KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 3, No 4, Februari 2023
Hal 323-329
https://djournals.com/klik

Prototype Sistem Deteksi Serangan Pada Server Samsat Menggunakan Intrusion Detection System (IDS) Berbasis Snort

Meli Pitriyanti[1], Nelly Khairani Daulay[1], Satrianansyah[2,*], M. Agus Syamsul Arifin[1]

[1] Fakultas Ilmu Teknik, Program Stud Rekayasa Sistem komputeri, Universitas Bina Insan, Kota Lubuklinggau, Indonesia
[2] Fakultas Ilmu Teknik, Program Studi Sistem Informasi, Universitas Bina Insan, Kota Lubuklinggau, Indonesia
Email: [1]1902010055@mhs.univbinainsan.ac.id, [2] nellykhairanilestari@gmail.com, [3,*] satrianansyah@univbinainsan.ac.id., [4]mas.arifin@univbinainsan.ac.id
Email Penulis Korespondensi: satrianansyah@univbinainsan.ac.id.

Abstrak−Permasalahan dari penelitian ini adalah belum adanya sistem keamanan server samsat terhadap serangan syn-flooding, sehingga diperlukan sebuah sistem yang dapat mendeteksi serangan syn-flooding. Pada Metode penelitian menggunakan metode survei dan observasi dimana informasi dikumpulkan dari responden melalui wawancara langsung dengan pengelola kantor dan pengelola server samsat. Hasil penelitian ini menunjukkan bahwa sistem berbasis Snort yang dirancang untuk mendeteksi serangan syn-flooding agar dapat mendeteksi serangan syn-flooding tersebut. Dari sini dapat disimpulkan bahwa sistem ini dapat bekerja dengan baik sebagai langkah awal proteksi server untuk mendeteksi serangan syn flood pada server Samsat.

Kata Kunci: Snort; Serangan; Sistem; Server; Syn-flooding

Abstract− Problems from study This is Not yet exists system security server samsat to attack syn-flooding, so that is required Asystem Which can detect attack syn-flooding. On Method study use method survey and observation Where information collected from respondents through interview direct with manager office and manager server samsat. Results study This show that system based Snort Which designed for detect attack syn-flooding so thatcan detect attack syn-flooding the. From here can concluded that system This can Work with Good as steps early protection server for detect attack his flood on server Samsat.
Keywords: Snort; Attack; System; Server; Syn-flooding

1. PENDAHULUAN

Karena keamanan jaringan informasi sebagai bagian dari sistem informasi sangat penting untuk menjaga keakuratan dan keutuhan informasi serta menjamin ketersediaan layanan kepada penggunanya. Sistem harus dilindungi dari semua jenis serangan dan upaya penyusupan oleh orang yang tidak berhak[1].

Kantor Sistem Administrasi Satu Atap atau yang lebih dikenal dengan Samsat Empat di Kabupaten Lawang merupakan sebuah instansi pemerintah yang menyelenggarakan pajak jalan raya yang transparan dan transparan kepada masyarakat. Keterbukaan dalam organisasi tentunya memiliki strategi pelayanan untuk mencapai visi dan misi organisasi. Implementasinya membutuhkan transparansi dan kerjasama dari semua peserta dalam pelaksanaan proses pelayanan[2]. Pengelolaan pelayanan perkantoran Samsat Kabupaten Empat Lawang menggunakan server Samsat sebagai pusat pengelolaan pelayanan masyarakat. Server ini penuh dengan informasi penting tentang pembayaran kendaraan di Kabupaten Empat Lawang.

Permasalahan di kantor samsat kabupaten empat lawang adalah server samsat tidak terlindungi dari serangan pihak-pihak yang tidak bertanggung jawab yang dapat menyebabkan kerusakan samsat di kabupaten empat lawang, baik itu kehilangan data atau kemudian data rusak. pelayanan kepada masyarakat[3]. Berdasarkan hal tersebut diperlukan suatu sistem untuk mendeteksi serangan pada server Samsat Kabupaten Empat Lawang untuk mencegah serangan dari pihak yang tidak bertanggung jawab dan mengamankan server Samsat dengan IDS (Intrusion Detection System) dengan Snort untuk mendeteksi serangan[4][5].

