UNJUK KERJA INTRUSION PREVENTION SISTEM (IPS) BERBASIS SURICATA PADA JARINGAN LOKAL AREA NETWORK LABORATORIUM TIA+ TEKNIK INFORMATIKA, UNIVERSITAS TRUNOJOYO

Dwi Kuswanto
Program Studi Teknik Informatika, Universitas Trunojoyo Madura
Jl. Raya Telang, PO BOX 2, Kamal, Bangkalan - 69162
dwikuswanto@if.trunojoyo.ac.id

ABSTRAK

Keamanan sebuah system jaringan komputer merupakan suatu satu hal yang sangat penting. Perkembangan teknologi yang semakin cepat berdampak terhadap sistem keamanan jaringan, Dengan berbagai metode system keamanan jaringan dikembangkan yang salah satunya dengan metode *attack* (penyusupan/ serangan). Hal ini mengancam keamanan sebuah data. Untuk menjaga kerahasiaan, keaslian dan ketersediaan data tersebut, maka diperlukan sebuah sistem yang mampu mendeteksi adanya *attacker* pada system jaringan komputer yang dapat berjalan secara *real time*. Salah satu metodenya yakni *Intrusion Prevention System* (IPS). IPS adalah sebuah sistem yang mampu memonitor dan memblokir trafik jaringan komputer. System jaringan dimaksud diimpelemntasikan di *Local Area Network* (LAN) Laboratorium TIA+ Teknik Informatika. IPS yang dibangun berbasis Suricata yang berfungsi sebagai pendeteksi attacker. IPS ini dihubungkan dengan Internet Protocol (IP) Tables yang berfungsi sebagai pemonitor dan pemfilter *attacker* yang dilengkapi dengan tampilan *Guide User Interface* untuk memudahkan admin dalam memonitoring trafik jaringan. Hasilnya adalah Suricata akan mengeluarkan *alert* ketika terdeteksi adanya indikasi *attacker* pada trafik jaringan yang kemudian alert disimpan pada file log Suricata. Pada saat yang sama WebAdmin menampilkan dialog *alert* dan memerintahkan *IPTables* untuk memblokir alamat Internet Protokol (IP) yang teridentifikasi sebagai *attacker*, sehingga akses attacker terhadap server akan terputus. Berdasarkan implementasi sistem yang telah dilakukan sebanyak 100 kali, Suricata dan *IPTables* dapat bekerja secara optimal dan mampu mendeteksi *attacker*.

Kata kunci: IPS (*Intrusion Prevention System*) Suricata, *IPTables*, *Alert*, *Attacker*

ABSTRACT

The security of a computer network system is a very important thing. Increasingly rapid technological developments have an impact on the network security system, the various methods of network security system is developed that one attack *method (intrusion / attack). This threatens the security of the data. To maintain confidentiality, authenticity and availability of these data, we need a system that can detect the presence of an attacker on a computer network system that can be run in real time. One method that is Intrusion Prevention System (IPS). IPS is a system that can monitor network traffic and block the computer. Network system is diimpelemntasikan in Local Area Network (LAN) TIA + Laboratory Informatics. IPS is built based Suricata which serves as a detector of the attacker. IPS is connected to the Internet Protocol (IP) Tables that serve as monitors and pemfilter attacker equipped with a display Guide User Interface for easy admin in network traffic monitoring. The result is Suricata will issue alerts when detected indications of the attacker on the network traffic that is then stored in the alert log file Suricata. At the same time WebAdmin dialog displays alerts and ordered IPTables to block Internet Protocol address (IP) which is identified as the attacker, so the attacker access to the server will be disconnected. Based on the implementation of the system that has been done as much as 100 times, Suricata and IPTables to work optimally and is able to detect the attacker.*

Keywords: IPS (Intrusion Prevention System) Suricata, IPTables, Alert, Attacker

1. PENDAHULUAN

Saat ini kebutuhan internet merupakan hal yang sangat penting dimana jaringan komputer dibutuhkan untuk mempercepat aktivitas dalam segala bidang. Hal ini berdampak pada pribadi untuk mengikuti perkembangan jaringan komputer global. Pada jaringan komputer keamanan sangat penting terlebih untuk menjaga valid dan integritas dari suatu data serta jaminan layanan bagi pengguna. Banyak cara untuk melakukan penyusupan pada jaringan. Berawal sekedar tes pada jaringan hingga berusaha merusak atau mencuri informasi penting pada server.

