Terakreditasi SINTA Peringkat 4
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 28/E/KPT/2019
masa berlaku mulai Vol.3 No. 1 tahun 2018 s.d Vol. 7 No. 1 tahun 2022

Terbit online pada laman web jurnal:
http://publishing-widyagama.ac.id/ejournal-v2/index.php/jointecs

JOINTECS

JOINTECS
(Journal of Information Technology and Computer Science)

Vol. 5 No. 1 (2020) 17 - 24

e-ISSN:2541-6448 p-ISSN:2541-3619

Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection and Prevention System

Hendri Alamsyah[1], Riska[2], Abdussalam Al Akbar[3]
[1,2]Program Studi Rekayasa Sistem Komputer, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
[3]Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu
[1]hendri.alamsyah@unived.ac.id, [2]riska.iskandar@unived.ac.id, [3]akbarabenk@unived.ac.id

Abstract

Security is an important aspect to be considered in computer networks. This security system can be a detection and prevention of attacks that are being done by the attacker (intruders). The problem of attacks that occur in computer networks is that intruders can do port scanning, enter the system using open ports such as telnet, ftp and others.. The purpose of this study is the implementation of IDPS, can be from. To do network security from various attack threats, a system that can detect and prevent it directly is needed. The method that can be used is Intrusion Detection and Prevention System (NIDPS). NIDPS can exchange and block the attacks. This security system is collaborated with IP Tables. IP Tables is used to filter incoming data packets and drop packets of data that are indicated by attack. With the Intrusion Detection and Prevention system, it can detect attacks and prevent them by blocking data packets sent by intruders through port scanning, FTP attacks, and telnets.

Keywords: network security; intrusion detection; prevention system; IP tables

Abstrak

Keamanan merupakan aspek penting yang harus diperhatikan dalam jaringan komputer. Sistem keamanan ini dapat beruapa pendeteksi dan pencegahan terjadinya serangan yang di lakukan oleh attacker (penyusup). Masalah serangan yang terjadi dalam jaringan komputer yaitu penyusup dapat melakukan port scanning, masuk pada sistem menggunakan port-port yang terbuka seperti telnet, ftp dan lainnya. Tujuan dari penelitian ini adalah mengimplementasikan IDPS, mampu mendeteksi dan memblokir adanya serangan dari penyusup. Untuk melakukan kemananan jaringan dari berbagai ancaman serangan dibutuhkan sebuah sistem yang dapat mendeteksi dan mencegah secara langsung. Metode yang dapat digunakan yaitu Intrusion Detection and Prevention System (NIDPS). NIDPS dapat mendeteksi dan melakukan blokir terhadap serangan yang terjadi. Sistem keamanan ini dikolaborasikan dengan IP Tables. IP Tables ini berfungsi untuk memfilter paket data yang masuk dan mendrop paket data yang terindikasi serangan. Dengan adanya Intrusion Detection and Prevention system ini dapat mendeteksi adanya serangan dan melakukan pencegahan dengan cara memblokir paket data yang dikirim oleh penyusup melalui port scanning, serangan ftp, dan telnet.

Kata kunci: keamanan jaringan; intrusion detection; prevention system; IP tables

1. Pendahuluan

Kebutuhan akan keamanan jaringan tentunya akan sangat dibutuhkan karena meningkatnya ilmu pengetahuan tentang hacking. Sangat banyak sekali software atau tools-tools yang di pergunakan oleh attacker untuk menyusup pada suatu jaringan ataupun server [1]. 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

Diterima Redaksi : 07-01-2020 | Selesai Revisi : 10-01-2020 | Diterbitkan Online : 28-01-2020

sedang bekerja ataupun tidak. Dengan demikian dibutuhkan sistem keamanan di dalam server itu sendiri yang mampu mendeteksi langsung [2]. Keamanan pada jaringan komputer sangat penting Seiring dengan semakin meningkatnya penggunaan *internet*, hal tersebut memberikan celah keamanan pada jaringan yang ada. Oleh karena itu keamanan jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah [3].

Syarat dari keamanan adalah prevention (pencegahan), yaitu memperkecil peluang penembusan oleh pemakai yang tak diotorisasi. Observation (observasi) yaitu identifikasi dan otentifikasi. Response (respon) yaitu upaya pengamanan data baik fisik maupun maya (software). Wall of Security atau tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindungan pada jarigan, baik secara fisik (kenyataan) maupun maya (menggunakan software) [4]. Salah satu metode yang sering digunakan oleh intruderadalah *distributed denial of service (DDos)* [5]. DDoS adalah aktifitas pengiriman paket dalam jaringan dalam jumlah besar yang ditujukan untuk membanjiri jaringan dengan data sehingga suatu host menjadi tidak dapat diakses oleh pengguna yang berhak [6].

