OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

Implementasi Internet Provider Dengan Metode *Intrusion Detection System* Dan *Simplewall* Untuk Mencegah Serangan Ddos

Hafizh Kurnia[1*], Riswal Hanafi Siregar[1]

[1]Fakultas Teknik, Teknik Informatika, Universitas Pamulang, Jl. Raya Puspiptek No. 46, Kel. Buaran, Kec. Serpong, Kota Tangerang Selatan. Banten 15310, Indonesia
Email: [1*]hafizhkurnia98@gmail.com, [2]dosen00268@unpam.ac.id
(* : coressponding author)

Abstrak– *Distributed Denial of Services* (DDOS) merupakan salah satu jenis eksploitasi kelemahan pada sebuah *web*. DDOS merupakan upaya serangan terhadap *server* di dalam jaringan internet dengan cara membanjiri banyak data pada lalu lintas jaringan untuk mengganggu jalannya lalu lintas normal pada *server*. *Intrusion Detection System* (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. *Simplewall* adalah perangkat lunak komputer yang digunakan sebagai *firewall* untuk memberikan perlindungan secara total terhadap setiap akses yang tidak dikehendaki. *Intrusion Detection Systems* (IDS) dan *Simplewall* sebagai pencegah adanya penyusup pada *server* jaringan komputer bahkan serangan DDOS sekaligus.

Kata Kunci: *Intrusion Detection System*, *Snort*, *Simplewall*, DDOS

Abstract*– Distributed Denial of Services (DDOS) is one type of exploitation of weaknesses on a web. DDOS is an attack attempt against a server on the internet network by flooding a lot of data on the network traffic to disrupt normal traffic on the server. Intrusion Detection System (IDS) is a system that can detect suspicious activity in a system or network. Simplewall is computer software that is used as a firewall to provide total protection against any unwanted access. Intrusion Detection Systems (IDS) and Simplewall as a deterrent to intruders on computer network servers and even DDOS attacks at once.*

Keywords*: Intrusion Detection System, Snort, Simplewall, DDOS*

1. PENDAHULUAN

Distributed Denial of Services (DDOS) merupakan salah satu jenis eksploitasi kelemahan pada sebuah *web*. DDOS merupakan upaya serangan terhadap *server* di dalam jaringan internet dengan cara membanjiri banyak data pada lalu lintas jaringan untuk mengganggu jalannya lalu lintas normal pada *server*. Serangan ini dapat mengakibatkan *server* menjadi *down* dan mengakibatkan sistem menjadi error. Oleh karena itu dibutuhkan teknik untuk mengamankan sumber daya yang ada dalam jaringan komputer yaitu menggunakan metode *Intrusion Detection Systems* (IDS) dan *Simplewall* yang memiliki keunggulan melakukan blok akses internet terhadap program *windows* agar terhindar dari penyusupan data melalui jaringan internet.

Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau *administrator* jaringan. Sedangkan *Simplewall* adalah perangkat lunak komputer yang digunakan sebagai *firewall* untuk memberikan perlindungan secara total terhadap setiap akses yang tidak dikehendaki. *Simplewall* akan mengidentifikasi sebuah paket yang diakses *user* melalui pengecekan alamat IP apakah memiliki indikasi merusak sekaligus memiliki kemampuan melakukan penyaringan IP *address* agar dapat memblok akses berbahaya berbagai tipe dapat dilakukan dengan menutup akses tertentu, sehingga seluruh aplikasi *windows* yang terkoneksi internet tersebut tidak dapat diakses *user* kecuali jika sudah disetujui aksesnya terlebih dahulu.

Pada penelitian ini menerapkan *Intrusion Detection Systems* (IDS) dan *Simplewall* sebagai pencegah adanya penyusup pada *server* jaringan komputer bahkan serangan DDOS sekaligus. Dengan menerapkan *Intrusion Detection Systems* (IDS) dapat mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak bisa dicegah oleh sistem umum seperti *firewall*, namun untuk meningkatkan keamanan jaringan maka diperlukan perangkat lunak seperti *Simplewall* yang

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

digunakan sebagai *firewall* guna menambah proteksi agar mencegah penyusupan data pada program *windows* yang dapat diakses melalui akses internet.