Untuk membantu dalam pemantauan paket data pada jaringan dan menganalisa paket-paket tersebut untuk mencegah dari hal-hal yang bersifat membahayakan jaringan, dibutuhkan suatu sistem pencegah serangan dan dapat menampilkan peringatan saat terjadi penyusupan. Sistem Intrusion Prevention System (IPS) adalah sistem yang dapat mencegah dan memberikan tindakan saat terjadi penyusupan..

Suricata merupakan salah satu produk pendeteksi serangan selain snort. Suricata memiliki fitur *multi-threaded* yang berfungsi untuk meningkatkan kinerja suricata. Suricata diharapkan dapat menjadi mesin *intusion detection* generasi berikutnya.

Penelitian ini ditujukan untuk mengimplementasikan *Intrusion Prevention System* (IPS) berbasis Suricata dengan mengkombinasikan IPTables pada jaringan komputer LAN Laboratorium TIA^{+} Teknik Informatika, dimana sistem tersebut dapat mencegah dan memantau jaringan komputer secara otomatis sehingga dapat mengurangi ancaman-ancaman pada jaringan komputer. IPS ini di bangun pada lingkungan Linux Ubuntu 12.04 Precise Pangolin. Batasan masalah pada tugas akhir ini bahwa metode pendeteksian menggunakan signature-base berbasis suricata serta dikonfigurasikan sehingga terhubung dengan IPTables.

2. DASAR TEORI

Secara sederhana jaringan komputer dapat diartikan sebagai kumpulan dari komputer yang dapat berkomunikasi satu sama lain melalui media jaringan secara bersama-sama.

Definisi jaringan komputer menurut ensiklopedia bebas bahasa indonesia adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (printer, CPU), berkomunikasi (surat elektronik, pesan instan), dan dapat mengakses informasi bersama.

Sehingga, dapat disimpulkan bahwa jaringan komputer adalah sekelompok komputer atau lebih yang terhubung satu sama lain untuk berbagi sumber daya sehingga dapat berkomunikasi satu sama lain.

Jaringan komputer yang saling terhubung kesuatu komputer server dengan menggunakan topologi tertentu, biasanya digunakan dalam kawasan satu gedung atau kawasan yang jaraknya tidak lebih dari 1 km.

Keamanan jaringan merupakan salah satu aspek penting dari sebuah sistem informasi. Terdapat suatu pandangan yang menyatakan bahwa masalah keamana komputer merupakan tanggung jawab sepenuhnya *administrator* jaringan. Suatu sistem keamanan membutuhkan dukungan dari pihak pengguna jaringan itu sendiri. Sehingga perlu adanya penggenalan akan pengetahuan keamanan.

Keamanan komputer yang dibangun memiliki beberapa tujuan, diantaranya C*onfidentiality, Integrity dan Availability.*

a. Jenis Attacker

Jenis dan teknik serangan yang mengganggu jaringan komputer beraneka jenis, diantaranya adalah : *Dos & DDoS*, *Port Scanning, IP Spoofing*, *ICMP Flood, UDP Flood* , *Packet Interception dan Smurf Attack*

b. Intrusion Detection System (IDS)

IDS merupakan program atau aplikasi yang dapat mendeteksi adanya gangguan pada sistem kita. Pada saat ini ada beberapa IDS yang umum digunakan pada jaringan, salah satunya adalah SURICATA. Adapun tujuan dari *tools* ini diantaranya: mengawasi jika terjadi penetrasi kedalam sistem, mengawasi *traffic* yang terjadi pada jaringan, mendeteksi *anomali* terjadinya penyimpangan dari sistem yang normal atau tingkah laku user, mendeteksi signature dan membedakan pola antara *signature user* dengan *attacker*. IDS juga memiliki cara kerja dalam menganalisa apakah paket data yang dianggap sebagai *intrusion* oleh *intruder*. Cara kerja IDS dibagi menjadi dua, yaitu, *Knowledge Based* dan *Behavior Based*

c. Intrusion Prevention System (IPS)

Intrusion Preventing System (IPS) merupakan jenis metode pengamanan jaringan baik software atau hardware yang dapat memonitor aktivitas yang tidak diinginkan atau intrusion dan dapat langsung bereaksi untuk untuk mencegah aktivitas tersebut. IPS merupakan pengembangan dari dari IDS. Sebagai pengembangann dari teknologi *firewall*, IPS melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *port* atau *IP address* seperti *firewall* umumnya. IDS Selain dapat memantau dan monitoring, IPS dapat juga mengambil kebijakan dengan memblock paket yang lewat dengan cara "melapor" ke *firewall*.