Firewall merupakan fitur keamanan pada jaringan komputer yang dapat mengatur masuk keluarnya paket data. Pada jaringan yang sederhana, *firewall* biasanya hanya implementasikan pada komputer yang bersangkutan. Padahal belum tentu *firewall* pada komputer mampu memproteksi keamanan paket data yang diakses oleh penggunanya. Oleh karena itu, sebaiknya dipersiapkan suatu *firewall* yang mampu memproteksi pengguna dari akses internal maupun eksternal [7]. Sistem *firewall* juga merupakan salah satu perangkat lunak yang mampu mencegah beberapa serangan dari luar, namun *firewall* tidak dapat memberikan peringatan terhadap serangan yang cukup kompleks seperti, D-Dos dan serangan pada port-port tertentu.[8].

IP Tables adalah suatu *tools* atau alat yang berfungsi untuk melakukan filter (penyaringan) terhadap lalu lintas data yang terdapat pada sistem operasi linux atau sebagai pengatur lalu lintas data. *IP tables* mempunyai tiga macam aturan dalam tabel penyaringan, aturan tersebut adalah firewall chain. Ketiga chain tersebut adalah *INPUT, OUTPUT dan FORWARD*, *ip tables* juga memliki tiga tabel yaitu, *NAT*, *MANGLE* atau *FILTER*. *IP tables* adalah suatu firewall populer dan juga powerfull yang tersedia pada sistem operasi linux. Fungsi ip tables adalah untuk konfigurasi, merawat dan memeriksa rules tables (tabel aturan) tentang filter paket IP yang terdapat pada kernel linux. Filter berfungsi untuk melakukan penyaringan *IP* Tables adalah suatu *tools* atau alat yang berfungsi untuk melakukan filter (penyaringan) terhadap lalu lintas data yang terdapat pada sistem operasi linux atau sebagai pengatur lalu lintas data.

IP tables mempunyai tiga macam aturan dalam tabel penyaringan, aturan tersebut adalah firewall chain. Ketiga chain tersebut adalah *INPUT, OUTPUT dan FORWARD*, *ip tables* juga memliki tiga tabel yaitu, *NAT*, *MANGLE* atau *FILTER*. *IP tables* adalah suatu firewall populer dan juga powerfull yang tersedia pada sistem operasi linux. Fungsi ip tables adalah untuk konfigurasi, merawat dan memeriksa rules tables (tabel aturan) tentang filter paket IP yang terdapat pada kernel linux. Filter berfungsi untuk melakukan penyaringan. Paket data, apakah paket data tersebut akan di *DROP*, *LOG*, *ACCEPT* atau *REJECT*. Sedangkan NAT berfungsi untuk melakukan network address translation sebagai pengganti alamat asal atau tujuan dari paket data. Mangle untuk melakukan penghalusan paket data seperti *TTL*, *TOS* dan *MARK*. *RAW* untuk mengkonfigurasi pengecualian dari *connection* tracking bersama-sama *NOTRACK* [9].

Untuk mengatasi serangan-serangan pada jaringan tersebut dapat dilakukan dengan menggunakan metode Intrusion Detection and Prevention System (IDPS). IDPS sendiri merupakan perkembangan dari intrusion detection system yang dipadukan dengan firewall pada hal ini menggunakan IP Tables. Pada beberapa penelitian terdahulu tentang IDPS, tujuan utama dari IDS adalah untuk mendeteksi serangan secara efisien. Selain itu, sama pentingnya dalam mendeteksi serangan untuk mengurangi dampaknya [10]. Penerapan Intrusion Detection and Prevention System (IDPS) digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu administrator dalam memantau dan menganalisa paket-paket berbahaya yang terdapat dalam sebuah jaringan [11].

IDS (Intrution Detection System) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan yang mencurigakan berhubungan dengan traffic jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan [12]. Ada dua tipe dasar yang terdapat pada IDS yaitu Pertama *Rule Based System* berdasarkan pada signature dan rule yang tersimpan di database. Jika IDS mencatat lalu lintas yang sesuai dengan rule dan signature yang ada, maka langsung dikatakan sebagai suatu serangan. Kedua *Adaptive System*, tipe ini menggunakan metode yang lebih canggih, tidak hanya berdasarkan database yang ada, tetapi juga membuka kemungkinan untuk mendeteksi bentuk-bentuk serangan baru.

