *server web*, *server database* dan sistem keamanan *server* Suricata. Dari gambar 4.2 dapat diuraikan bahwa :

a. Internet Speedy dihubungkan dengan Eth0 pada router dengan alamat IP publik dari Telkom 180.96.130.193/30 dan subnetmask 255.255.255.252
b. Sedangkan Eth1 pada router dihubungkan dengan switch (sw1) dengan alamat IP lokal 192.168.1.1/24 dan subnetmask 255.255.255.0
c. Server yang terhubung dengan Switch (sw1) mendapatkan alamat IP 192.168.1.4 karena rentang IP kelas C dengan /24 pada Switch utama mulai dari 192.168.1.2 sampai 192.168.1.254
d. Switch (sw1) juga terhubung dengan switch lainnya yang akan membagi jaringan ke labor KKPI, labor perakitan dan labor jaringan. Masing-masing labor memiliki rata-rata 21 *host* /PC dengan alamat IP yang diberikan secara DCHP karena jumlah *host* kelas C dengan /24 adalah 255 *host*
e. Switch (sw1) juga terhubung dengan beberapa access point yang ditempatkan masing-masing pada ruang majelis guru dan TU, sekretariat TKJ, labor jurusan busana dan aula.

3.3 Perancangan system

User akan melakukan konfigurasi dan mengaktifkan aplikasi *Suricata*, lalu dari penyerang akan memulai pengujian dengan melakukan serangan menggunakan *tools* yang sudah disediakan, penyerang akan melakukan pengujian serangan terhadap jaringan maupun *host* yang sudah dilindungi oleh aplikasi Suricata tersebut, saat aplikasi Suricata mulai di aktifkan maka suricata menampilakan log suricata dan si-penyerang tidak bisa melakukan serangan. Pada gambar 4 ditampilkan *flowchart* Suricata untuk mendeteksi serangan menggunakan IDS Suricata.



Gambar 4 Flowcahart Sistem IDS Suricata

Gambar 4 menjabarkan system kerja *Suricata.* Di mana *server* menjalankan perintah untuk mengaktifkan apliksi Suricata, sedangkan *client* menjalankan perintah untuk login ke *server* yang digunakan, intruder melakukan penyerangandan *Logs* menampilkan informasi siapa yang masuk kedalam *server*.

3.4 Pengujian system dengan teknik penyerangan

Sistem yang sudah di instal Suricata dan settingan tehadap web server dan database server yang digunakan siap untuk diuji oleh penyerang. Seorang intruder biasanya melakukan penyusupan dengan Nmap, yang mana Nmap dapat memantau port-port yang terbuka pada server akan tetapi dengan menggunakan IDS Suricata, maka Nmap tidak dapat lagi memantau port-port yang terbuka pada server[7], hal ini disebabkan Suricata telah melakukan tindakan Preventif atau pencegahan dengan cara melakukan blocking terhadap tindakan scanning dari si penyerang. Begitu juga dengan Brute force [8] dapat merupakan serangan pada password dengan mencoba segala kemungkinan agar password dapat diketahui dan server diambil alih, Setelah Suricata diaktifkan dapat dilihat bahwa brutus tidak lagi dapat menyerang, hal ini

disebabkan karena Suricata telah memutuskan koneksi sehingga brutus tidak dapat menemukan target karena koneksi telah terputus.

> ***Suricata akan melakukan deteksi ancaman yang terjadi dengan cara Signature Matching terhadap rules yang tersedia pada direktori Suricata dan akan ditentukan respon yang akan diberikan sesuai dengan aturan yang telah ditetapkan, apakah paket yang terdeteksi tersebut akan di berikan tindakan Pass, Drop, Reject, ataupun Alert. Setiap kegiatan yang terjadi dalam jaringan, Suricata akan merekam kegiatan tersebut dan menyimpan kedalam sebuah log. Admin dapat memantau seluruh kegiatan yang terjadi melalui log yang terekam tersebut.***

3.4.1 Pengujian Terhadap Sistem Tanpa Sistim Keamanan

Pengujian awal dilakukan dengan dengan metode *Port Scannig* menggunakan aplikasi *Nmap*. *Nmap* adalah aplikasi *open source* untuk eksplorasi jaringan atau audit keamanan seperti melakukan aktifitas *scanning port* atau peninjauan terhadap sebuah *server* yang dapat menampilkan *port-port* yang terbuka. Salah satau kelebihan dari *Nmap* adalah dapat digunakan dalam sistem jaringan yang besar namun dengan tingkat keandalan yang tinggi. *Nmap* dapat berjalan dalam semua sistem operasi baik Linux, Windows maupun Mac[9].

Penyerangan dengan mengunakan aplikasi Nmap yaitu dengan cara *Port Scanning* yaitu dengan memantau *port-port* yang terbuka, *port* yang terbuka langsung di *scan o*leh sipenyerang dan si penyerang bisa masuk ke dalam server. Pada gambar 6 pengujian dilakukan sebelum *Suricata* diaktifkan, dapat dilihat bahwa ada banyak *port* terbuka pada *server* yang dapat dipantau melalui aplikasi *Nmap*.