Metode IPS untuk melakukan seleksi apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut yakni. *Signature-based Detection System* dan *Anomaly-based Intrusion Detection System*

d. Suricata

Open Information Security Foundation (OISF) adalah yayasan non-profit diselenggarakan untuk membangun generasi mesin IDS / IPS berikutnya. OISF telah membentuk kelompok multi-nasional dari pengembang perangkat lunak terkemuka di industri keamanan. Selain pengembang dan konsorsium yang terdiri dari perusahaan-perusahaan terkemuka dunia maya keamanan, OISF telah terlibat komunitas sumber keamanan terbuka untuk mengidentifikasi IDS saat ini dan masa depan / kebutuhan IPS dan keinginan.

Berikut adalah fitur utama Suricata. Yakni, *Multi Threading*, *Performance Statistics*, *Automatic Protocol Detection*, *Gzip Decompression*, *Independent HTP Library*, *Standard Input Methods*, *Unified2 Output*, *Flow Variables*, *Fast IP Matching*, *HTTP Log Module*, *Graphics Card Acceleration*, *IP Reputation* dan *Flowint*

e. IPTables

IPTables merupakan perintah untuk menentukan sebuah *rule-rule* firewall dalam tugasnya menjaga sebuah jaringan. *IPTables* memiliki tiga fungsi utama untuk menentukan arah putaran paket data. Ketiga fungsi tersebut yaitu packet *Filtering*, *NAT*, *Packet Mangling*. Paket *filtering* digunakan untuk memilah dan memberikan ijin *ACCEPT*/*DROP* pada suatu paket data, sedangkan *NAT* digunakan untuk mengubah alamat *IP* sumber atau tujuan dari suatu paket dalam jaringan, dan untuk Paket Mangling digunakan untuk memodifikasi paket QoS (*Quality of Service*). *IPTables* juga memiliki tiga macam daftar aturan bawaan dalam table penyaringan, daftar tersebut dinamakan rantai *firewall* (firewall *chain*) atau sering disebut chain saja. Pada saat sebuah paket sampai pada sebuah lingkaran, maka disitulah terjadi proses penyaringan.

Rantai akan memutuskan nasib paket tersebut. Apabila keputusannya adalah *DROP*, maka paket tersebut akan di *drop*, tetapi jika rantai memutuskan untuk *ACCEPT*, maka paket akan dilewatkan melalui diagram tersebut.

f. MySQL

MySQL dikembangakan pada tahun 1990an sebagai jawaban dari kebutuhan komputer untuk mengatur informasi dengan cerdas. MySQL adalah sebuah *relational databese management system* yang menyimpan data dalam tabel-tabel yang terpisah, bukan dengan meletakkannya dalam sebuah tempat untuk menigkatkan fleksibelitas dan kecepatan. Kepanjangan *SQL* pada *MySQL* adalah *Structured Querry Language*, adalah bahasa untuk mengakses *database*.

Contoh tipe data yang ada dalam MySql antara lain :

1. VARCHAR () : Tipe data string dengan lebar variasi yang dapat memiliki panjang antara 0 hingga 255 karakter.
2. TINYTEXT : Tipe data string dengan panjang maksimum 255 karakter.
3. TEXT ; Tipe data string dengan panjang maksimum 65565 karakter.
4. INT() : Integer yang berukuran normal, jangkauan unsigned adalah 0 hingga 4294967295
5. FLOAT : Bilangan floating-point, tidak dapat bersifat unsigned.