Sebagai solusi dari permasalahan yang ada, penulis merumuskan masalah bahwa samsat empat lawang membtuhkan sistem deteksi intrusi server samsat empat lawang, yang menggunakan sistem deteksi intrusi 'IDS'. berbasis Snort untuk mencegah serangan terhadap server oleh pihak yang tidak bertanggung jawab yang dapat mengakibatkan kerugian bagi Samsat Empat Lawang [6]. Tujuan umum penelitian ini adalah untuk memenuhi salah satu syarat penulisan tesis sarjana (S-1) pada mata kuliah Teknik Sistem Komputer Fakultas Ilmu Komputer Universitas Bina Insan Lubuklinggau, Secara keseluruhan, tujuan dari penelitian ini adalah untuk membuat sistem deteksi intrusi server Samsat Empat Lawang menggunakan IDS (Intrusion Detection System) berbasis Snort, Manfaat pengembangan keilmuan merupakan cara mengembangkan ilmu untuk meningkatkan pelayanan publik Samsat Empat Lawang, yang dapat dijadikan tolak ukur dalam penelitian sejenis dan sebagaia Pengujian sistem menggunakan pengujian fungsional, yaitu. Server Ubuntu sebagai server dan Linux sebagai penyerang sistem.

2. METODOLOGI PENELITIAN

2.1 Metode Pengumpulan Data

a. Observasi

Metode observasi adalah cara pengumpulan data melalui pengamatan langsung terhadap subjek yang akan diteliti. Dalam mengumpulkan data-data yang diperlukan untuk penelitian ini, penulis melakukan observasi langsung ke kantor Samsat Empat Lawang.

b. Wawancara

Penulis mewawancarai dan merespon langsung kantor Samsat Empat Lawang dari server Samsat Empat Lawang.

c. Studi literatur

Bentuk pencarian informasi dengan membaca/mengambil informasi dari buku, majalah ilmiah, buku dan juga dengan menggunakan internet sebagai sumber informasi, melihat informasi yang disediakan oleh website, forum diskusi, mailing lis, dan lain-lain.

2.2 Metode Pengembangan Sistem

a. Identifikasi

Fase pertama ini dilakukan untuk mengetahui berbagai masalah keamanan yang dihadapi jaringan saat ini dan bagaimana sistem saat ini bekerja di perusahaan.

b. Analisis

Dari informasi yang diperoleh pada tahap identifikasi, dilakukan proses analisis kebutuhan pengguna.

c. Desain

Pada tahap desain ini dibuat gambar desain topologi untuk sistem keamanan yang akan dibangun, dijelaskan alur sistem autentikasi, dan dijelaskan kebutuhan sistem untuk perangkat lunak dan perangkat keras.

d. Implementasi

Pada fase ini, hasil perencanaan dari fase sebelumnya diimplementasikan. Dikarenakan keterbatasan kewenangan perusahaan dalam melaksanakan implementasinya. hasil desain disimulasikan dalam jaringan yang lebih kecil. Dimulai dengan menginstal perangkat dan mengonfigurasi perangkat lunak dan perangkat keras yang diperlukan.

e. Audit

Pada fase ini, sistem yang disimulasikan diuji secara sistematis untuk memastikan bahwa sistem keamanan yang diterapkan sesuai dengan tujuan awalnya. Langkah ini dilakukan dengan skenario pengujian.

f. Evaluasi

Pada fase ini, hasil pengujian yang dilakukan dievaluasi sejauh mana efektivitas teknologi keamanan yang dibangun dapat dicapai dan dibandingkan dengan tujuan awal dan kondisi ideal yang diharapkan. Hasil analisis menjadi titik awal untuk perbaikan sistem dan sebagai saran untuk perbaikan di masa mendatang[7].