Pada dasarnya ada dua macam IDS, yaitu: Host-Based yan terdiri dari IDS host-based bekerja pada host yang akan dilindungi. IDS jenis ini dapat melakukan berbagai macam tugas untuk mendeteksi serangan yang dilakukan pada host tersebu. Keunggulan IDS host-based adalah pada tugas-tugas yang berhubungan

dengan keamanan file. Misalnya ada tidaknya file yang telah diubah atau ada usaha untuk mendapatkan akses ke file-file yang sensitif. Network based : IDS network based biasanya berupa suatu mesin yang khusus dipergunakan untuk melakukan monitoring seluruh segmen dari jaringan. IDS network based akan mengumpulkan peket-paket data yang terdapat pada jaringan dan kemudian menganalisisnya serta menentukan apakah paket-paket itu berupa suatu paket yang normal atau suatu serangan atau berupa aktivitas yang mencurigakan. Intrusion prevention system (IPS) adalah proses pendeteksi aktvitas intrusi atau ancaman dan pengelolaan tindakan responsif terhadap intrusi dan ancaman yang terdeteksi pada jaringan. IPS memantau lalu lintas paket secara real time dengan aktivitas jahat atau yang sesuai dengan profil tertentu dan akan memicu peringatan, melakukan drop, memblokir lalu lintas yang melalui jaringan secara real time. Tindakan utama IPS adalah menghentikan serangan yang sedang berlangsung [8].

Untuk melakukan kebijakan paket data layak atau tidak masuk jaringan ada beberapa metode IPS yang digunakan, pertama Signature-based Intrusion Prevention System, pada metode ini telah disediakan daftar signature yang bisa digunakan untuk menilai paket yang dikirim berbahya atau tidak. Sebuah paket akan dibandingkan dengan daftar yang telah tersedia. Metode ini melindungi sistem dari serangan yang sudak di ketahui sebelumnya. Untuk menjaga keamanan jaringan komputer data yang ada pada signature mesti selalu ter-update. Selanjutnya *Anomaly-based Intrusion Prevention* System, Metode ini harus melakukan konfigurasi dahulu pada IDS dan IPS yang ada, sehingga bisa mengetahui pola paket apa saja yang akan ada pada sebuah sistem jaringan komputer. Paket anomaly merupakan paket yang tidak sesuai pada kebiasaan jaringan komputer. Jika IDS dan IPS mendapatkan anomaly pada paket yang diterima atau dikirimkan, maka IDS dan IPS secara otomatis akan memberikan alarm atau peringatan dan menolak paket tersebut.

Suricata adalah IDS yang lebih baru. Awalnya didanai oleh Direktorat Ilmu Pengetahuan dan Teknologi Departemen Dalam Negeri dan dirancang untuk bekerja dengan peraturan Snort. Rule set tersedia dari Emerging Threats atau Emerging Threats Pro. Suricata dikembangkan menjadi "mesin IDS generasi berikutnya" dengan kemampuan IPS (Intrusion Prevention System) yang dirancang agar kompatibel dengan peraturan Snort. Suricata dirancang sebagai sistem multi-threaded, memungkinkannya memanfaatkan beberapa core. Pada mesin single core, Snort telah terbukti mengungguli Suricata. Oleh karena itu, Suricata menunjukkan kinerja yang superior pada mesin multi-core dengan aturan yang dioptimalkan untuk Suricata. Akibatnya, dengan mudah bisa memeriksa volume lalu lintas yang banyak tanpa harus mengurangi jumlah aturan. Suricata juga dibedakan oleh kemampuannya untuk memberikan visibilitas ke lapisan Aplikasi dan penguraian HTTP yang lebih cepat. Ini dapat memeriksa lalu lintas HTTP terlepas dari nomor port yang digunakan dan tidak bergantung pada nomor port untuk mengidentifikasi lalu lintas. Suricata juga memungkinkan pemeriksaan di dalam aliran protokol dan sebagai hasilnya dapat mengekstrak file dari sesi HTTP untuk pemeriksaan lebih lanjut [13].

Untuk IDS pada Suricata, saat mendeteksi adanya serangan maka Suricata hanya akan akan menampilkan alert.[14]. Adapun fitur utama Suricata adalah sebagai berikut, *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.*[15]. Pemanfaatan Intrusion Detection and Prevention System (IDPS) selain berfungsi untuk mendeteksi serangan yang terjadi pada jaringan, juga untuk mencatat setiap aktifitas intrusi yang terjadi. Data intrusi yang dicatat ke dalam database yang memuat informasi mengenai sumber serangan, waktu kejadian, jenis serangan, serta dampak yang dihasilkan bisa digunakan sebagai keperluan analisis forensik jaringan yang biasanya dilakuakn oleh administrator jaringan [16].