2. METODOLOGI PENELITIAN

Metode yang digunakan pada penelitian ini menggunakan metode *Snort* sebagai sistem pendeteksi ancaman serta *Simplewall* sebagai *firewall* guna menangkal segala ancaman dari jaringan luar. Berikut ini merupakan tahapan yang akan dirancang untuk penelitian:

a. Perencanaan

Pada tahap ini kegiatan yang dilakukan yaitu merancang jaringan usulan yang akan dijadikan sampel dan membuat sistem pendeteksi ancaman yang akan digunakan untuk penelitian. Tahap ini disesuaikan dengan metode yang akan dibawakan pada penelitian.

b. Analisis Kebutuhan

Pada tahap ini peneliti melaksanakan uji coba sistem pendeteksi (IDS) pada sampel penelitian serta menguji coba dan menganalisis sistem pendeteksi ancaman dengan menggunakan *ping attack* dan *port scanning*. Metode pada penelitian ini menggunakan metode *snort* pada *windows* sebagai *Intrusion Detection System* (IDS) dan *simplewall* sebagai *firewall* untuk membantu memproteksi sistem keamanan dari ancaman serangan luar.

c. Perancangan Sistem

Pada tahap ini peneliti merancang bagaimana sistem akan bekerja, bagaimana bentuknya, dan mengatasi masalah yang didapat dari tahap analisis. Perancangan ini juga bertujuan untuk menggambarkan seperti apa sistem pendeteksi ancaman dan apa saja yang akan terjadi setelah menggunakan sistem pendeteksi ancaman.

d. Implementasi

Pada tahap ini peneliti mengimplementasikan sistem pendeteksi ancaman pada *windows* dan mengembangkan sistem ini agar dapat efektif mendeteksi serta mencegah terjadinya serangan luar pada saat terkoneksi internet. Implementasi pada penelitian ini juga dapat mengetahui kekurangan serta kelebihan dari penelitian yang akan diuji coba.

e. Uji Coba

Pada tahap ini peneliti dapat menjalankan sistem pendeteksi ancaman pada *windows* apakah sistem pendeteksi dapat mendeteksi ancaman yang masuk atau dapatkah koneksi berbahaya tersaring pada sistem pendeteksi ancaman agar dapat melindungi sumber daya yang ada dalam jaringan komputer dari serangan DDOS yang dapat merusak *server* dan *server* menjadi *down*.

3. ANALISA DAN PEMBAHASAN

3.1 Analisa Sistem Berjalan

Analisa sistem berjalan yang menggunakan metode *Snort* dapat mendeteksi ancaman jaringan yang masuk melalui IP *address* dan *port* pada saat terkoneksi internet dan dapat ditangkal oleh *Simplewall* apabila terdapat jaringan luar yang masuk ke dalam sumber daya jaringan. Penelitian ini juga dibantu oleh beberapa program seperti *Kiwi Syslog Server* yang bertugas untuk mendeteksi IP *address* yang masuk ke dalam jaringan. Program ini terhubung oleh *Snort* yang bertugas mendeteksi adanya ancaman jaringan. Program yang lainnya seperti *PeerBlock* juga dapat membantu menyaring IP *address* dan dapat memblokir akses apabila terdapat IP *address* yang mencurigakan dan dapat menimbulkan ancaman pada jaringan. Program lain yang digunakan seperti *Wireshark* mirip seperti *Snort* yang digunakan untuk mendeteksi adanya jaringan asing yang masuk menggunakan *filtering*.

3.2 Analisa Sistem Usulan

Analisis sistem usulan menggunakan metode *Snort* pada *Intrusion Detection System* (IDS) dan penggunaan *Simplewall* sebagai *firewall* guna mencegah terjadinya ancaman atau serangan jaringan seperti *virus*, *malware*, *worm*, *hacking*, *carding*, *cyber crime*, dan DDOS. Penelitian ini

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

dilaksanakan dengan fokus pengamatan pada kinerja jaringan serta keamanan jaringan dari gangguan lalu lintas jaringan. Objek pengambilan data terdiri dari data aktivitas lalu lintas jaringan pada jaringan lokal, menganalisa lalu lintas jaringan yang mencurigakan dengan aplikasi *snort*, dan menampilkan hasil analisa menggunakan tampilan GUI.

Penelitian ini untuk menguji pengaruh Variabel X (IDS dan *Simplewall*) terhadap Y (ancaman serangan DDOS atau *cyber crime*). Sedangkan untuk menganalisis pengaruh masing-masing variabel menggunakan metode *snort* untuk pendeteksian ancaman jaringan.