2.3 Analisis Kebutuhan Dan Analisis Sistem

a. Analisis Kebutuhan

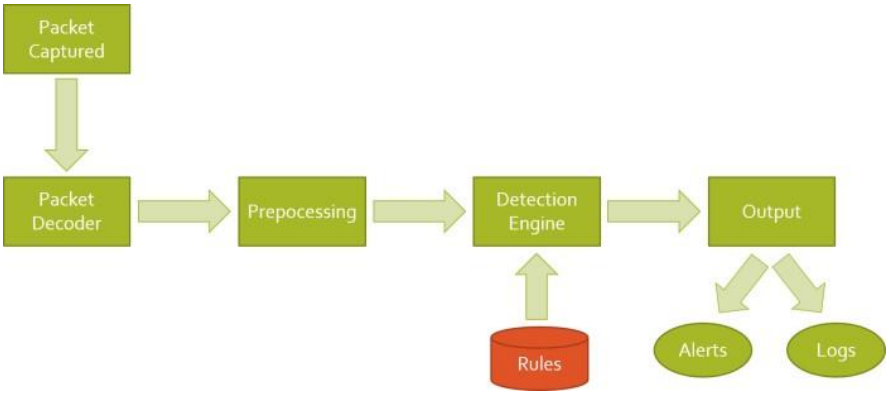
Penulis menganalisis kantor SAMSAT di Kabupaten Empat Lawang. memperkenalkan pajak kendaraan yang transparan kepada masyarakat. keterbukaan dalam organisasi tentunya memiliki strategi pelayanan untuk mencapai visi dan misi organisasi. Implementasinya membutuhkan transparansi dan kerjasama dari semua peserta dalam pelaksanaan proses pelayanan[8]. Pengelolaan pelayanan kantor Samsat Kabupaten Empat Lawang menggunakan server Samsat sebagai pusat pengelolaan pelayanan masyarakat. Server ini penuh dengan informasi penting tentang pembayaran kendaraan di Kabupaten Empat Lawang. Permasalahan di kantor samsat kabupaten empat lawang adalah server samsat tidak terlindungi dari serangan pihak-pihak yang tidak bertanggung jawab yang dapat menyebabkan kerusakan samsat di kabupaten empat lawang, baik itu kehilangan data atau kemudian data rusak[9]. pelayanan kepada masyarakat. Sebagai solusi dari permasalahan tersebut, sistem yang dapat mendeteksi serangan ping-flooding pada server Empat Lawang mengharapkan adanya kerusakan server yang berujung pada hilangnya layanan SAMSAT Empat Lawang.

b. Analisis Sistem

Berdasarkan analisis kebutuhan sistem yang telah dijelaskan di atas, maka diperlukan suatu sistem yang dapat mendeteksi serangan pada server Samsat Kabupaten Empat Lawang yaitu sistem yang dirancang untuk Intrusion Detection System (IDS)[10]. Didukung oleh SNORT, Snort adalah program NIDS (Network Intrusion Detection System) yang mendeteksi lalu lintas jaringan dan aktivitas paket secara real time. Snort melakukan analisis protokol dan konten yang mirip dengan model serangan yang ada.

Snort memiliki beberapa mode diantaranya:

a. Packet Sniffer - Membaca paket dari jaringan dan menampilkannya sebagai aliran berkelanjutan di layar konsol
b. Packet Logger - Merekam semua paket yang melewati jaringan untuk analisis selanjutnya
c. Mode Deteksi Serangan - Dalam mode ini, Snort mendeteksi serangan yang terjadi melalui jaringan komputer. Untuk menggunakan mode IDS, beberapa aturan harus ditentukan yang memisahkan paket normal dari paket serangan.



Gambar 1. Alur IDS Menggunakan SNORT

a. *Packet Capture*
Packet Capture merupakan proses memisahkan paket data yang melalui Ethernet card untuk selanjutnya digunakan oleh snort.

b. *Packet Decoder*
Packet Decoder adalah prose mengambil data di layer 2 hasil dari packet capture. Pertama akan dipisahkan data link seperti ethernet dan token ring kemudian protocol IP dan selanjutnya paket TCP dan UDP. Setelah pemisahan data selesai, snort telah mempunyai informasi protocol yang dapat diproses lebih lanjut

c. *Preprocessing*
Preprocessing adalah tahap analisis atau manipulasi terhadap paket sebelum dikirim ke detection engine. Manipulasi paket dapat berupa ditandai, dikelompokkan, atau bahkan dihentikan.

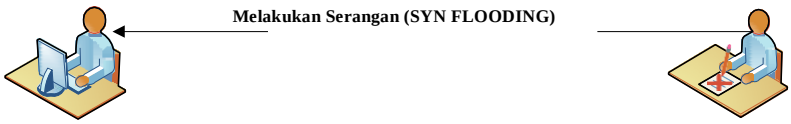
d. *Detect Engine*
Detcet Engine adalah proses packet akan dibandingkan dengan rule yang telah ditetapkan sebelumnya. Rule tersebut berisi tanda-tanda (signature) yang termasuk serangan

e. Rules Database Signature
Rules Database Signature adalah Kumpulan ruleset yang disimpan di dalam database snort sebagai perbandingan untuk memeriksa paket yang masuk ke jaringan

f. Output
Output yang dihasilkan dapat berupa report dan alert Ada banyak variasi output yang dihasilkan snort.