2. Metode Penelitian

2.1. Kerangka Kerja Penelitian

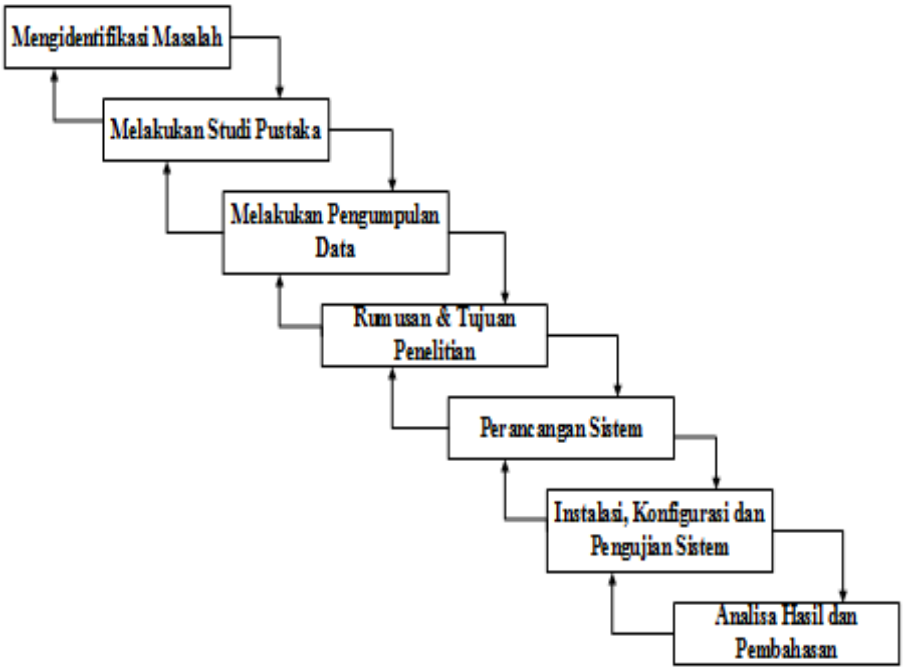
Kerangka kerja penelitian merupakan tahapan-yahapan yang harus dilalui dalam penelitian untuk menghasilkan *output* yang diinginkan. Ilustrasi kerangka kerja penelitian terlihat pada Gambar 1

2.2. Tahapan Analisa dan Perancangan

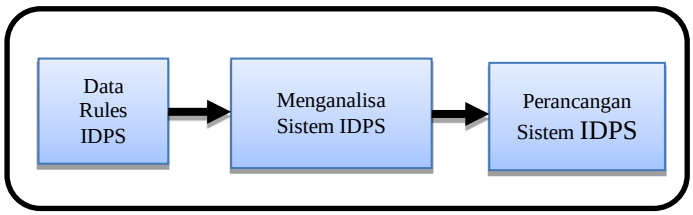
Berdasarkan kerangka kerja penelitian yang terdapat pada metodologi penelitian pada Gambar 2, bahwa tahapan kerja terdiri dari ruang lingkup masalah, mempelajari literatur, melakukan pengumpulan data, perancangan sistem, implementasi dan pengujian sistem. Untuk memudahkan dalam analisa dan perancangan sistem maka dibuat bagan alir analisa dan perancangan seperti pada Gambar 2 bagan alir analisa dan perancangan.

2.3. Analisa Sistem

Sebagaimana yang telah digambarkan pada bagan alir analisa dan perancangan yang ditunjukan Gambar 2, maka dalam menganalisa sistem keamanan jaringan menggunakan metode network intrusion detection and prevention system memiliki langkah-langkah seperti yang terdiri dari menetukan rules IDPS, detection, proses pencocokan rules, penyimpanan data pada *log*, hasil deteksi dan menampilkan hasil *log*.



Gambar 1. Kerangka Kerja Penelitian



Gambar 2. Bagan Alir Analisa Dan Perancangan

3. Hasil dan Pembahasan

Berdasarkan metode yang digunakan, pada proses deteksi dan pencegahan akan dijalankan dalam bentuk inline. Sistem akan bekerja ketika perintah pada IDPS dijalankan dan paket-paket yang masuk pada jaringan akan dianalisa berdasarkan data rules yang telah ditentukan pada saat konfigurasi suricata.

3.1. Perancangan Topologi

Rancangan topologi jaringan ini dibuat sebagai desain atau sebagai Gambar perancangan sistem jaringan yang akandigunakan pada network intrusion detection and prevention system pada Universitas Dehasen Bengkulu. Adapun rancangan topologi yang akan digunakan pada jaringan ini dapat dilihat pada Gambar 3.