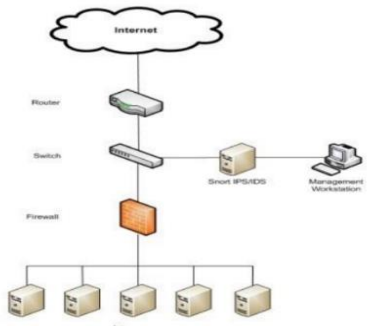
Alasan dipilihnya jenis penelitian ini karena peneliti ingin mengetahui seberapa besar pengaruh IDS dan *Simplewall* terhadap ancaman dari serangan DDOS atau *cyber crime* lainnya. Penelitian ini terdiri dari dua variable: variabel bebas (X) yaitu IDS dan *Simplewall* dan variabel terikat (Y) yaitu ancaman serangan DDOS atau *cyber crime*.

3.3 Analisis Sistem Jaringan

Sistem jaringan yang berjalan masih kurangnya sistem keamanan jaringan dari ancaman jaringan luar yang hanya menggunakan *firewall* bawaan dari sistem operasi. Banyak penyimpanan data pada perusahaan dan lalu lintas jaringan yang tidak terkontrol dengan baik menjadi permasalahan yang harus diperbaiki serta melakukan pencegahan terhadap serangan siber atau ancaman lainnya guna mengamankan *database* perusahaan dari *hacker* atau serangan DDOS.

3.4 Manajemen Jaringan Usulan

IDS merupakan suatu sistem yang memiliki kemampuan untuk menganalisis data secara *real-time* dalam mendeteksi, mencatat (log) dan mencegah dari penyerangan. IDS merupakan *security tools* yang dapat digunakan untuk menghadapi aktivitas *hackers* dan *cyber crime* termasuk DDOS *attack*. IDS ini mampu memberikan peringatan kepada *administrator* apabila terjadi suatu serangan atau ancaman di dalam jaringan, bahkan peringatan itu dapat pula menunjukkan alamat IP dari sebuah sistem penyerang.

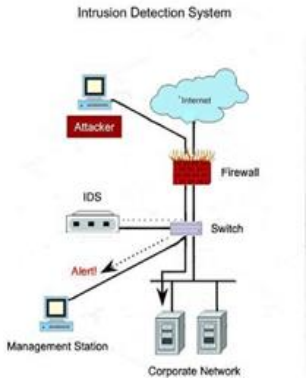


Gambar 1. Topologi Jaringan Usulan

3.5 Cara Kerja *Intrusion Detection System* (IDS)

Gambar dibawah menyatakan bahwa *Instrusion Detection Systems* (IDS) bekerja dengan mendeteksi adanya aktivitas yang mencurigakan atau adanya penyusup. Apabila penyusup terdeteksi maka akan memberi peringatan dan menyaring data pada *Management Station*. Jika tidak terdeteksi maka data akan menuju ke jaringan lokal komputer.

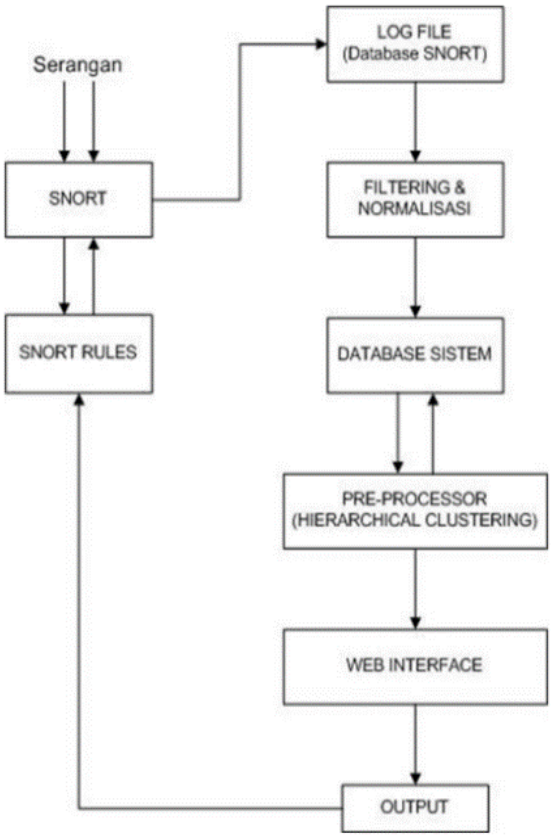
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328



Gambar 2. IDS Dalam Menghalau Serangan Atau Penyusup

3.6 Desain Sistem *Snort* Pada IDS

Snort ialah perangkat lunak yang berfungsi mengamati aktivitas dalam suatu jaringan, yang bersifat *opensoure* dan gratis. Desain pada sistem *snort* berawal dari serangan yang terjadi pada sistem akan di *capture* oleh *snort* dan akan disimpan pada *log file snort*, selanjutnya di *filtering* parameter apa saja yang akan dipilih dan dimasukkan ke dalam database dan nantinya di analisa dan di *clustering* pada *pre-processor* dengan *hierarchical clustering*, lalu hasil dari *clustering* ditampilkan pada *user interface* berbasis *web* secara *real-time*. *Output web interface* akan selalu meng-*update rules snort* jika ada serangan baru atau yang belum dikenali oleh *snort*, sehingga *snort* akan melakukan action dengan memblokir IP address yang digunakan untuk melakukan serangan pada sistem jaringan tersebut.



OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

Gambar 3. Desain Sistem *Snort* IDS

4. IMPLEMENTASI

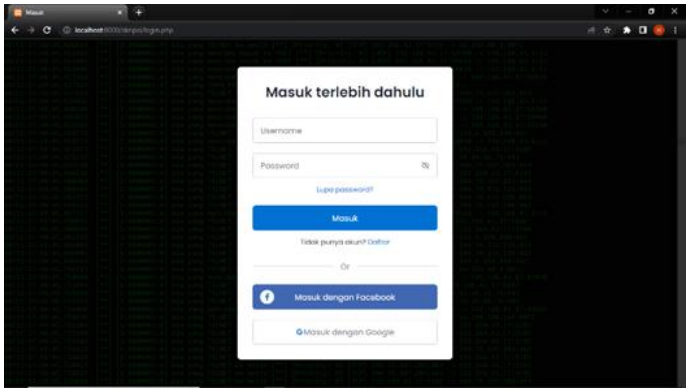
Pada tahap ini bertujuan untuk mewujudkan rancangan yang sudah dianalisis dan dirancang sebelumnya. Tahap ini menghasilkan metode *Snort* yang telah berjalan untuk mendeteksi adanya ancaman jaringan serta *Simplewall* yang telah berjalan untuk memblokir adanya jaringan yang masuk melalui program di *windows* agar sumber daya jaringan dapat terhindar dari penyusupan dan pencurian data oleh *cyber crime*. Berikut adalah implementasi dari metode *Snort* dan *Simplewall* yang telah peneliti rancang.

4.1 Implementasi *Interface*

Implementasi interface akan menampilkan tampilan *web* yang telah dirancang meliputi halaman *login*, beranda, dasbor, hingga aplikasi yang sudah siap dijalankan pada metode penelitian tersebut.

a. Implementasi Halaman *Login*

Halaman *login* merupakan halaman dimana ketika *user* ingin mengakses *web*, jika telah terdaftar maka *user* hanya akan memasuki *username* dan *password*.



Gambar 4. Implementasi Halaman *Login*

b. Implementasi Tampilan Beranda

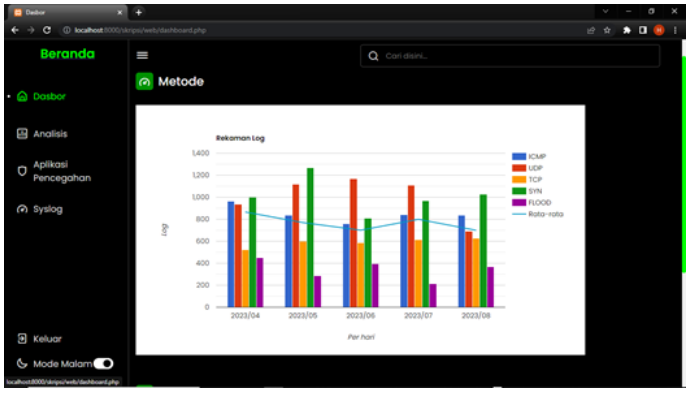
Halaman Beranda merupakan tampilan setelah *user* berhasil masuk dari halaman *login* dan merupakan tampilan awalan dari sebuah *website*.

Gambar 5. Implementasi Halaman Beranda

c. Implementasi Tampilan *Dasbboard*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

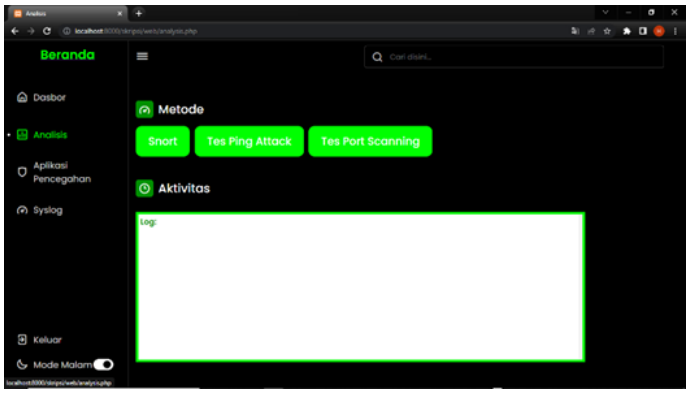
Halaman *Dasboard* merupakan halaman yang menampilkan *Interface* pada sebuah *website* pada umumnya.