2.6 Pengujian Sistem

Pengujian dilakukan menggunakan metode eksperimental untuk mendeteksi serangan banjir SYN dengan benar pada sistem Snort. Pengujian dilakukan dengan SYN banjir dijalankan oleh mesin klien.



Server Samsat (Ubuntu + Snort) **Attacker (Kali Linux)**

Gambar 2. Alur pengujian sistem

Tabel 1. Komponen Pengujian Sistem

No	Komponen Pengujian	Proses Pengujian	Hasil Pengujian
1	Komputer server	Kinerja *Snort* pada IDS.	Snort dapat mendeteksi serangan yang dilakukan *client*.
2	Komputer Client	Melakukan *Syn flood* ke komputer *server*.	Paket-paket data yang berisi serangan *Syn flood*.

3. HASIL DAN PEMBAHASAN

3.1 Gambaran Umum Samsat Empat Lawang

SAMSAT adalah singkatan dari Sistem Administrasi Manunggal Terpadu Satu Pintu. Menurut Peraturan Presiden Nomor 5 Tahun 2015 tentang Penyelenggaraan SAMSAT, SAMSAT sendiri merupakan sekumpulan sistem yang menjalankan tugas-tugas BBNKB, Pendaftaran dan Tanda Pengenal Kendaraan Bermotor (Ranmor Regident). dan pembayaran wajib untuk Asuransi Kecelakaan dan Angkutan Jalan (SWDKLLJ)[11].

Berkembangnya SAMSAT tidak terlepas dari misinya yang terbagi menjadi tiga instansi administratif dan disebut Tim Pembina SAMSAT. Pertama, ada tim dari Dinas Pajak Daerah (Dispenda) yang bertanggung jawab atas administrasi pajak kendaraan. Kedua, Direktorat Lalu Lintas Kepolisian Daerah (Ditlantas Polda) yang menjalankan fungsi Regident Ranmor[12]. Terakhir, PT Jasa Raharja (Persero) bertanggung jawab mengelola SWDKLLJ. Dulu, perpanjangan Surat Tanda Nomor Kendaraan (STNK) selalu memakan waktu yang sangat lama. Karena itu, pemilik kendaraan harus mengunjungi tiga kantor terpisah.

Untuk membayar pajak jalan, mereka harus datang ke kantor pajak setempat untuk mengurusnya. Setelah itu, mereka juga harus membayar di kantor asuransi SWDKLLJ., mereka masih harus melapor ke polisi lalu lintas sebelum akhirnya bisa mendapatkan perpanjangan STNK[13]. Hingga akhirnya pada tahun 1974 dilakukan percobaan untuk membentuk perpanjangan SAMSAT. Kantor SAMSAT pertama adalah Polda Metro Jaya di DKI Jakarta.

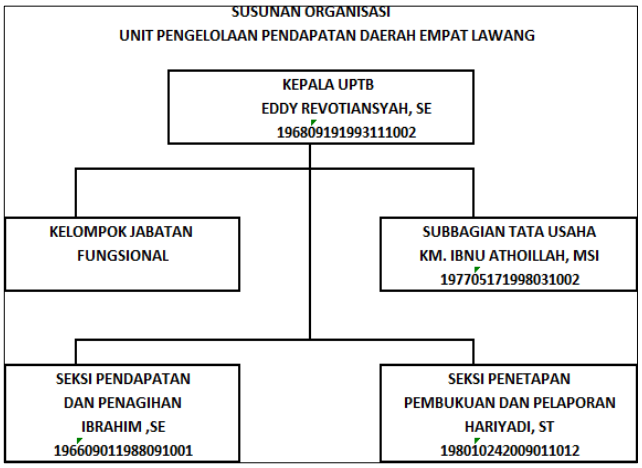
Tujuannya agar Regident Ranmor lebih mudah dioperasikan dan merekam informasi driver dengan lebih akur. Pada tahun 1976, SAMSAT diresmikan di seluruh Indonesia berdasarkan Surat Perintah Bersama (INBERS) oleh tiga menteri, yaitu Menhankam (Menteri Pertahanan dan Keamanan), Menteri Keuangan (Menkeu) dan Menteri Dalam Negeri (Mendagri). Di bawah naungan Polri, PT Jasa Raharja (Persero) dan Ditjen Pajak Provinsi.