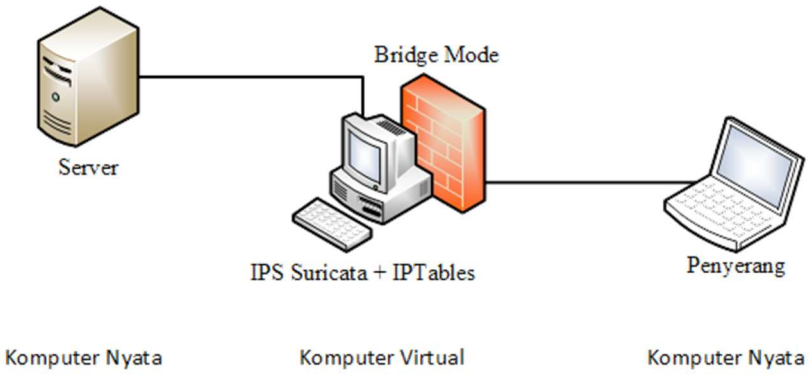
3. METODE PENELITIAN

Intrusion Prevention System (IPS) merupakan jenis pengamanan jaringan baik *software* atau *hardware* yang dapat memonitor aktivitas yang tidak diinginkan atau *intrusion* dan dapat langsung bereaksi untuk mencegah aktivitas tersebut. IPS merupakan pengembangan dari IDS. Sebagai pengembangan dari teknologi *firewall*, IPS dapat melakukan kontrol dari suatu sistem berdasarkan aplikasi konten atau *pattern*, tidak hanya berdasarkan *port* atau IP *address* seperti *firewall* umumnya. Selain dapat memantau dan monitoring, IPS dapat juga mengambil kebijakan dengan memblok paket yang lewat dengan cara "melapor" ke *firewall*.

Metode *rule-based detection* atau dikenal sebagai *signature-based detection* merupakan metode pendeteksian dengan cara menilai apakah paket data yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini dapat melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data signature yang ada harus tetap diperbaruhi.

Suricata merupakan *intrusion detection system* (IDS) kinerja tinggi yang dikembangkan oleh sebuah yayasan *non-profit Open Information Security Foundation* (OISF). Suricata dikembangkan oleh OISF dan vendor pendukungnya.

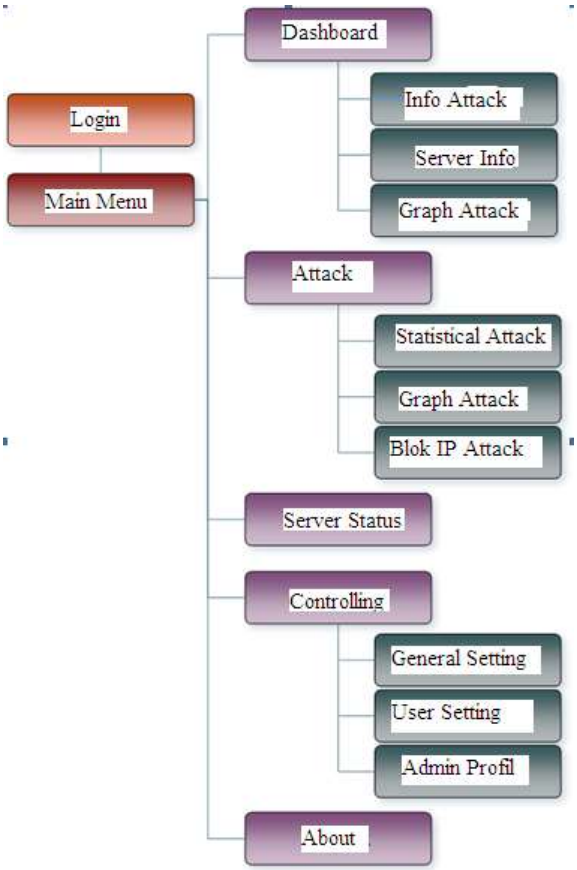
Pada Penelitian ini *Intrusion Prevention System* (IPS) sebagai *bridge* antara *server* dengan jaringan lokal sehingga *server* terlindungi oleh IPS. Topologi *Intrusion Prevention System* (IPS) pada penelitian ini cukup sederhana. IPS Suricata dipasang pada perangakat komputer yang juga difungiskan sebagai bridge untuk melindungi server dari segala aktivitas yang mengancam *server* tersebut. Pamasangan *Intrusion Prevention System* (IPS) seperti gambar 1adalah upaya untuk mencegah adanya aktivitas yang dapat mengancam server dari jaringan lain.



