Penerapan Snort Sebagai Sistem Keamanan Jaringan

Jusep ferlyzon[1], Indra Kanedi[2], Reno Supardi[3]

[1] Mahasiswa Program Studi Informatika,Fakultas IlmuKomputer Universitas Dehasen Bengkulu,
E-mail: jusepferlyzon22@gmail.com
[2,] Dosen Program Studi Sistem Informasi. Fakultas IlmuKomputer Universitas Dehasen Bengkulu
*E-mail:*indrakanedi12@Gmail.com.
[,3] *Dosen Program Studi Informatika, Fakultas IlmuKomputer Universitas Dehasen Bengkulu*
Email: *renosupardi00@gmail.com*
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139;

(Received: Nopember 2024, Revised: Februari 2025, Accepied: April 2025)

Abstract— SMA Negeri 5 South Bengkulu is one of the State Senior High Schools in South Bengkulu Regency, Bengkulu Province. The school already has internet access and a computer network in the Lab that can be accessed by teachers, students, and staff within the school. However, access to the network does not yet have a security system that can prevent several threats from attacking the network. The purpose of this research is to implement snort on computer networks at SMA Negeri 5 South Bengkulu. Securing the computer network at SMA Negeri 5 South Bengkulu to avoid unwanted things by implementing Snort in it which will detect if there is a threat of attacks. Snort will be tasked with detecting attacks that occur if a client attacks the server in the form of pinging of death or DDos attacks. Based on the test results that have been carried out, the application of snort can help schools in knowing security system information on computer networks at school, as well as securing computer networks at school.
Keyword: Snort, Security, Network.

Intisari— SMA Negeri 5 Bengkulu Selatan merupakan salah satu Sekolah Menengah Atas Negeri yang terdapat di Kabupaten Bengkulu Selatan Provinsi Bengkulu. Pada Sekolah tersebut sudah terdapat akses internet dan jaringan komputer di Lab yang dapat diakses oleh guru, siswa, staf di ruang lingkup sekolah. Namun akses pada jaringan tersebut belum terdapat suatu sistem keamanan yang dapat mencegah jika terjadi beberapa ancaman serangan pada jaringan. Tujuan dari penelitian ini yaitu untuk menerapkan snort pada jaringan komputer di SMA Negeri 5 Bengkulu Selatan. Pengamanan terhadap jaringan komputer di SMA Negeri 5 Bengkulu Selatan untuk menghindari hal-hal yang tidak diinginkan dengan menerapkan Snort di dalamnya yang akan mendeteksi apabila terdapat ancaman serangan-serangan. Snort akan bertugas untuk mendeteksi serangan-serangan yang terjadi jika ada client yang melakukan penyerangan terharap server berupa melakukan ping of death ataupun serangan DDos. Berdasarkan hasil pengujian yang telah dilakukan penerapan snort dapat membantu pihak sekolah dalam mengetahui informasi sistem keamanan pada jaringan komputer di sekolah, serta mengamankan jaringan komputer di Sekolah.
Kata Kunci: Snort, Keamanan, Jaringan pendahuluan.