3.1.1 Visi Dan Misi

Visi Samsat Empat Lawang adalah : “Demi Mencapai Pelayanan Optimal Untuk Kepuasan Masyarakat” Visi Samsat Empat Lawang:

a. Meningkatkan kinerja seluruh jajaran KPPD untuk mendukung kualitas pelayanan masyarakat.
b. Meningkatkan kualitas pelayanan untuk meningkatkan pendapatan daerah.
c. Pengetahuan, keterampilan, dan sikap karyawan terus dikembangkan.
d. Memberikan pelayanan yang memuaskan kepada seluruh pelanggan internal dan eksternal

3.1.2 Struktur Organisasi



Gambar 3. Struktur Organisasi

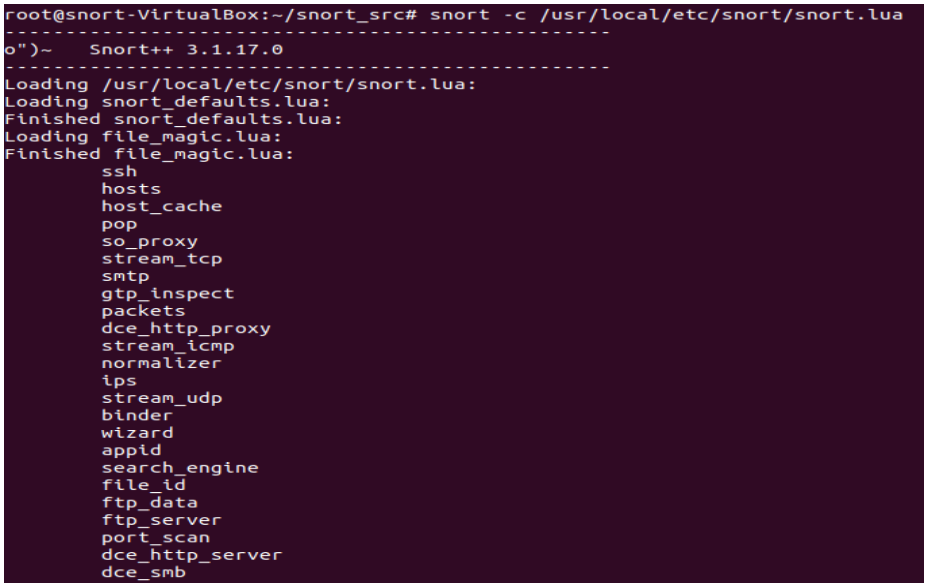
3.2 Hasil Penelitian

Hasil penelitian selama enam bulan Samsat Empat Lawang, hasil yang diperoleh adalah penulis mengembangkan sistem deteksi serangan syn-flood berbasis Snort. Sistem legacy yang sebelumnya dioperasikan di lokasi ini belum memiliki sistem yang mampu mendeteksi serangan syn flooding sehingga rentan terhadap penyerang. Dalam hal ini sistem diimplementasikan sebagai langkah pengamanan awal terhadap Empat Lawang, terhadap serangan Syn Flooding server Samsat.

3.3 Hasil Instalasi Snort

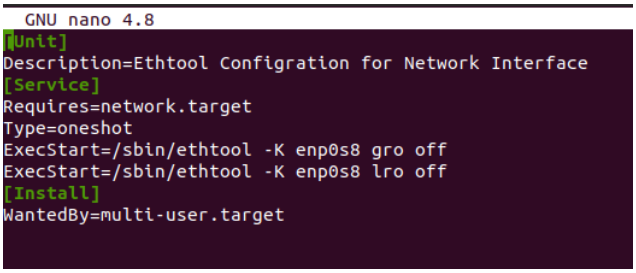
Untuk tahap pertama dari adalah hasil instalasi snort 3 dapat ditunjukkan pada gambar berikut:

Gambar 4. Hasil Instalasi Snort

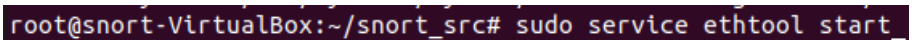


Gambar 5. Pengujian Hasil Insatalasi

Gambar 5. dan gambar 6. menunjukkan konfigurasi perangkat ethernet yang akan di monitor atau diawasi oleh snort dan mengaktifkannya[14].

