Vol 1 (2020) No 2

Jitsi Jurnal Ilmiah Teknologi Sistem Informasi

http://jurnal-itsi.org ISSN 2722-4619 (Print) ISSN 2722-4600 (Online)

Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server

Elsa Stephani[#], Fitri Nova[#], Ervan Asri[#]

[#] *Jurusan Teknologi Informasi, Politeknik Negeri Padang, Padang, 25164, Indonesia*
E-mail: elsastephani380@gmail.com, fitrinova@pnp.ac.id, ervan@pnp.ac.id

A B S T R A C T S

The defense system against servers is generally still done manually by administrators. To overcome this, we need a system that functions to inform threats that occur optimally and be resolved quickly. The IDS network security system was developed using Suricata. Suricata itself will be built using OPNsense. With the Suricata system using OPNsense, it can detect or prevent incoming attacks.

K A T A K U N C I

Suricata,
IDS,
OPNsense

A B S T R A K

Sistem pertahanan terhadap server umumnya masih dilakukan secara manual oleh administrator. Untuk mengatasi hal ini, maka dibutuhkan sebuah sistem yang berfungsi untuk menginformasikan ancaman yang terjadi secara optimal dan diatasi dengan cepat. Maka dikembangkanlah sistem keamanan jaringan IDS menggunakan Suricata. Suricata sendiri akan dibangun menggunakan OPNsense. Dengan adanya sistem Suricata menggunakan OPNsense ini, dapat mendeteksi maupun mencegah serangan yang masuk.

1. PENDAHULUAN

Sistem pertahanan terhadap server masih banyak yang tergantung secara manual kepada admininistrator, sehingga membuat integritas sistem menjadi tergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi. Apabila gangguan tersebut telah berhasil membuat server down atau jaringan menjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara remote. Sehingga administrator tidak dapat melakukan pemulihan jaringan dengan cepat. Administrator membutuhkan suatu sistem yang dapat menginformasikan ancaman yang terjadi secara optimal dan dapat diatasi dengan cepat. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem.

Suricata merupakan IDS yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan rules yang telah ada. Cara kerja dari suricata adalah ketika adanya penyerangan suricata akan melakukan pengecekan paket/serangan yang ada melalui rules yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat log serangan yang dilakukan.

Paper ini membahas tentang Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server di Jurusan Teknologi Informasi Politeknik Negeri Padang. Didukung oleh jurnal (Dwi Kuswanto : 2014) dengan judul "Kerja Intrusion Prevention Sistem (IPS) Berbasis Suricata Pada Jaringan Lokal Area Network Laboratorium TIA+ Teknik Informatika, Universitas Trunojoyo" 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 [1].

Selanjutnya didukung oleh jurnal (Muhammad Ravis, dkk : 2019) dengan judul "Perbandingan Performansi Single Web Server dan Multi Web Server dengan Metode Paired Sample T Test" [2]. Didukung juga oleh buku dengan judul "Kali Linux Revealed Mastering the Penetration Testing Distribution Book [3]." Jurnal dari (Ziyad

R. Al Ashhab, dkk. : 2019) dengan judul "Detection of HTTP Flooding DDoS Attack using Hadoop with MapReduce : A Survey" [4].

Selanjutnya, ada jurnal dari (Raharja, R. Anton. Yunianto, Afri. Widyantoro, Wisesa : 2001) dengan judul "Open Source Campus Agreement – Modul Pelatihan "ADMINISTRASI SISTEM LINUX" [5]. Dan jurnal dari (Sarifin, Agus dan Astuti, Bhekti Ratna Timur : 2012) dengan judul "Penerapan Router PfSense Berbasis Free BSD di Warnet Emax Sragen" [6]. Serta jurnal dari (Bagas Suryo Anggoro dan, Wiwin Sulistyo : 2019) dengan judul "Implementasi Instrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi" [7]. Dan yang terakhir ada penelitian dari (Inayah Nur : 2008) dengan judul penelitian "Pengembangan Firewall Pada Wireless Network Dengan Sistem Operasi GNU Linux [8]."

Alasan diadakan penelitian ini

- Mendapatkan hasil dari sistem kerja Suricata untuk membuat sebuah sistem IDS yang dapat mendeteksi ancaman pada webserver
- Mengimplementasikan rules ke sistem IDS Suricata untuk pendeteksian serangan dengan metode Web Penetration Testing dengan tools Skipfish dan Dirbuster dan DDoS dengan tools Slowloris.