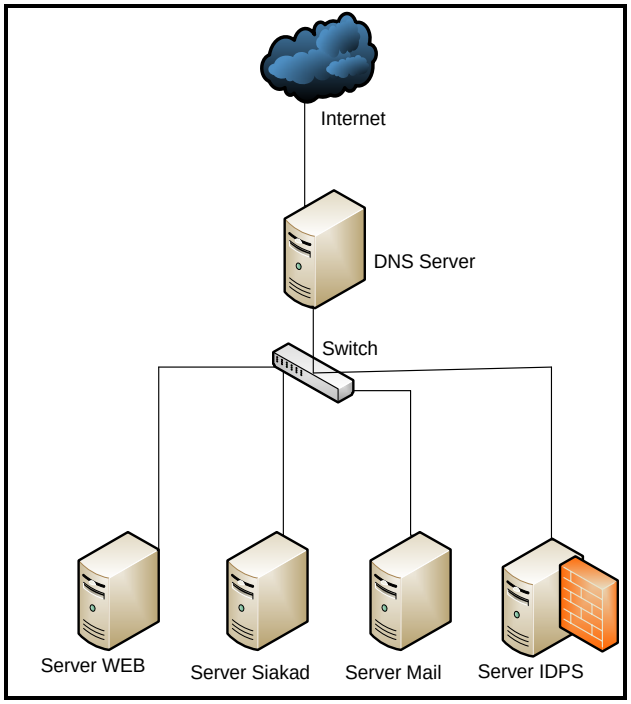
3.2. Perancangan Desain Proses

Desain proses dalam perancangan server intrusion detection and prevention system Universitas Dehasen Bengkulu dimodelkan dalam bentuk model diagram use case. Use case model diagram ini menggambarkan proses perancangan dari tahap instalasi sampai dengan tahap pengujian sistem. Use case model diagram perancangan sistem IDPS dapat dilihat pada Gambar 4 *use case* model diagram.

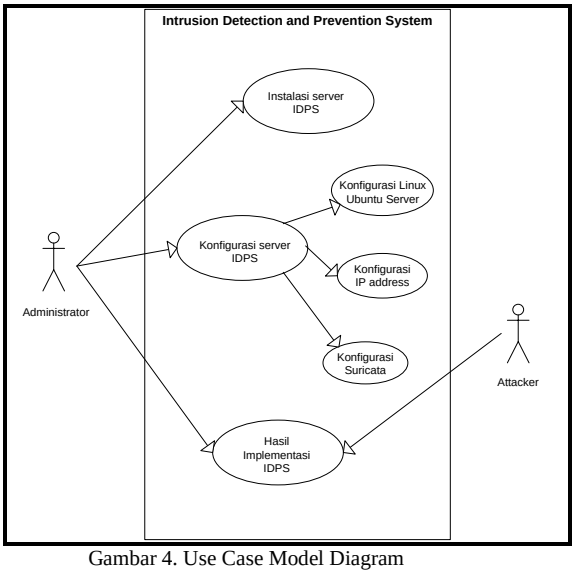
3.3. Perancangan Interface Web

Perancangan interface web dibuat untuk menampilkan hasil dari deteksi serangan yang berada pada log suricata. Pada aplikasi ini terdapat tiga tampilan interface yaitu halaman login, halaman beranda, dan halaman log serangan.Pertama merancangan halaman login ini merupakan form yang harus diisi oleh administrator untuk dapat mengakses menu dan fitur yang ada di dalam web. Pada halaman login ini administrator harus menginputkan username dan password.

Kedua merancang halaman beranda yang berfungsi untuk menampilkan beberapa widget dan juga grafik yang berisi mengenai informasi jumlah serangan yang terjadi pada jaringan, baik berdasarkan waktu (hari, minggu, bulan dan tahun), berdasarkan protocol, dan berdasarkan port yang diserang. Selanjutnya perancangan yang ketiga yaitu merancang halaman log serangan yang menampilkan detail serangan yang terjadi pada network, dimana pada halaman log serangan ini akan ditampilkan berdasarkan timeline waktu serangan terbaru.



Gambar 3. Rancangan Topologi



Gambar 4. Use Case Model Diagram

3.4. Perancangan Interface Web

Perancangan interface web dibuat untuk menampilkan hasil dari deteksi serangan yang berada pada log suricata. Pada aplikasi ini terdapat tiga tampilan interface yaitu halaman login, halaman beranda, dan halaman log serangan.

Pertama merancangan halaman login ini merupakan form yang harus diisi oleh administrator untuk dapat mengakses menu dan fitur yang ada di dalam web. Pada halaman login ini administrator harus menginputkan username dan password.

Kedua merancang halaman beranda yang berfungsi untuk menampilkan beberapa widget dan juga grafik yang berisi mengenai informasi jumlah serangan yang terjadi pada jaringan, baik berdasarkan waktu (hari, minggu, bulan dan tahun), berdasarkan protocol, dan berdasarkan port yang diserang.

Selanjutnya perancangan yang ketiga yaitu merancang halaman log serangan yang menampilkan detail serangan yang terjadi pada network, dimana pada halaman log serangan ini akan ditampilkan berdasarkan timeline waktu serangan terbaru.

3.5. Tahapan Proses Kerja IDPS

Tahapan-tahapan yang dilakukan pada sistem IDPS yang digunakan untuk mendeteksi dan mencegah lalulintas data yang mencurigakan. Menentukan Rules IDPS: Data rules yang telah ditentukan diinputkan pada sistem IDPS. Pada dasarnya rules telah tersedia pada saat instalasi suricata. Karena pada penelitian ini yang digunakan adalah rules yang berkaitan dengan protocol ftp dan telnet, maka hanya rules tersebut yang digunakan. Untuk menginputkan rules yang digunakan dapat dilakukan denga cara ketik /etc/suricata/rules.