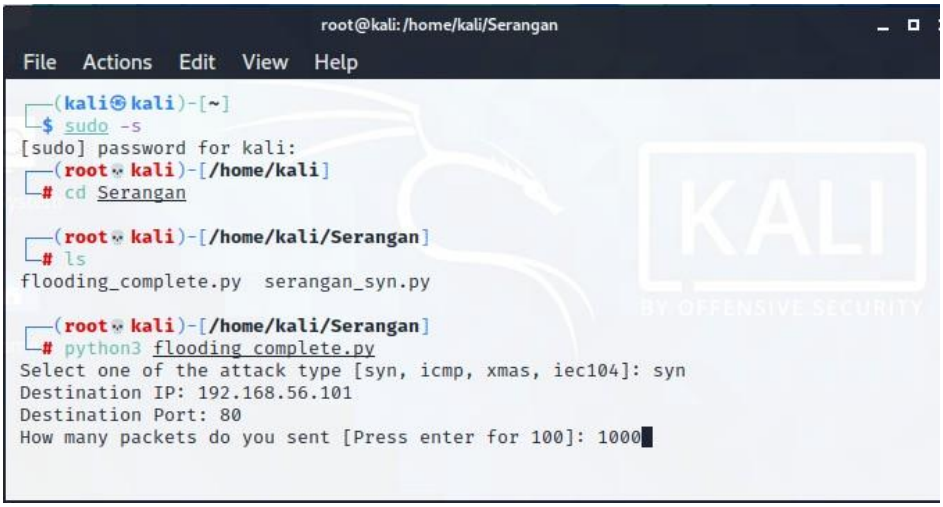


Gambar 6. Pengaturan Perangkat *Ethernet*



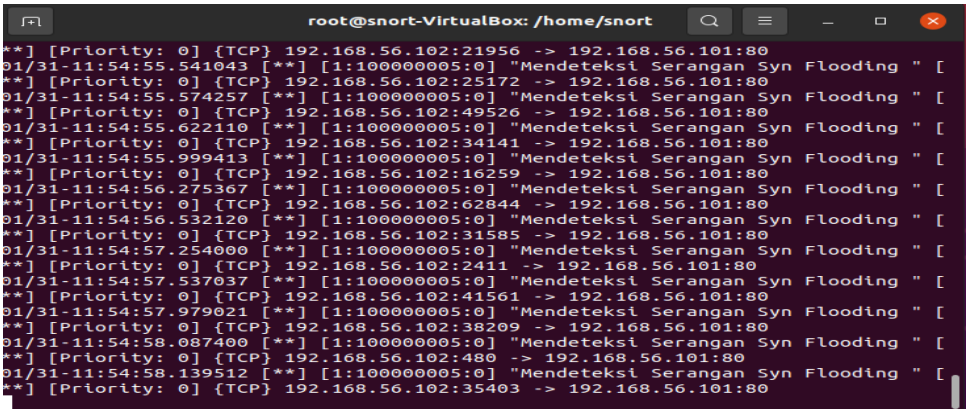
Gambar 7. Aktifasi Perangkat *Ethernet*

Gambar 7 menunjukkan direktori untuk menyimpan *rule* snort, *rule* ini digunakan untuk menyimpan perintah pada snort dalam mendeteksi serangan yang sudah didefinisikan.



Gambar 8. Serangan *Syn Flood* Dari Kali Linux

Gambar 8 memperlihatkan proses penyerangan dari komputer penyerang ke server Ubuntu dengan mengirimkan 1000 paket syn. Serangan syn-flood menggunakan paket data protokol TCP yang dikirim secara massal, menyebabkan server menerima paket data ekstra sehingga mencegah orang lain mengakses server[15].



Gambar 9. *Rule* Snort Deteksi *Syn Flooding.*

Rule atau aturan yang penulis buat pada komputer server untuk mendeteksi *Syn flooding* adalah dengan mendeteksi paket data TCP yang berlebihan, dan melewati ethernet yang sudah dimasukkan dalam pengaturan snort untuk diawasi[16].