Pertanyaan tujuan

- Bagaimana membuat rules yang efektif agar dapat menangkap ancaman serangan diserver dengan Suricata dalam berbentuk log file?
- Apa pengaruh penerapan Suricata rules yang ada pada web server dimana IDS diimplementasikan?
- Apa yang dihasilkan dari pengujian penyerangan menggunakan metode Web Penetration Testing dengan tools Skipfish, Dirbuster?
- Apa yang dihasilkan dari pengujian penyerangan menggunakan metode DDoS dengan Slowloris?

2. METODOLOGI PENELITIAN

1. Teknik Pengumpulan Data.
   a. Observasi

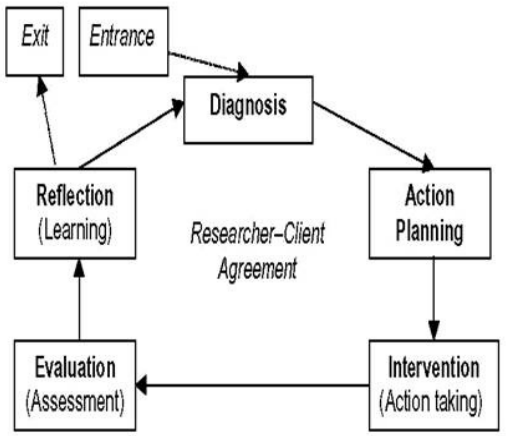
Pengumpulan data dengan observasi langsung dengan pengamatan langsung adalah cara pengambilan data dengan menggunakan mata tanpa ada pertolongan alat standar lain untuk keperluan tersebut. Pada metode ini melakukan pengujian terhadap Sistem Operasi OPNsense dan mencatat hasil penyerangan ke server yang sudah diberi keamanan oleh Suricata.

   b. Studi Pustaka

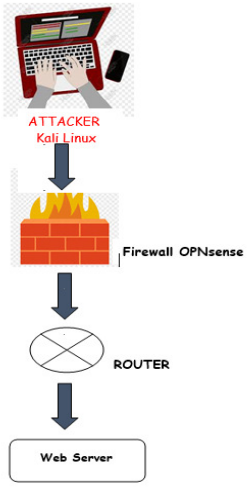
Studi kepustakaan merupakan langkah yang penting dimana setelah seseorang peneliti menetapkan topik penelitian, langkah selanjutnya adalah melakukan kajian yang berkaitan dengan teori yang berkaitan dengan topik penelitian. Studi pustaka yang di lakukan adalah mencari jurnal referensi di internet serta mengunjungi perpustakaan untuk mencari buku-buku yang berhubungan dengan masalah yang akan diteliti.

2. Metode Penelitian.

Menurut Davison, Martinson & Kock dalam Mukmin (2017), menyebutkan penelitian tindakan sebagai metode penelitian, didirikan atas asumsi bahwa teori dan praktek dapat secara tertutup diintegrasikan dengan pembelajaran dari hasil intervensi yang direncanakan setelah diagnosis yang rinci terhadap konteks masalahnya. Terlihat tahapan Metode Action Research pada Gambar 1 [9].



GAMBAR 1. Tahapan Action Research



GAMBAR 2. Skema Perancangan Sistem IDS Suricata

1. Diagnosis
   Pada tahapan ini penulis mengidentifikasi permasalahan mengenai serangan pada *web server*.
2. Action Planning
   Pada tahapan ini penulis melakukan pemahaman terhadap alat apa saja yang dibutuhkan yaitu :
   a. Software *OPNsense* yang sudah memiliki paket *Suricata* berfungsi sebagai Intrusion Detection System yang akan mendeteksi serangan apa yang akan datang ke *web server* yang telah disediakan.
   b. Rules file *suricata* dipasang di software Intrusion Detection System, *suricata* file rules tersebut berfungsi sesuai rules apa yang akan dipasang untuk mendeteksi serangan ke *web server* tersebut.
   c. Laptop Penyerang.
3. Intervention (Action Taking)
   Tahap ini juga peneliti mulai melakukan serangan menggunakan tools yang telah disiapkan dan mengkonfigurasi IDS *Suricata* yang telah disiapkan setelah selesai penguji akan menuliskan bagaimana System *Suricata* bekerja untuk mendeteksi serangan.
4. Evaluation (Assessment)
   Bagian tahap ini penulis mengumpulkan hasil dari penyerangan yang ada di log *Suricata* dan penulis juga mengevaluasi apakah *Suricata* dapat mendeteksi serangan tersebut.
5. Reflection (Learning)
   Pada tahap ini penulis mendapatkan hasil dari pengujian serangan tersebut apakah *suricata* dapat mendeteksi serangan tersebut. Disini juga ditambah *rule* untuk meningkatkan keamanan *suricata* tersebut.