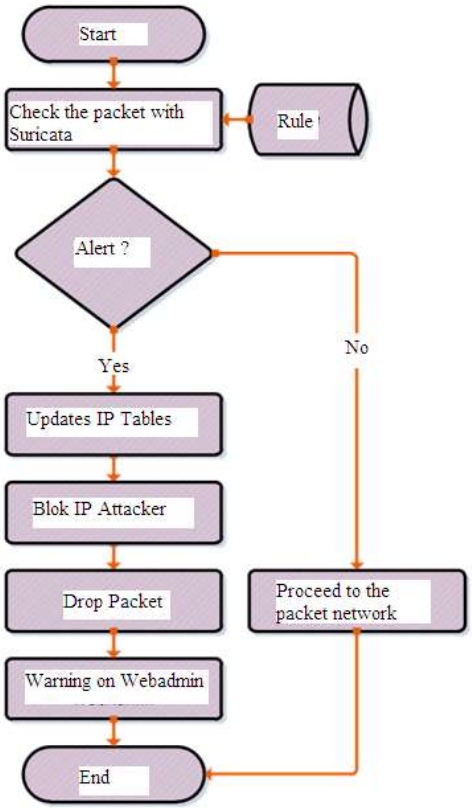
Gambar 1. Rancangan Topologi Jaringan Lokal Area Network Laboratorium TIA+ Teknik Informatika

Intrusion Prevention System (IPS) ini dibangun berdasarkan penggabungan dari beberapa komponen yakni :

1. Suricata *detection engine* berjalan pada mode *inline*, sehingga dapat bekerja sebagai pemeriksa dan penganalisa paket yang terindikasi sebagai serangan dan membuat alert ke dalam *file log* suricata.
2. IPTables memblokir atau meneruskan paket pada jaringan.
3. WebAdmin membaca dan memproses *file log* dan disimpanpada database MySQL.
4. Database MySQL menyimpan catatan kejadian untuk analisis selanjutnya.
5. WebAdmin menampilkan kejadian-kejadian dalam bentuk *web*secara real-time.

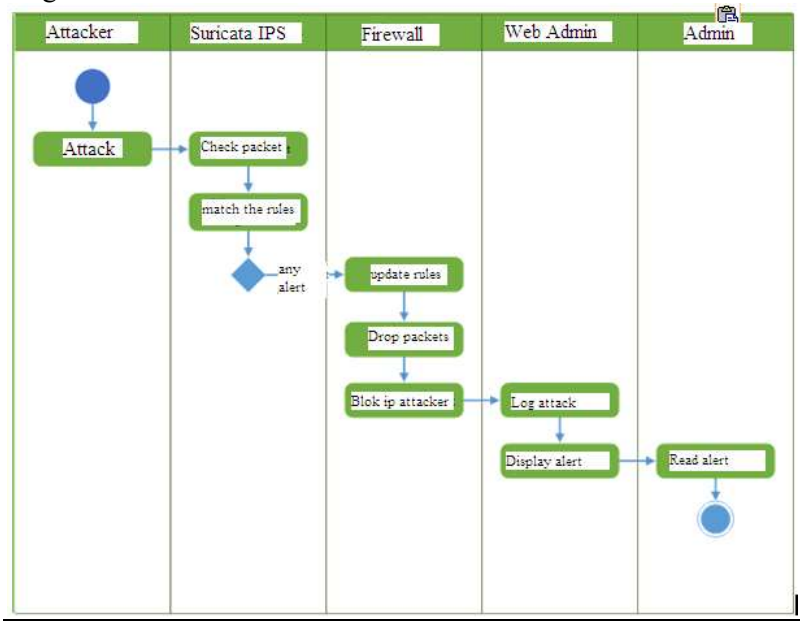


Gambar 2. Rancangan Admin User



Gambar 3. *Flowcart* IPS Suricata

Flowcart diatas menjelaskan mengenai cara kerja sistem IPS suricata secara keseluruhan. Paket data yang menuju *server* dilakukan pengecekan terlebih dahulu oleh suricata. Paket data tersebut kemudian dicocokkan dengan *rules* suricata. Jika paket data tersebut terindikasi sebagai serangan, maka suricata membuat alert. Selanjutnya *firewall* meng-*updaterule* IPTables untuk memblokir penyerang kemudian men-*drop*.paket data tersebut. Setelah itu WebAdmin menampilkan peringatan disertai suara.