Gambar 6 Port Scaning sebelum Suricata diaktifkan

Sebelum *Suricata* diaktifkan didapat informasi-informasi *port* yang terbuka, antara lain :

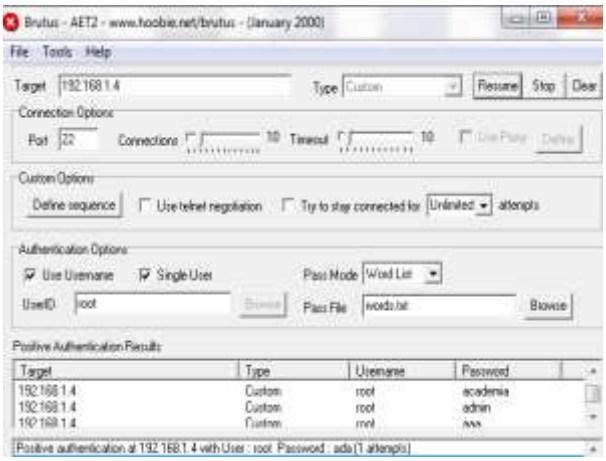
a. *Port* 21 yaitu *port* untuk FTP (*File Transfer Protocol)* yang merupakan *port* untuk mengirim dan menerima file.
b. *Port* 22 yaitu *port* untuk layanan SSH (*Socket Secure Host)* yang merupakan *port* untuk remote (pengendalian)
c. *Port* 80 yaitu *port* untuk layanan *http*. *Http* merupakan *port* yang digunakan untuk dapat mengakses halaman *web*
d. *Port* 110 yaitu *port* untuk layanan *pop3*. *Pop3* merupakan *port* untuk menerima pesan *E-mail*
e. *Port* 139 yaitu *port* untuk layanan *Netbio*s. *Netbios* digunakan untuk menangani *file sharing*.

Kedua pengujian juga dilakukan dengan metode penyerangan *Brute Force* dengan aplikasi Brutus. Brutus merupakan aplikasi penyerangan brutal terhadap *password* yang cara kerjanya mencocokkan *password* dengan *list* yang telah disediakan.

Kelebihan Brutus yaitu tidak perlu mengetahui sistem *enkripsi* yang rumit, namun hanya dengan mencoba segala kemugkinan *password* yang digunakan sampai si penyerang

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

mendapatkan *password* yang benar. *Brute force* merupakan serangan pada *password* dengan mencoba segala kemungkinan agar *password* dapat diketahui dan *server* dapat diambil alih, seperti terlihat pada gambar 7 pengujian dilakukan sebelum *Suricata* diaktifkan.

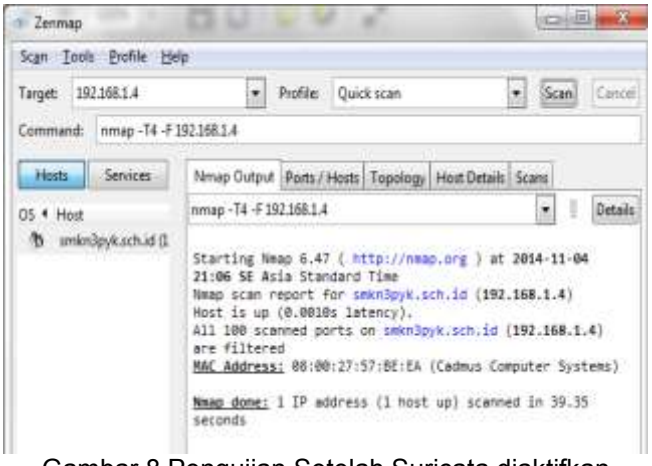


Gambar 7 Pengujian Sebelum Suricata

Dari gambar diatas, dapat dijelaskan bahwa target penyerangan adalah *host* dengan alamat IP 192.168.1.4 melalui *port* 22. Untuk memulai penyerangan hanya dengan menekan tombol start, kemudian pada bagian bawah ditampilkan beberapa kemungkinan *password.*

2. Pengujian Terhadap Sistem yang dilindungi suricata

Pengujian ini dilakukan terhadap sistem yang sudah di proteksi oleh sistem, yaitu dengan menggunakan IDS *Suricata*. Sewaktu *intruder* melakukan serangan terhadap sistem seperti melakukan *Nmap* atau Brutus atau mencoba untuk *login* ke dalam sistem, sistem dapat mendeteksi aktivitas tersebut. Jika data yang dikirim berbahaya atau tidak atau aktivitas yang dilakukan oleh penyerang terhadap sistem. Kemudian *Suricata* di aktifkan, kembali dilakukan pengujian dengan *Nmap*, dapat dilihat pada gambar 8 bahwa *Nmap* tidak dapat memantau *port* terbuka pada *server.*



Gambar 8 Pengujian Setelah Suricata diaktifkan

Setelah *Suricata* diaktifkan, didapatkan informasi bahwa *Nmap* tidak dapat lagi memantau *port-port* yang terbuka pada *server*, hal ini disebabkan *Suricata* telah melakukan tindakan *Preventif* atau pencegahan dengan cara melakukan *blocking* terhadap tindakan *scanning* dari si penyerang[10].