3. HASIL DAN PEMBAHASAN

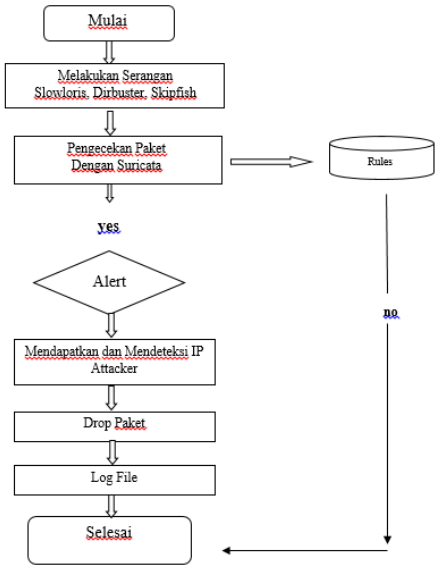
Hasil dan pembahasan mencakup penjelasan dari metode penelitian. Pada tahap analisis menekankan pada proses pencarian diintensifkan dan difokuskan pada software. Dimana dari analisis didapatkan bahwa adanya kelemahan dari sistem untuk mendeteksi serangan pada jaringan. Web Server membutuhan sistem keamanan yang dapat melindungi segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak ketiga. Tahap desain menerapkan rancangan dari beberapa hal yang dibutuhkan pada tahapan sebelumnya sebagai konfigurasi dari aplikasi/sistem [10].

Gambar 2 merupakan skema perancangan IDS dimana penyerang berada dibagian luar dari Web Server, Serangan dapat masuk melalui internet kemudian masuk ke router yang kemudian akan dilakukan pengecekan oleh sistem IDS Suricata. Serangan tersebut akan dilakukan pengecekan sistem IDS dengan dua cara yang pertama signature-based yaitu dengan pecocokan lalu lintas jaringan dengan basis data yang berisi cara serangan dan penyusupan yang sering dilakukan oleh penyerang. Anomaly-based merupakan cara kedua yaitu dengan membandingkan pola serangan yang sering terjadi dengan pola serangan yang sedang dipantau. IDS yang digunakan ialah Suricata pada sistem operasi Kali Linux yang bertujuan untuk melindungi real server, client server dan jaringan dibawahnya. Suricata memerlukan package maupun library untuk membangun Suricata, selain itu dibutuhkan package untuk rules Suricata karena IDS akan bekerja sesuai dengan rules yang dibuat, rules disini sangat penting dari Suricata yang berupa script yang dapat mengenali tindakan penyusupan yang sedang terjadi pada jaringan yang dipasang sistem IPS. IPS menggunakan firewall untuk block paket yang sesuai dengan rules yang dibuat.

Dalam membangun sebuah jaringan ataupun server, langkah pertama kali yaitu menentukan bagaimana bentuk dari topologi yang akan digunakan, Berikut adalah bentuk dari topologi yang akan dibangun :

GAMBAR 3. Topologi Keamanan Jaringan IDS Menggunakan Suricata Pada Web Server

Dari topologi diatas dapat dijelaskan bahwa disini diperlukan 3 komponen penting yaitu OPNsense sebagai router sekaligus firewall yang mana akan mendeteksi serangan yang berasal dari Kali Linux. Kali Linux disini berfungsi sebagai attacker atau penyerang yang mana IP Address dari Kali Linux 192.168.30.2 dan IP Address dari OPNsense 192.168.20.1. Serta, objek yang akan diserang adalah Web Server dimana IP Address dari Web Server 192.168.20.2. Metode pengujian yang akan digunakan ada 2 dan memiliki 3 tools yaitu, metode DDoS dengan tools Slowloris, dan metode Web Penetration Testing dengan tools Dirbuster dan Skipfish