Detection: Untuk dapat mendeteksi adanya serangan pada jaringan, langkah selanjutnya adalah menjalankan suricata dalam mode inline. Adapun cara untuk menjalankan suricata dapat dilakukan dengan cara ketik perintah dibawah ini pada terminal server IDPS.

suricata -c /etc/suricata/suricata.yaml -i enp0s15

Proses Pencocokan Rules: Setelah rules dan proses detection dijalankan, maka proses yang dilakukan pada sistem IDPS selanjutnya yaitu mencocokan rules yang terdapat pada directory /etc/suricata/rules dengan paket data yang terdeteksi sebagai serangan yang masuk pada jaringan. Apabila paket data tersebut cocok maka akan tersimpan pada log.

Penyimpanan Data Pada Log: Ketika proses pencocokan rules berhasil, selanjutnya mesin IDPS suricata akan menyimpan file semua rekaman alert dan kegiatan lalulintas pada jaringan di sebuah directory /var/log/suricata. Fileyang tersimpan dalam default log dir /var/log/suricata, dapat dibuka menggunakan program yang mendukung format file pcap.

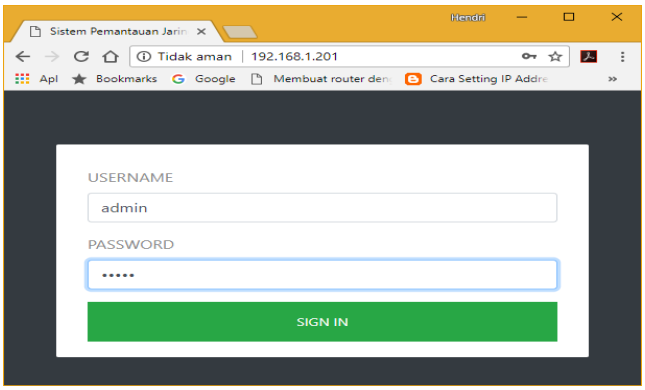
3.6. Hasil

Untuk hasil deteksi akan masuk pada log suricata yang telah ditetapkan. Adapun hasil deteksi dapat dilihat pada directory /var/log/suricata. Pada directory suricata terdapat ada beberapa jenis log, tetapi hasil deteksi akan masuk pada file eve.json. Adapun contoh hasil deteksi pada log serangan dapat diinput kedalam Tabel 1 hasil deteksi.

Berdasarkan Tabel 1 hasil deteksi dapat dijelaskan bahwa pada kolom times tamp merupakan keteran dari waktu terjadinya percobaan serangan, pada source ip adalah identitas dari ip address yang digunakan oleh attacker untuk melakukan penyusupan pada system

Tabel 1. Hasil Deteksi

Times Tamp	Source IP	Src Port	Dest IP	Dest Port	Event Name
Monday, March 05 2018	192.168.115.1	-	192.168.115.133	-	ICMP Detection
Monday, March 05 2018	192.168.115.133	-	192.168.115.1	-	ICMP Detection
Monday, March 05 2018	192.168.115.1	-	192.168.115.133	-	ICMP Detection
Monday, March 05 2018	192.168.115.133	-	192.168.115.1	-	ICMP Detection
Monday, March 05 2018	192.168.115.133	-	192.168.115.1	-	ICMP Detection
Monday, March 05 2018	192.168.115.1	-	192.168.115.133	-	ICMP Detection
Monday, March 05 2018	192.168.115.133	-	192.168.115.1	-	ICMP Detection
Monday, March 05 2018	192.168.115.1	-	192.168.115.133	-	ICMP Detection