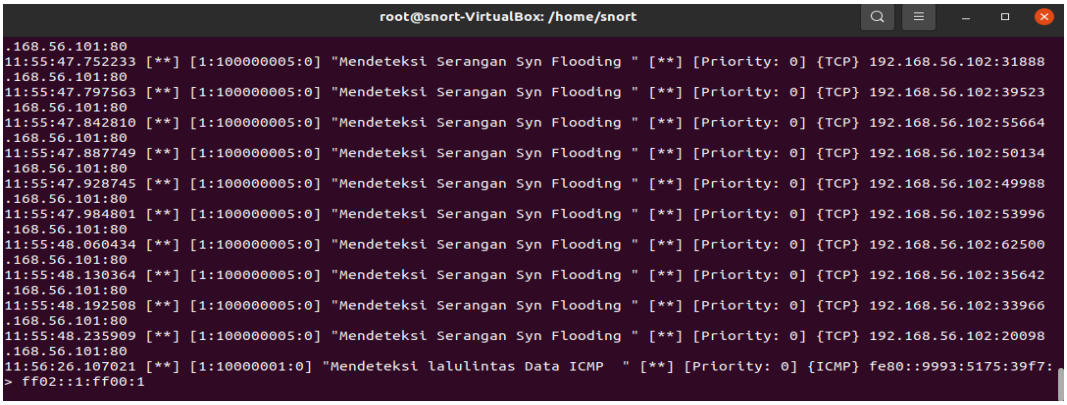
3.4 Pengujian Sistem

Pengujian sistem dilakukan menggunakan dua buah PC komputer, satu komputer sebagai server menggunakan sistem operasi Linux Ubuntu, dan komputer lainnya sebagai *attacker* menggunakan sistem operasi Kali Linux[17].

Gambar 10 dan 11 menunjukkan penggunaan *rule* untuk mendeteksi serangan *syn flooding* dan hasil deteksi serangan *syn flooding* pada *server*

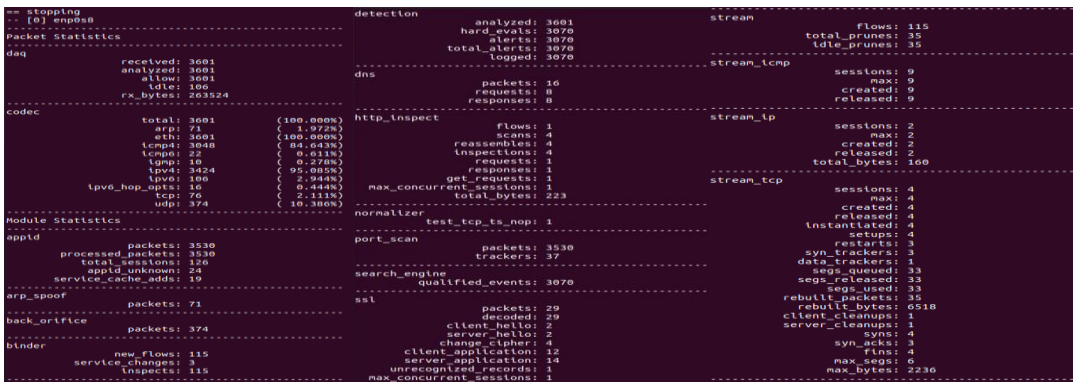
```
root@snort-VirtualBox:~/snort_src# sudo snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules \
> -i enp0s8 -A alert_fast -s 65535 -k none
```

Gambar 10. *Penerapan* Rule *Snort* Deteksi *Syn Flooding* Secara *Real Time*



Gambar 11. Hasil Deteksi Serangan Syn Flooding Secara Real Time

Gambar 11 menunjukkan statistik hasil deteksi *syn flooding* secara *real time* menggunakan *snort*. Dari gambar 11 tersebut dapat dilihat *IP Address* dari komputer penyerang yaitu 192.168.56.102 dengan serangan syn yang membanjiri lalu lintas data di *protocol TCP* port 80.



Gambar 11. Hasil Deteksi Serangan *Syn Flooding*

Dari pengujian yang telah dilakukan maka dapat ditarik kesimpulan sistem deteksi serangan *syn flooding* dapat mendeteksi serangan tersebut secara *real time.*

4. KESIMPULAN

Dari kegiatan yang telah kami lakukan ini maka kami menyimpulkan ada beberapa hal yang perlu menjadi perhatian kita diantaranya adalah Perlu dibangunnya sistem pendeteksi serangan syn-flood di Samsat Empat Lawang untuk mencegah serangan dari pihak yang tidak bertanggung jawab. Oleh karena itu, penulis memanfaatkan SNORT menjadi sistem pendeteksi serangan syn-flood pada jaringan server Samsat Empat Lawang.