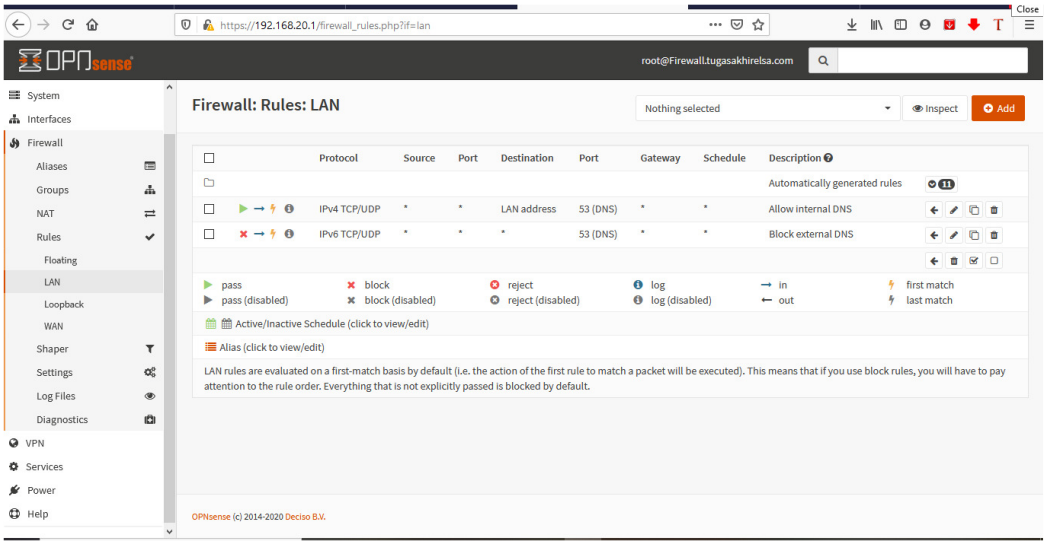


GAMBAR 4. Flowchart Sistem IDS Suricata

Flowcart diatas menjelaskan mengenai cara kerja sistem IDS *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* akan membuat alert dan Log File [11].

Pada *OPNsense* disediakan rules dimana pada rules inilah dapat mengatur bagaimana *Suricata* dapat bekerja user dapat mengatur rules *Suricata* untuk memblokir atau mengizinkan serangan yang masuk ke *Web Server*.

Untuk interface LAN ada 2 rules yang digunakan yaitu allow untuk internal DNS, sedangkan satu lagi memblock external DNS. Maksudnya adalah *Suricata* mengizinkan akses melalui internal DNS, dan memblock segala jenis akses yang berasal dari luar DNS