Gambar 6. Implementasi Halaman *Dashboard*

d. Implementasi Tampilan Analisis

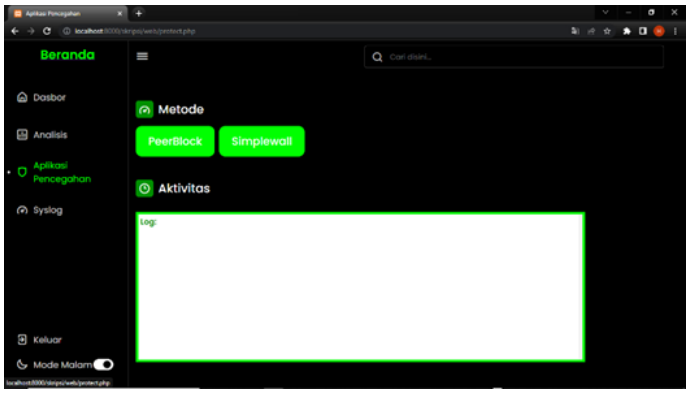
Halaman Analisis ini akan menampilkan metode yang telah dirancang pada penelitian ini, meliputi *Snort*, Tes *Ping Attack*, dan Tes *Port Scanning*.



Gambar 7. Implementasi Halaman Analisis

e. Implementasi Tampilan Aplikasi Pencegahan

Halaman Aplikasi Pencegahan ini akan menampilkan aplikasi penyaring IP *address* dan *firewall* pada penelitian ini, meliputi *PearBlock* dan *Simplewall*.

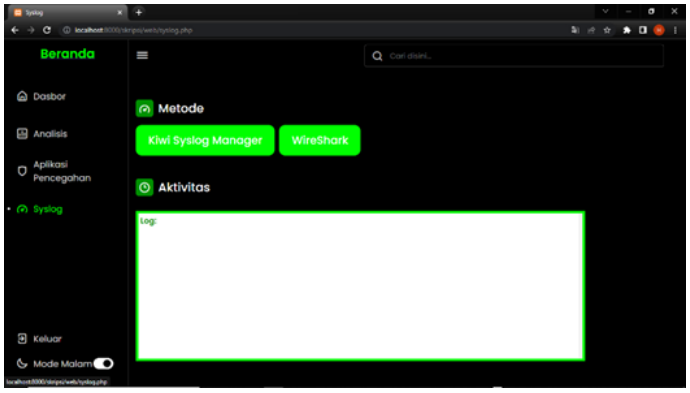


Gambar 8. Implementasi Halaman Aplikasi Pencegahan

f. Implementasi Tampilan Syslog

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

Halaman Syslog ini akan menampilkan aplikasi perekam log / *history log* dari metode *Snort* untuk mendeteksi jaringan luar yang masuk, meliputi *Kiwi Syslog Manager* dan *Wireshark.*



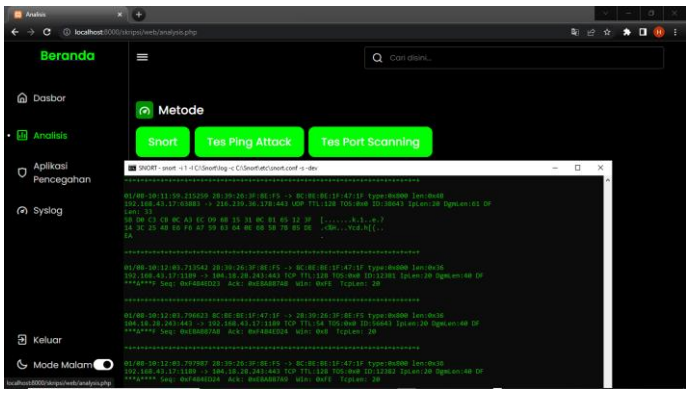
Gambar 9. Implementasi Halaman Syslog

4.2 Pengujian Sistem

Pada tahap ini dilakukan uji coba sistem dengan metode *Snort* dan *Simplewall* sebagai *firewall* guna mencegah terjadinya ancaman jaringan yang masuk ke dalam sumber daya jaringan. Uji coba ini juga dibantu oleh *Kiwi Syslog Service* yang berfungsi merekam log dari *Snort* serta *Wireshark* yang berfungsi memfilter aktifitas jaringan yang masuk. Program pembantu lainnya seperti *PeerBlock* dapat menyaring IP *address* bahkan memblokir apabila terdapat IP *address* yang mencurigakan dan dapat merusak sumber daya jaringan. Metode tes *Ping Attack* dan *Port Scanning* juga digunakan untuk simulasi serangan terhadap metode *Snort* apakah *Snort* akan mendeteksi adanya ancaman pada rekaman log / *history log*.

a. Pengujian *Snort*

Pada pengujian ini *Snort* akan melakukan *monitoring* IP *address* pada *windows* dan sedang mendeteksi adanya IP *address* yang masuk pada jaringan computer.