REFERENCES

[1] T. Pangestu, R. Liza, P. Studi, T. Informatika, and U. H. Medan, "ISSN 2338-5677 Cetak ISSN 2548-6646 Online Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing ISSN 2338-5677 Cetak ISSN 2548-6646 Online," vol. 10, no. 2, pp. 60–67, 2022.

[2] A. W. Oki Kurniawan, Pribadi Widodo, "Eksperimen Perancangan Kemampuan Daya Serap Panel Akustik dari Sampah Kotak Karton Gelombang," *J. ITENAS Rekarupa*, vol. 3, no. 1, pp. 1–8, 2016.

[3] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[4] M. Mahmud and M. Hasnawi, "Implementasi Bot Telegram Untuk Monitoring Jaringan Dengan Pendekatan Security Policy Development Life Cycle Pada Kementerian Kelautan dan Perikanan Untia," vol. 3, no. 2, pp. 127–133, 2022.

[5] D. Kurnia, "PEMANFAATAN BETTERCAP SEBAGAI TEKNIK SNIFFING PADA PAKET TRAFIK JARINGAN WIFI," pp. 83–85.

[6] F. Nurohman, S. Ratnasari, R. Gunawan, F. Maulana, S. Nursuwars, and U. Siliwangi, "RANCANG BANGUN PROTOTYPE," vol. 5, no. 2, pp. 106–114.

[7] B. Santoso, A. Sobri, L. Sunardi, and B. Santoso, "KEPADA SATPOLPP KOTA LUBUKLINGGAU," vol. 7, no. 1, pp. 68–78, 2022.

[8] S. Pada and P. D. Devi, "PERENCANAAN SISTEM INFORMASI BERBASIS WEB UNTUK SISTEM PERSEDIAAN DAN SISTEM PEMESANAN PRODUK JADI KONVEKSI," vol. 3, no. 2, pp. 2788–2794, 2016.

[9] D. Wijayanti, N. Lestari, N. K. Daulay, D. Wijayanti, N. Lestari, and N. K. Daulay, "PROTOTYPE SISTEM MONITORING PARKIR PINTAR BERBASIS IOT (IINTERNET OF THINGS)," vol. 7, no. 2, pp. 123–131, 2022.

[10] W. Fathoni, G. N. Nurkahfi, P. I. Komputasi, and F. Informatika, "DETEKSI PENYUSUPAN PADA JARINGAN KOMPUTER MENGGUNAKAN IDS," vol. 3, no. 1, pp. 1169–1172, 2016.

[11] F. Teknik, U. N. Surabaya, J. T. Informatika, F. Teknik, U. N. Surabaya, and A. Point, "MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS Achmad Rizal Fauzi I Made Suartana Abstrak."

[12] D. M. Informatika, F. Teknik, and U. N. Surabaya, "DETEKSI PAKET SNIFFING PADA WIRELLES MENGGUNAKAN ARP WATCH Aditya Ariyanto Asmunin Abstrak," vol. 8, pp. 178–181, 2018.

[13] M. Ulfa, "IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) DI JARINGAN UNIVERSITAS BINA DARMA," no. 12, pp. 27–42, 2009.

[14] A. Akhriana and A. Irmayana, "Web App Pendeteksi Jenis Serangan Jaringan Komputer dengan Memanfaatkan Snort Dan Log Honeypot," vol. 12, no. 1, pp. 87–98, 1978.

[15] U. M. Surakarta and B. A. Nugroho, "ANALISIS KEAMANAN JARINGAN PADA FASILITAS INTERNET (WIFI) TERHADAP SERANGAN PACKET SNIFFING," 2012.

[16] N. KURNIASIH, D. P. SARI, and D. A. RIZKA FIRDAUS, "Rancang Bangun Prototype Sistem Monitoring Pendeteksi Dini Banjir Berbasis Short Message Service Menggunakan PLTS On Grid," *Kilat*, vol. 10, no. 1, pp. 77–88, 2021, doi: 10.33322/kilat.v10i1.1018.

[17] O. I. Sanjaya, I. A. D. Giriantari, and I. N. S. Kumara, "Perancangan Sistem Pompa Irigasi Pembangkit Listrik Tenaga Surya (PLTS) Untuk Pertanian Subak Semaagung," vol. 6, no. 3, pp. 114–121, 2019.