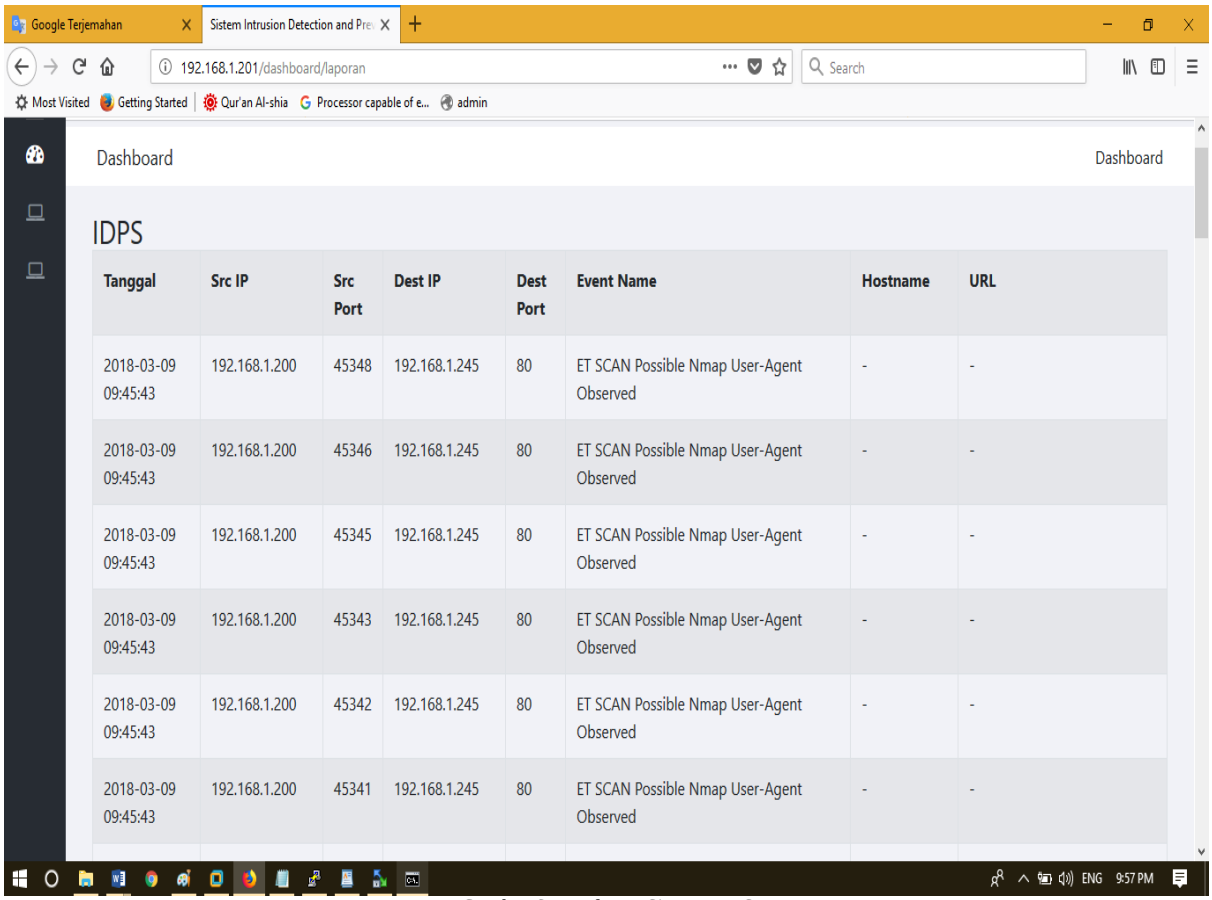


Gambar 5. *Form Login* Sistem IDPS

3.7. Hasil Tampilan Web GUI

Setelah melakukan pengujian, selanjutnya untuk melihat hasil dari deteksi yang dilakukan oleh sistem keamanan IDPS dapat dilihat secara realtime dalam bentuk web interface. Untuk langkah-langkah yang digunakan untuk melihat hasi dari deteksi ini. *Login* digunakan ntuk dapat melihat hasil dari log sistem keamanan IDPS ini, langkah pertama yang harus dilakukan adalah akses ip address sistem keamanan IDPS menggunakan browser. Setelah sistem dapat diakses selanjutnya inputkan username dan password kemudian klik tombol login. Adapun form login yang digunakan seperti pada Gambar 5. Hasil *Log IDPS* Untuk melihat hasil dari deteksi sistem keamanan IDPS klik laporan pemantauan.

Berdasarkan Gambar 6 terlihat hasil dari deteksi sistem keamanan IDPS terdapat percobaan port scanning. Hal ini dikarenakan adanya alert yang masuk pada log sistem keamanan IDPS. Pertama tanggal terjadinya proses percobaan port scanning yaitu pada tanggal 09-03-2018 pada pukul 09:45:43 WIB. Kedua Source ip atau ip addres yang digunakan penyusup untuk melakukan portscanning adalah 192.168.1.200 dengan source port 4534 Ketiga *destination* ip adalah ip addres yang menjadi target penyusup yang dalam halini ip address yang digunakannya adalah 192.168.1.245 dengan port tujuan 80yang masuk pada sistem keamanan IDPS. Keempat Event name adalah pesan yang dikirimkan oleh sistem keamanan IDPS bahwa adanya percobaan port scanning menggunakan Nmap.