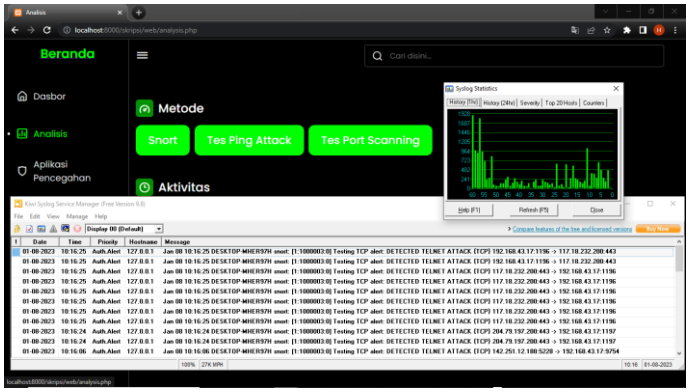


Gambar 10. Pengujian *Snort*

b. Tampilan Rekaman Log / *History Log*

Kiwi Sylog Server berfungsi sebagai *monitoring interfaces* pada *Snort* untuk dapat mengetahui lebih jelas IP *address* yang masuk beserta mendeteksi adanya ancaman jaringan yang mengganggu lalu lintas jaringan.

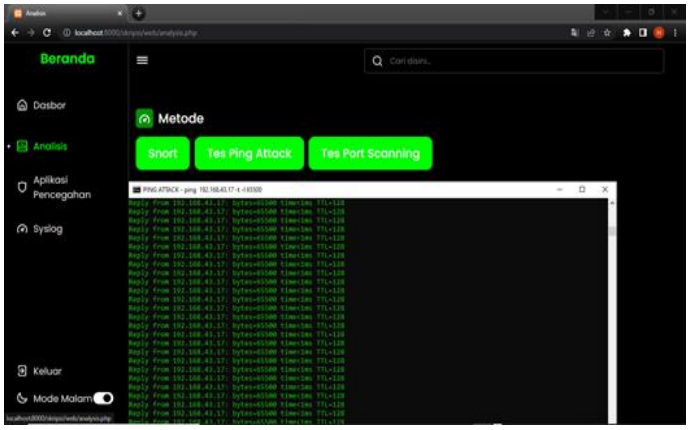
OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328



Gambar 11. Tampilan *History Log* dari *Snort*

c. Simulasi *Ping Attack*

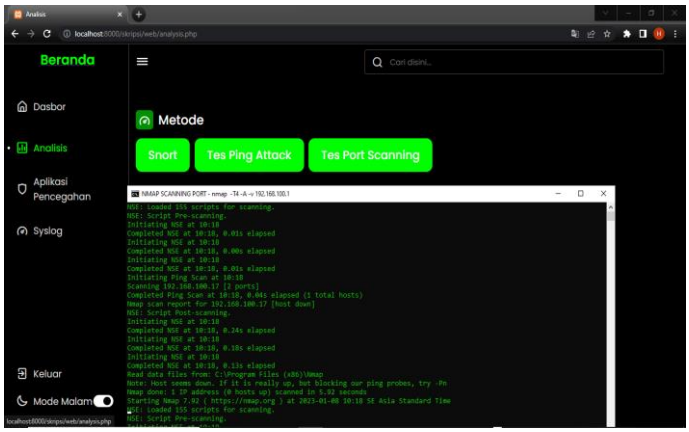
Pada tahap ini peneliti melakukan simulasi serangan serangan ping atau biasa disebut *Ping Attack* untuk melihat apakah *Snort* akan mendeteksi adanya *Ping Attack* atau serangan ping yang menyerang lalu lintas jaringan.



Gambar 12. *Simulasi Serangan Ping Attack*

d. Simulasi *Port Scanning*

Pada tahap ini juga peneliti melakukan simulai serangan *port* atau disebut *Port Scanning*. *Port Scanning* ini melakukan serangan dengan memasuki *port* pada *website* dan mengacak-acak lalu lintas pada jaringan tersebut.