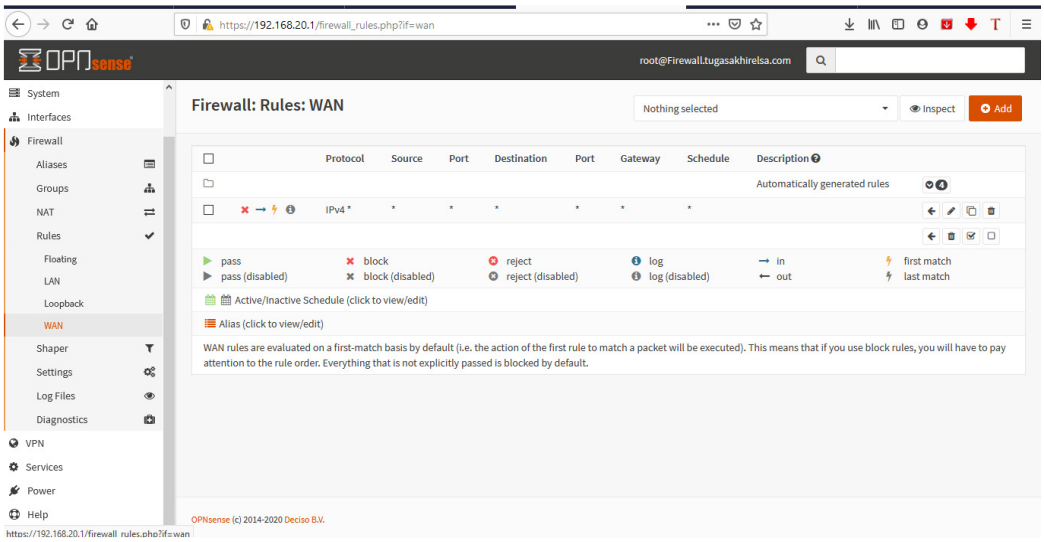


GAMBAR 5. Mengatur rules pada interface LAN

Untuk interface WAN hanya memiiliki satu rules saja yang mana memblok segala jenis serangan yang berasal dari *interface* WAN. Setelah mengatur Rule yang ada dilanjutkan untuk melakukan pengetesan menggunakan Kali Linux dengan Tools Dirbuster, Skipfish dan Slowloris.Untuk mengetahui sistem yang dibangun dapat berjalan sesuai perancangan. Diperlukan pengujian-pengujian sebagai berikut :

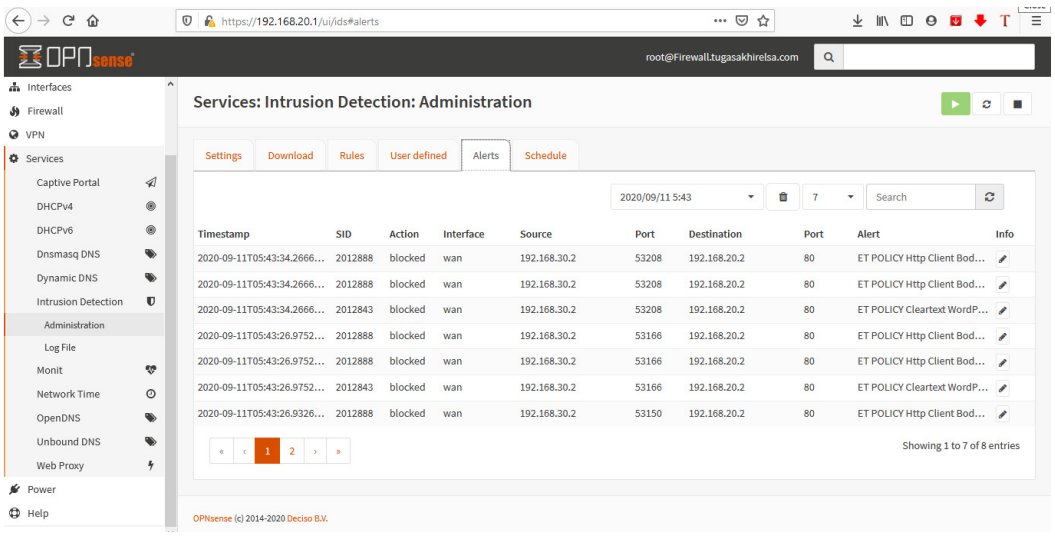
a. Pengujian menggunakan tools Slowloris
   1. Melakukan pengetesan menggunakan kali linux. Dengan metode DDoS dengan tools Slowloris
   2. Terlebih dahulu mendownload slowloris.pl di https://github.com/Ogglas/Orignal-Slowloris-HTTP-DoS/blob/master/slowloris.p.
   3. Buka terminal, lalu ketikkan “perl slowloris.pl”
   4. Dan, selanjutnya mengetikan perintah “perl slowloris.pl –dns 192.168.20.2 (alamat server atau web server yang akan diserang)”
   5. Setelah itu suricata melalui firewall OPNsense, mendapatkan log serangan yang menyerang web server tersebut.

6. Di suricata yang ada di OPNsense di ketahuilah bahwa terjadi penyerangan atau tidak, melalui alert dan log file yang tersedia



GAMBAR 6. Mengatur rules pada interface WAN

b. Pengujian menggunakan tools Dirbuster
   1. Membuka tools dirbuster pada sistem operasi Kali Linux.
   2. Mengisi IP dari web server yang akan di serang.
   3. Browse dan pilih file daftar kata (biasanya terletak di / usr / share / dirbuster / wordlists) yang ingin digunakan untuk brute force
   4. Setelah itu suricata melalui firewall OPNsense, mendapatkan log serangan yang menyerang web server tersebut.
   5. Di suricata yang ada di OPNsense di ketahuilah bahwa terjadi penyerangan atau tidak, melalui alert dan log file yang tersedia.