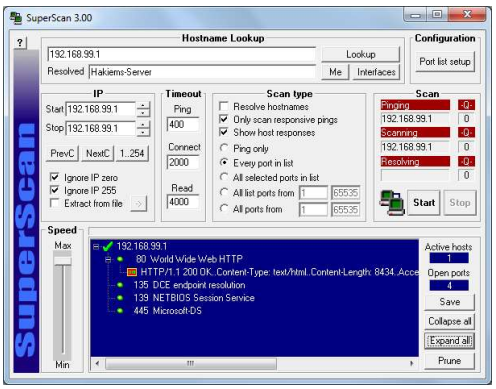


Gambar 4. Diagram *Activity* IPS Suricata

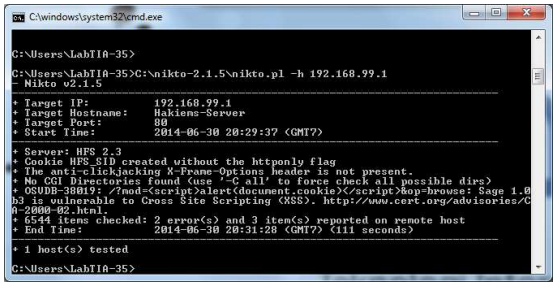
4. HASIL DAN PEMBAHASAN

Pada penelitian ini telah dilakukan uji coba pada sistem pendeteksi serangan dengan suricata dengan disertai Admin User untuk memantau hasil serangan.Uji coba ini dilakukan bertujuan untuk memastikan bahwa sistem IPS Suricata yang telah dibangun sesuai dengan tujuannya. Uji coba dilakukan antara *client* dengan *server* yang difokuskan pada jaringan Lokal Area network Laboratorium TIA+.

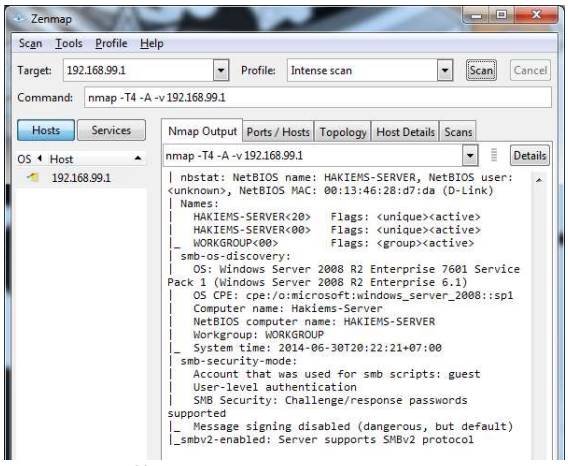
- Untuk menjalankan suricata pada modus inline menggunakan perintah sudo suricata –c /etc/suricata/suricata.yaml –q 0.
- Dan jika ingin memberhentikan suricata maka dengan menekan tombol ctrl + c pada keyboard.
- Untuk mengetahui status *chain* IPTables menggunakan perintah sudo iptables –vnL.
- Setelah langkah konfigurasi dan uji coba fungsi IPS suricata selesai, maka suricata siap untuk dilakukan uji coba pendeteksian dan fungsi *drop* paket dari penyerang. Dalam uji coba serangan ini menggunakan perangkat lunak superscan, nmap, dan nikto.