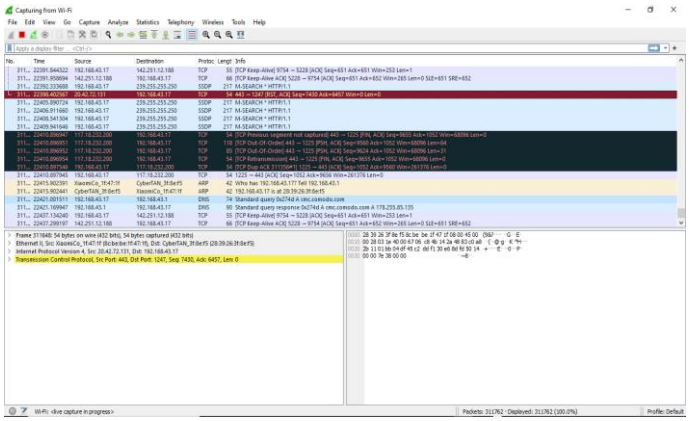


Gambar 13. *Simulasi Serangan Port Scanning*

OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

e. Tampilan *Filtering* pada *Wireshark*

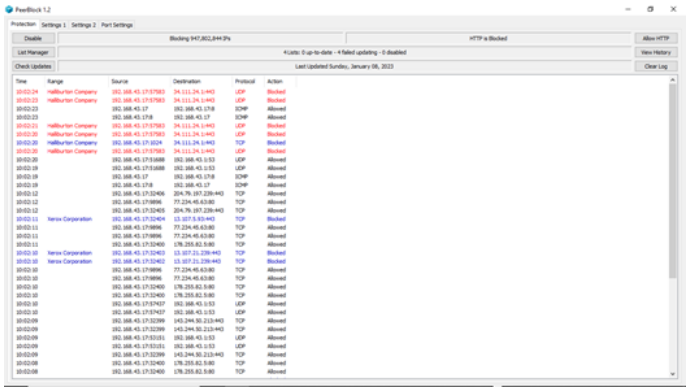
Pada tahap ini peneliti melakukan *filtering* pada *Wireshark* yang berfungsi mirip seperti *Snort* yakni memonitoring jaringan dengan tampilan yang lebih kompleks.



Gambar 14. Tampilan *Filtering Wireshark*

f. Penyaringan IP *address PearBlock*

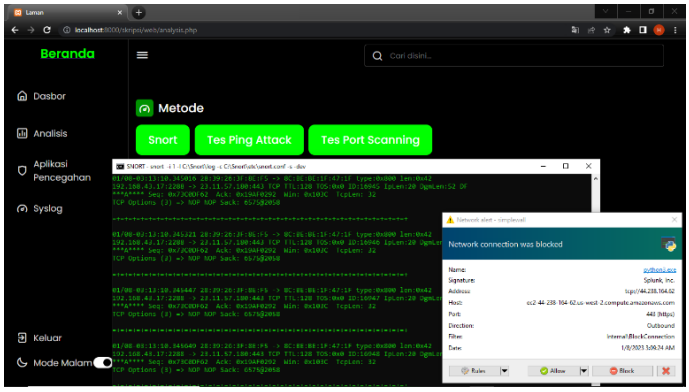
PeerBlock melakukan penyaringan IP *address* dan memblokirnya apabila terdapat IP *address* yang mencurigakan dan berpotensi merusak sumber daya jaringan.



Gambar 15. Tampilan Penyaringan *IP address* oleh *PearBlock*

g. Pemblokiran IP *address* yang mencurigakan pada *Simplewall*

Simplewall akan memblokir IP *address* & *port* mencurigakan yang akan masuk melalui program *windows* pada saat terkoneksi internet. Apabila tidak diblokir dapat memicu pencurian data atau penyusup di dalam program *windows* yang terhubung ke internet.

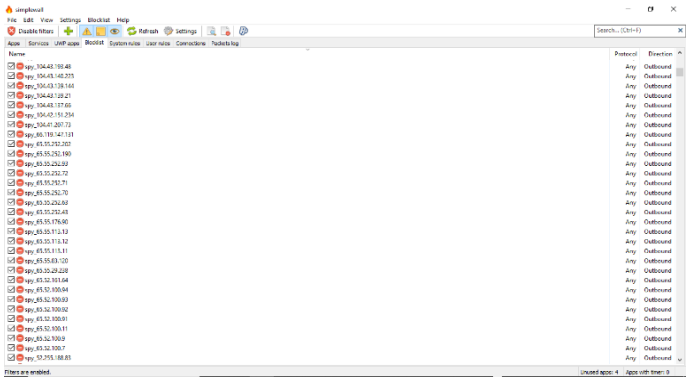


OKTAL : Jurnal Ilmu Komputer dan Science
Volume 2, No. 12, Desember 2023
ISSN 2828-2442 (media online)
Hal 3319-3328

Gambar 16. Tampilan Penyaringan *IP address* oleh *Simplewall*

h. Tampilan IP *address* yang mencurigakan terblokir oleh *Simplewall*

Simplewall juga dapat memblokir sebuah IP *address* yang diketahui pengintai oleh *firewall* ini agar pengintai atau penyusup tidak dapat memasuki jaringan pada komputer.