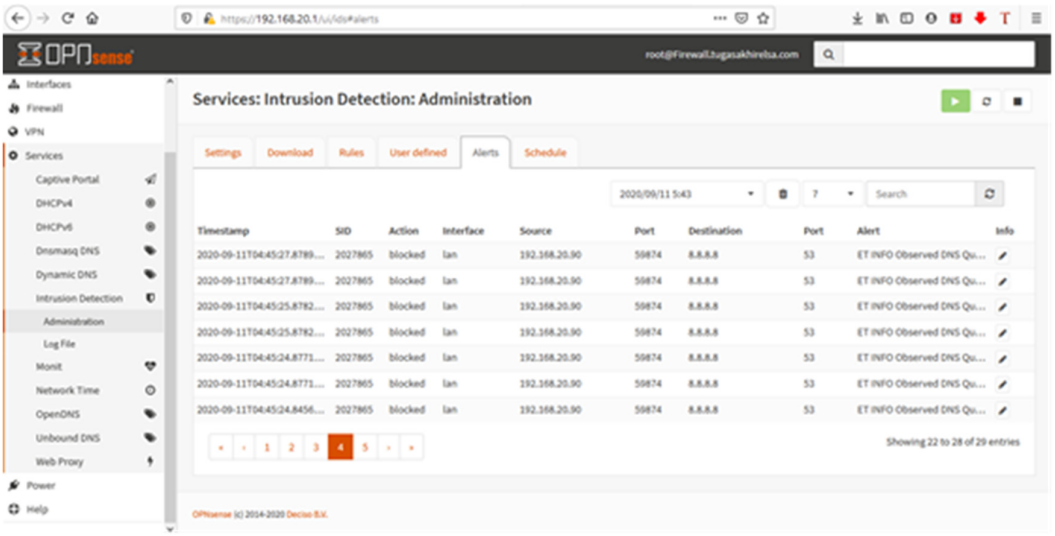


GAMBAR 7. Hasil Alert dari interface WAN yang di block oleh Suricata

c. Pengujian menggunakan tools Skipfish
   1. Membuka terminal lalu mengetikkan skipfish –h.

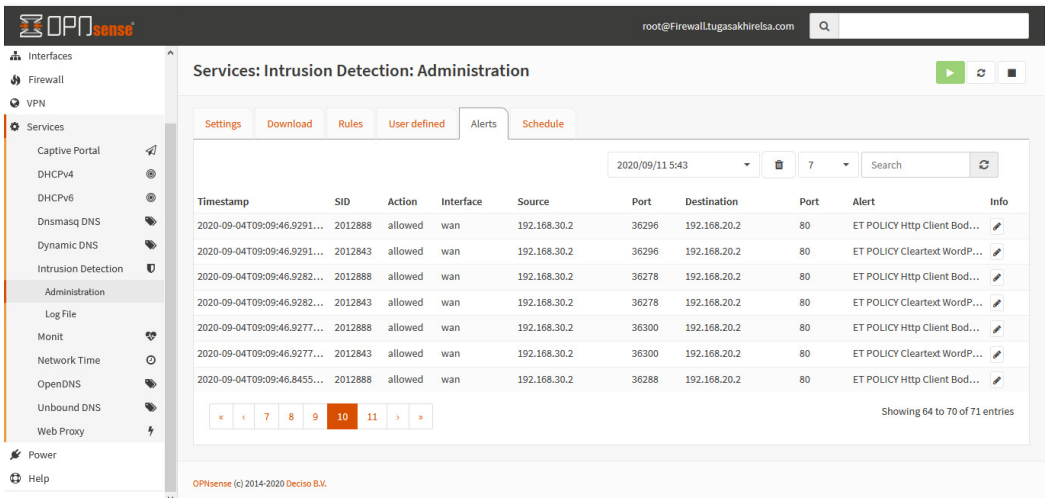
2. Setelah itu membuat folder baru untuk menampung informasi yang dicoba diretas dari web server oleh skipfish. Dengan perintah *skipfish –o elsa http://192.168.20.2.*
3. Setelah melakukan scanning, maka buka "index.html" yang mana sudah ada di dalam folder yang dibuat sebelumnya. Disana terdapat berbagai informasi dari web server tujuan.