Pengujian juga dilakukan dengan metode penyerangan *Brute Force* dengan aplikasi Brutus. Brutus merupakan aplikasi penyerangan brutal terhadap *password* yang cara kerjanya

mencocokkan *password* dengan *list* yang telah disediakan. Salah satu kelebihan Brutus yaitu tidak perlu mengetahui sistem *enkripsi* yang rumit, namun hanya dengan mencoba segala kemugkinan *password* yang digunakan sampai si penyerang mendapatkan *password* yang benar.

Brute force merupakan serangan pada *password* dengan mencoba segala kemungkinan agar *password* dapat diketahui dan *server* dapat diambil alih, seperti terlihat pada gambar 5.60 pengujian dilakukan sebelum *Suricata* diaktifkan[11]. Setelah *Suricata* diaktifkan dapat dilihat bahwa brutus tidak lagi dapat menyerang, hal ini disebabkan karena *Suricata* telah memutuskan koneksi sehingga brutus tidak dapat menemukan target karena koneksi telah terputus. Berdasarkan hasil pengujian di atas, baik pengujian pada serangan seperti *Nmap* dan Brutus dapat dilihat bahwa sistem telah bekerja sesuai dengan yang diharapkan. Secara umum hasil semua pengujian pada sistem dengan IDS *Suricata* dapat di lihat dari tabel 1.

Tabel 5.1 Hasil Pengujian

No	Indikator	Hasil
1.	Serangan seperti *Nmap*, Brutus	Diketahui oleh administrator
2.	Log Aktivitas	Adanya *record* ke dalam log *client*
3.	Celah *login* pada *web server* dan *Database server*	Ditolak Sistem/ tidak dapat memantau *port-port* yang terbuka dan koneksi langsung terputus

Berdasarkan hasil pengujian di atas, baik pengujian pada serangan seperti *Nmap* dan Brutus dapat dilihat bahwa sistem telah bekerja sesuai dengan yang diharapkan.

4. Kesimpulan

Dari Analisa keamanan Web Server dan Database Server menggunakan Suricata pada Linux Debian yang telah dilaksanakan di SMK Negeri 3 Payakumbuh, dapat diambil beberapa kesimpulan diantaranya :

1. *Rule* yang dirumuskan dalam suricata telah bekerja dengan baik.
2. Sebagai sistem pendeteksi dan pencegah gangguan, Suricata dapat mendeteksi dan mencegah gangguan seperti *Port Scanning atau* aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status *port* (biasanya *port* TCP) pada sebuah *host*, dan *Brute force* atau metode untuk mendapatkan *password* dari user yang menjadi target.
3. Bisa membantu tugas *network* admin untuk melakukan tindakan *preventif* terhadap serangan *Nmap*

Daftar Pustaka

[1] S. Dave, B. Trivedi, and J. Mahadevia, “Application Profiling based on Attack Alert Aggregation,” *Glob. J. Comput. Sci. Technol. Network, Web Secur.*, vol. 13, no. 16, pp. 20–30, 2013.
[2] W. I. E. Nvironment, “Efficacy Of Attack Detection Capability Of IDPS Based On ITSD Eployment In Wired and Wireless Environtment,” *Int. J. Netw. Secur. Its Appl.*, vol. 5, no. 2, pp. 103–115, 2013.
[3] T. Oisf *et al.*, “Known issues & missing features About Suricata,” pp. 1–2.
[4] J.M. Kizza (springer-Verlag London), *Computer Communications and Networks*. 2013.
[5] A. M. R. Wajong, “Kerentanan yang dapat terjadi dijaringan komputer umumnya,” *ComTech*, vol. 3, no. 9, pp. 474–481, 2012.
[6] M. Anif, S. Hws, and M. D. Huri, “Penerapan Intrusion Detection System (IDS) dengan metode Deteksi Port Scanning pada Jaringan Komputer di Politeknik Negeri Semarang,” *J. Tele*, vol. 13, no. Maret, pp. 25–30, 2015.
[7] B. S. Candra, “Analisis Penerapan Keamanan Menggunakan IDN dan Honeypot,” *Fak. Ilmu Komput.*, vol. 1, no. Mei, pp. 1–23, 2015.
[8] A. Dan, I. Honeypot, and M. Honeyd, “Analisis dan Implementasi Honeypot menggunakan Honeyd sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan pada Jaringan,” *J. Jarkom*, vol. 1,

no. 1, pp. 40–48, 2013.
[9] G. Singh, “Intrusion Detection Using Network Monitoring Tools,” pp. 1–12, 2014.
[10] É. Leblond and V. Julien, “Suricata Features Advanced functionalities IPS basics IPS advanced functions,” *Open Inf. Secur. Found.*, pp. 30–41, 2013.
[11] L. Kulkarni and J. Bakal, “Intrusion Detection System (IDS) for Wireless Ad-hoc Networks using Evolution Identification on Streaming Network Data for Detecting Unknown Network Attacks,” *Int. J. Res. Comput. Commun. Technol.*, vol. 3, no. 2, pp. 213–218, 2014.