Gambar 6. Hasil *Log Sistem IDPS*

4. Kesimpulan

Berdasarkan pada pembahasan dan pengujian yang dilakukan pada analisa keamanan jaringan menggunakan intrusion detection and prevention system (IDPS), maka dapat ditarik suatu kesimpulan, Pertama konsep kerja dari sistem IDPS dalam keamanan sebuah jaringan komputer adalah mendeteksi dan mencegah adanya serangan yang masuk pada sistem jaringan komputer melalui port scanning, akses telnet dan ftp. Sistem Keamanan IDPS dapat di implementasikan dan dapat melindungi komputer / host yang terhubung pada jaringan. Administrator Sistem keamanan jaringan IDPS dapat mengontrol lalu lintas data yang masuk pada jaringan komputer.

Sistem keamanan IDPS dapat mendeteksi dan memblokir adanya serangan yang masuk pada jaringan. Hal ini dapat di lihat ketika pengujian sistem keamanan IDPS dilakukan. Dari pengujian tersebut paket data yang terdeteksi sebagai penyusup pada lalu lintas jaringan masuk pada log sistem dan dapat ditampilkan pada web GUI.

Untuk peneliti selanjutnya dapat menerapkan sistem keamanan jaringan menggunakan aplikasi lainnya selain suricata dan coba menerapkan dengan menggunakan metode host IDPS agar dapat mengamankan host tersebut secara langsung tanpa melalui keamanan jaringan.

Daftar Pustaka

[1] N. Alip, I. Fitri, and N. D. Nathasia, “Network Monitoring System Data Radar Penerbangan berbasis PRTG dan ADSB,” vol. 3, no. 3, pp. 127–134, 2018.

[2] L. A. Network, “Intrusion Detection Prevention System (IDPS) pada Local Area Network (LAN),” vol. 8, no. 1, pp. 24–42, 2015.

[3] D. Lumena, A. Anton, and E. R. Nainggolan, “Analisa Dan Perancangan Jaringan Private Cloud Computing Berbasis Web Eyeos,” *None*, vol. 13, no. 1, pp. 1–8, 2016.

[4] N. Fahriani, P. A. R. Devi, and D. Aditama, “Alternatif Penanganan Jenis Serangan Pencurian Data Pada Jaringan Komputer,” *Pros. Semin. Nas. Teknol. dan Rekayasa Inf. Tahun 2017*, no. November, pp. 19–24, 2017.

[5] F. Ridho, A. Yudhana, and I. Riadi, “Analisis Forensik Router Untuk Mendeteksi Serangan Distributed Danial of Service (DDoS) Secara Real Time,” vol. 2, no. 1, pp. 111–116, 2016.

[6] A. Yasin and I. Mohidin, “Dampak Serangan

DDoS pada Software Based Openfow Switch di Perangkat HG553," *J. Technopreneur*, vol. 6, no. 2, p. 72, 2018.

[7] I. Suryadinata, S. Ismail, and M. Rizal, "Implementasi Firewall Dan Ids Pada Smoothwall Express," vol. 1, no. 2, p. 48, 2015.

[8] S. Khadafi, B. D. Meilani, and S. Arifin, "Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System)," *J. IPTEK*, vol. 21, no. 2, p. 67, 2017.

[9] R. Mentang, A. A. E. Sinsuw, X. B. N. Najoan, and J. T. Elektro-ft, "Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System," vol. 5, no. 7, pp. 35–44, 2015.

[10] J. Jabez and B. Muthukumar, "Detection Approach," *Procedia - Procedia Comput. Sci.*, vol. 48, no. Iccc, pp. 338–346, 2015.

[11] F. Arsin, M. Yamin, and L. Surimi, "Implementasi Security System Menggunakan Metode Idps (Intrusion Detection And Prevention System) Dengan Layanan Realtime Notification," vol. 3, no. 2, pp. 39–48, 2017.

[12] E. S. J. Atmadji, B. M. Susanto, and R. Wiratama, "Pemanfaatan IPTables Sebagai Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) Pada Linux Server," *Teknika*, vol. 6, no. 1, pp. 19–23, 2017.

[13] K. Wong, C. Dillabaugh, N. Seddigh, and B. Nandy, "Enhancing Suricata Intrusion Detection System for Cyber Security in SCADA Networks," pp. 1–5, 2017.

[14] F. B. Perdana, I. R. Munadi, and A. I. Irawan, "IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN SURICATA DAN NTOPNG IMPLEMENTATION OF NETWORK SECURITY SYSTEM USING SURICATA AND NTOPNG," vol. 6, no. 2, pp. 4076–4083, 2019.

[15] Y. Ariyanto and B. Harijanto, "Implementasi Suricata Pada Server CLOUD PROXMOX VE Sebagai Intrusion Detection System (IDS) Dalam Pengamanan Jaringan," vol. 3, pp. 178–189, 2017.

[16] E. P. Nugroho, E. Nugraha, and M. N. Zulfikar, "Sistem Reporting Keamanan pada Jaringan Cloud Computing Melalui bot Telegram dengan Menggunakan Teknik Intrussion Detection and Prevention System," vol. 5, no. 2, pp. 49–57, 2019.