Dapat dilihat bahwa Suricata mampu melakukan deteksi dan melakukan block dari serangan yang masuk ke Web Server sesuai dengan rule yang telah dibuat. Disini alert yang dicatat sesuai dengan rule yang telah dibuat, pada gambar dibawah ini merupakan bukti bahwa Suricata telah memblock serangan yang berasal dari interface WAN atau melalui interface WAN. Serangan yang berasal dari luar DNS interface LAN, maka Suricata akan langsung melakukan blocked.



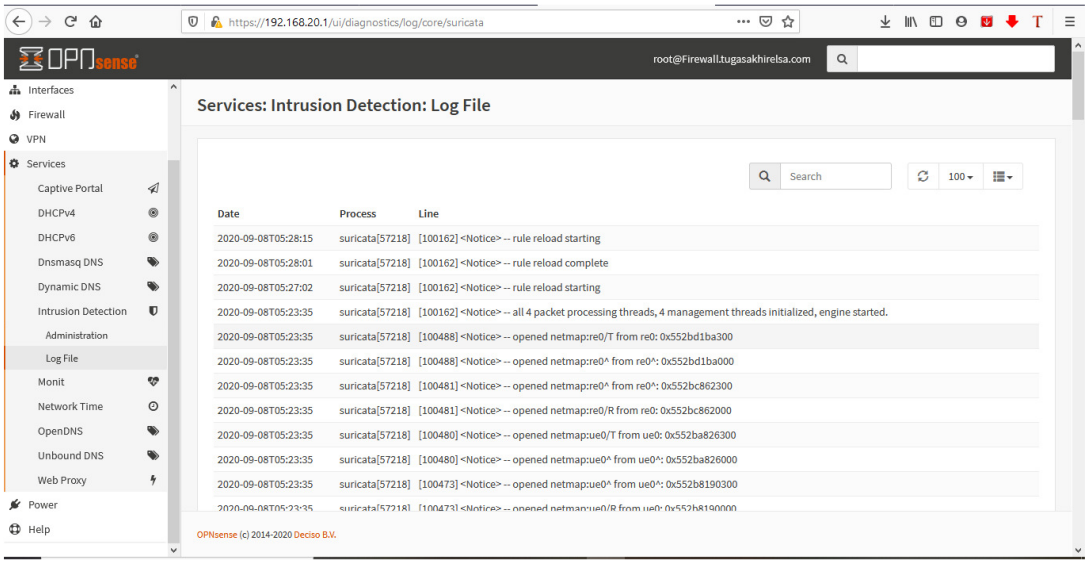
GAMBAR 8. Hasil Alert dari interface LAN yang di block oleh Suricata

Dan Suricata mampu melakukan deteksi dan mengizinkan serangan masuk ke Web Server. Jika pada rule di setting secara "Pass" atau "Allow"



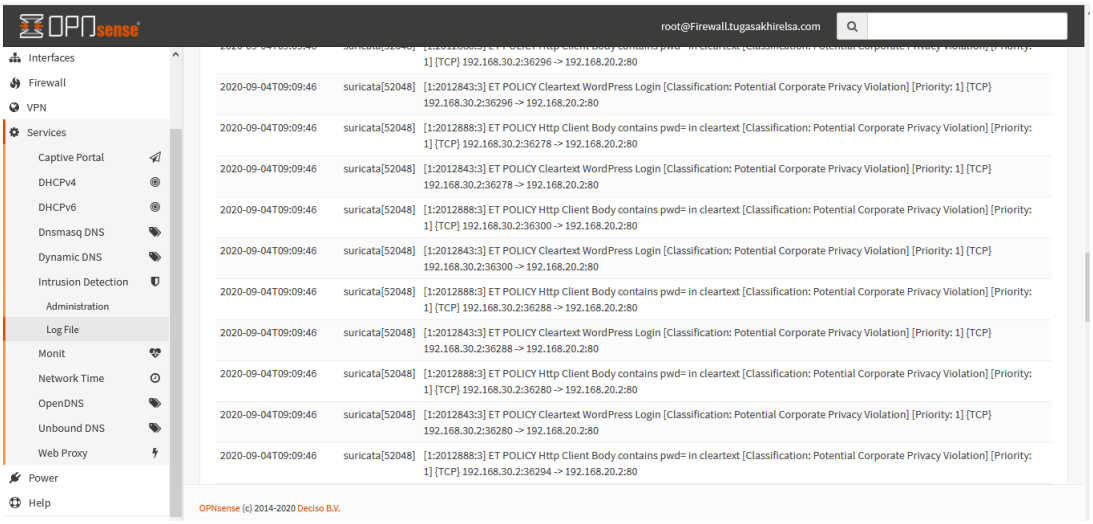
GAMBAR 9. Hasil Alert dari interface WAN yang di allow oleh Suricata