Gambar 17. Tampilan Penyaringan *IP address yang Mencurigakan Terblokir* oleh *Simplewall*

4.3 Hasil Penelitian

Hasil dari penelitian mengenai metode *Snort* dan *Simplewall* sebagai *firewall* dapat bekerja sebagaimana mestinya. Diharapkan dapat mencegah terjadinya serangan DDOS yang dapat merusak sumber daya jaringan dan dapat menghambat lalu lintas jaringan pada umumnya. Dengan hasil ini maka dipastikan berhasil mendeteksi adanya IP *address* dan *port* yang mencurigakan, memblokir IP *address*, melihat aktifitas lalu lintas jaringan serta dapat melihat rekaman log / *history log* yang bertujuan untuk memonitoring jaringan yang dapat memicu terjadinya bentrok lalu lintas jaringan.

5. KESIMPULAN

Intrusion Detection System (IDS) menggunakan metode *Snort* dan *Simplewall* sebagai *firewall* dapat mendeteksi adanya IP *address* & *port* masuk yang rentan terjadinya pencurian data atau serangan siber lainnya. Metode *Snort* ini menampilkan rekaman log / *history log* dari aplikasi bernama *Kiwi Syslog Service* namun juga dapat menampilkannya pada *Snort* itu sendiri sesuai yang diinginkan. DDOS dapat mengakibatkan lalu lintas jaringan menjadi terhambat dan bahkan merusak sumber daya jaringan, begitu juga dengan serangan siber lainnya seperti pencurian data, penyusup masuk melalui jaringan dan merusak database, serta *virus*, *malware*, *keylogger*, dan lain-lain.

REFERENCES

Dyakso Anindito Nugroho, Dkk. *Perancangan Dan Implementasi Intrusion Detection System Di Jaringan Universitas Diponegoro*, Universitas Diponegoro Vol. 3, No. 2. Tahun 2015.

Evan Porter. *Apa Itu Serangan DDoS dan Cara Mencegahnya di 2022*, Safety Detectives, Tahun 2022.

M. Alfine Ridho, Dkk. *Analisis Serangan DDoS Menggunakan Metode Jaringan Saraf Tiruan*, STMIK GI MDP Department Informatics Management Vol. 09, No. 3, Tahun 2020.

Nadila Sugianti, Dkk. *Deteksi Serangan Distributed Denial of Services (DDOS) Berbasis HTTP Menggunakan Metode Fuzzy Sugeno*, Universitas Islam Negeri Vol. 4, No. 3, Tahun 2020.

Ririn Agustin, Dkk. *Implementasi Metode Intrusion Detection Systems (IDS) Dan Intrusion Prevention System (IPS) Berbasis Snort Server Untuk Keamanan Jaringan Lan*, Universitas Nasional Vol.18, Tahun 2018.

Septian Geges, Dkk. *Pengembangan Pencegahan Serangan Distributed Denial Of Service (DDOS) Pada Sumber Daya Jaringan Dengan Integrasi Network Behavior Analysis Dan Client Puzzle*, Institut Teknologi Sepuluh Nopember Vol. 13, No. 1, Tahun 2015.

Sutarti, Dkk. *Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan Sman 1 Cikeusal*, Universitas Serang Raya Vol. 5, No. 1, Tahun 2018.

Fathoni, W., Fitryani, Nurkahfi, G. *Deteksi Penyusup Pada Jaringan Komputer Menggunakan IDS SNORT*, E-Proceeding of Engineering Vol. 3. No. (1), Tahun 2016.

Masse, F., Hidayat, A., dan Badrianto. *Penerapan Network Intrusion Detection System Menggunakan Snort Berbasis Database Mysql Pada Hotspot Kota*, Jurnal Elektronik Sistem Informasi dan Komputer Vol. 1. No. (2). 1-16, Tahun 2015.

Harjono Harjono, Agung Purwo Wicaksono. *Sistem Deteksi Intrusi Dengan Snort*, Juita Vol. 3 Nomor 1, Tahun 2014