Gambar 5. Uji coba serangan dengan tool Superscan

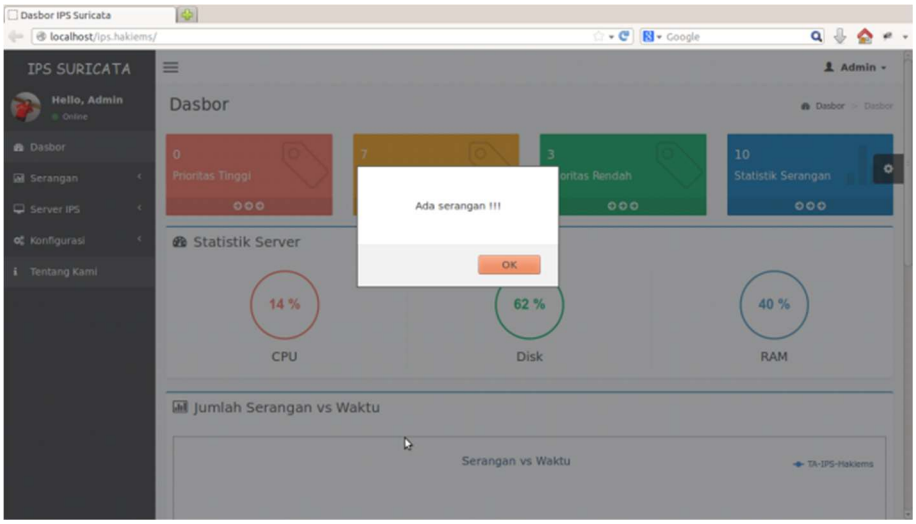


Gambar 6. Uji coba serangan dengan tool Nikto



Gambar 75. Uji coba serangan dengan tool Nmap

Setelah serangan dilancarkan maka suricata melakukan pengecekan pada setiap paket yang menuju server. Jika paket tersebut dianggap serangan, maka suricata mengeluarkan alert dan disimpan pada file *log* suricata. Alert tersebut kemudian dibaca oleh Admin User untuk ditampilkan pada laman web dan membuat peringatan sehingga admin lebih mudah memeriksa kondisi jaringan.



Gambar 8. Web Admin memberi peringatan ada serangan

5. KESIMPULAN

Hasil penelitian implementasi Unjuk Kerja I*ntrusion Prevention System* (IPS) suricata pada Laboratorium TIA^{+} Teknik Informatika menghasilkan beberapa kesimpulan yaitu:

1. Implementasi Suricata dan IPTables yang telah dikonfigurasi menjadi modus inline dapat bekerja dengan baik.
2. Sistem WebAdmin mampu mengkoneksikan antara suricata dan IPTables dengan baik sehingga dapat memblokir 100% IP penyerang melalui web.
3. Implementasi dari Intrusion Prevention System dapat melindungi server dari ancaman Attacker, karena IPS dapat mendeteksi dan mencegah adanya serangan yang mencurigakan pada jaringan.
4. WebAdmin memudahkan seorang Administrator jaringan dengan bantuan peringatan jika ada serangan dan dapat mengamati statistik serangan dan keadaan komputer IPS.

6. DAFTAR PUSTAKA

[1] Wicaksono, Bayu. Perancangan Dan Implementasi IPS (Intrusion Prevention System) Berbasis Web Menggunakan Snort Dan IPTables. 2012.
[2] Aryadi, Tamsir. Implementasi Intrusion Prevention System (IPS) Pada Jaringan Komputer Kampus B Universitas Bina Darma. Vol 14: 1-14. 2012.
[3] Ulum, Bahrul. Rancang Bangun Intrusion Prevention System Pada Jaringan TCP/IP mengunakan Snort dan IPTables. 2013.
[4] Stiawan Deris, "Intrusion Prevention System(IPS) dan Tantangan dalam pengembangannya," FASILKOM, UNSRI, Palembang, Indonesia.
[5] Purbo, Onno, 2010. Keamanan Jaringan Komputer. Handry Pratama. Jakarta.
[6] Open Information Security. Open Information Security Foundation. URL: http://www.openinfosecfoundation.org, diakses tanggal 1 Desember 2013.
[7] Aldeid Foundation. Suricata/Introduction. 5 April 2011. URL: http://www.aldeid.com/wiki/Suricata/Introduction#Description, diakses tanggal 3 Desember 2013.

[8] Suricatayaml - Suricata - Open Information Security Foundation. URL: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricatayaml, diakses tanggal 20 Mei 2014.
[9] Lukman, Tutorial IPTables, 5 Agustus 2003, URL: http://rootbox.or.id/tips/IPTables.html, diakses tanggal 20 Juni 2014.
Hakiems, Arif Rahman, Dwi Kuswanto, Rancang Bangun Intrusion Prevention System (IPS) Suricata, 2014.