Serta *Suricata* juga akan menerima beberapa Log File yang mana pada Log File inilah user mengetahui rentenan kejadian apa saja yang telah terjadi dan dilakukan oleh *Suricata*



GAMBAR 10. Hasil dari Log File IDS Suricata

Lanjutan dari hasil Log File yang diterima oleh Suricata. Pada log file inilah tercatat log atau aktifitas dari sebuah serangan yang menyerang Web Server. Pada log file inilah diketahui rule Suricata apa saja yang berjalan dalam melakukan deteksi terhadap serangan serta menunjukan usaha penjebolan keamanan yang dilakukan.



GAMBAR 11. . Lanjutan dari Log File IDS Suricata

Suricata dapat melakukan deteksi sesuai dengan rules yang telah dibuat, dan hasil akhir dari pengujian IDS menggunakan *Suricata* adalah mendapatkan Log File serta Alert dari serangan yang masuk ke *Web Server*

4. KESIMPULAN

IDS (Intrusion Detection System) menggunakan Suricata dapat memonitoring traffic pada web server dan menyimpan hasil deteksi dan pencegah jika ada penyusup yang memasuki webserver. Serta dapat mengetahui apabila terdapat aktifitas mencurigakan masuk ke log Suricata.

Implementasi Suricata dengan firewall OPNsense dapat mendeteksi dan mencegah anomali pada web server dari penyusup. Pengimplementasian Intrusion Detection System (IDS) menggunakan Suricata pada web server di Jurusan Teknologi Informasi Politeknik Negeri Padang dapat digunakan untuk membantu memberikan informasi terkait deteksi adanya serangan web scanning dengan memanfaatkan tools dirbuster dan skipfish, serta

penggunaan slowloris dari metode DDoS yang diterapkan untuk pengetesan serangan pada Intrusion Detection System (IDS) Suricata. Dan, Suricata tidak memiliki shared object rules seperti software intrusi lainnya

REFERENSI

[1] D. Kuswanto, "Kerja Intrusion Prevention Sistem (IPS) Berbasis Suricata Pada Jaringan Lokal Area Network Laboratorium TIA+ Teknik Informatika, Universitas Trunojoyo," Jurnal Ilmiah Nero, vol. 01 No. 02, 2014.
[2] d. Muhammad Ravis, "Perbandingan Performasi Single Web Server dan Multi Web Server dengan Metode Paired Sample T Test," 2019.
[3] Kali Linux Revealed Mastering the Penetration Testing Distribution Book.
[4] d. Ziyad R. Al Ashhab, "Detection Of HTTP Flooding DDoS Attack Using Hadoop with MapReduce," 2019.
[5] R. A. d. Raharja, "Open Source Campus Agreement-Modul Pelatihan "Administrasi Sistem Linux"," 2001.
[6] A. d. A. B. R. T. Sarifin, "Penerapan Router PFsense Berbasis FreeBSD di Warnet Emax Sragen," 2012.
[7] B. S. A. d. W. Sulistyo, "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi," 2019.
[8] I. Nur, "Pengembangan Firewall Pada Wireless Network dengan Sistem Operasi GNU Linux," 2008.
[9] Mukmin, "Tahapan Action Research," 2017.
[10] W. F. d. G. N. Fanthoni, "Deteksi Penyusupan Pada Jaringan Komputer Menggunakan IDS Snort, E-Proceeding Of Engineering," vol. 3, pp. 1169-1172, 2006.
[11] B. S. d. W. S. Anggoro, "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Gramedia Informasi," Seminar Nasional APTIKOM, 2019.