I. PENDAHULUAN

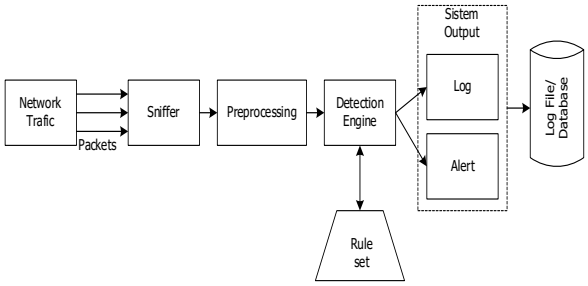
Teknologi setiap hari terus berkembang diberbagai bidang teknologi. Dengan kemajuan teknologi yang pesat masyarakat harus mengikuti perkembangannya karena seiring perkembangan teknologi saat ini sangat membantu berbagai kegiatan masyarakat baik dalam pekerjaan, rumah tangga, dan lainnya. Teknologi sebagai sarana transaksi pembayaran *online*, sehingga banyak data yang tersebar lewat jaringan internet. Keamanan merupakan aspek penting dalam membangun sebuah jaringan. pada dasarnya keamanan yang ada pada sistem operasi belum cukup untuk mengamankan suatu jaringan komputer. Banyak sekali ancaman keamanan yang terjadi pada jaringan komputer, salah satunya yaitu *flooding*. *Flooding* merupakan serangan yang mengakibatkan suatu sistem akan dibanjiri oleh data-data secara terus menerus dalam waktu yang singkat, dan mengakibatkan lalu lintas jaringan menjadi padat sehingga pengguna yang akan mengakses ke dalam sistem jaringan menjadi terganggu. SMA Negeri 5 Bengkulu Selatan merupakan salah satu Sekolah Menengah Atas Negeri yang terdapat di Kabupaten Bengkulu Selatan Provinsi Bengkulu. Pada Sekolah tersebut sudah terdapat akses internet dan jaringan komputer di Lab yang dapat diakses oleh guru, siswa, staf di ruang lingkup sekolah. Namun akses pada jaringan tersebut belum terdapat suatu sistem keamanan yang dapat mencegah jika terjadi beberapa ancaman serangan pada jaringan. Hal ini dikarenakan minimnya pengetahuan pihak sekolah terkait dengan sistem keamanan jaringan. Keamanan jaringan menjadi hal yang penting untuk menjaga keamanan jaringan, data dan informasi yang berada didalamnya. Berdasarkan perlindungan keamanan data/informasi dalam suatu jaringan, umumnya semua teori keamanan berbasis data dibuat dan diaplikasikan untuk mengamankan suatu jaringan tertentu Oleh karena itu, dalam penelitian ini dilakukan pengembangan terhadap sistem jaringan yang sudah ada saat ini di Sekolah dengan menambahkan server yang akan mengidentifikasi serangan-serangan yang terjadi dalam jaringan komputer. Untuk mendeteksi serangan

P-ISSN 1858-2680
E-ISSN 2723-4673

tersebut, maka diterapkan *snort* yang akan di instalasi dan konfigurasi pada server. Selain itu, untuk mempermudah pihak sekolah dalam mengetahui serangan-serangan yang terjadi, maka dibangun GUI menggunakan *Base* berbasis web yang dapat diakses melalui browser. Berdasarkan uraian tersebut, maka dalam penelitian ini peneliti tertarik mengangkat judul penelitian tentang **Penerapan *Snort* Sebagai Sistem Keamanan Jaringan**.

II. TINJAUAN PUSTAKA

Snort adalah sebuah aplikasi yang memiliki fungsi dapat mencegah intruksi dan serangan jaringan. *Snort* dapat membentuk analis trafik-trafik dan *logging* paket-paket secara real *time* dalam jaringan berbasis TCP/IP. Adapun orang yang pertama kali menulis *snort* adalah Martin Roesch dan saat ini dikelola oleh *Sourcefire*, yang mana Roesch sebagai pendiri dan CTO (*Chief of Technical Officer*). *Snort* adalah penggabungan dari *system* analisis *protocol* dan *system* pendeteksi penyusupan, hal ini sangatlah bermanfaat untuk mendeteksi serangan terhadap *host* dalam jaringan (Dasmen, et al., 2022). *Snort* adalah sebuah sistem pendeteksi intrusi *open source* yang diciptakan oleh Roesch dan pertama kali muncul pada 22 Desember 1998. IDS ini dapat menganalisis lalu lintas jaringan dan paket *logging* secara real *time* dengan 3 mode utama, yaitu sebagai *packet sniffer*, *packet logger*, dan *IDS* jaringan (Sau & Siswantyo, 2021). Arsitektur dari IDS *Snort* digambarkan pada Gambar.



Gambar 1. Arsitektur *Snort*

Snort merupakan sistem pencegahan dan deteksi intrusi jaringan bersifat *open source* dengan berbasis aturan (*rule-driven*) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan atau *alert* ketika ancaman terdeteksi. *Snort* merupakan salah satu alat pada IDS dengan komunitas open *source*, sehingga *Snort* merupakan alat yang disukai untuk melindungi keamanan jaringan komputer. Deteksi intrusi adalah proses memantau kejadian yang terjadi di sistem komputer atau jaringan dan menganalisis kemungkinan kejadian. Ada beberapa alasan untuk kejadian tersebut, seperti *malware* (seperti *worm* dan *spyware*) dan penyerang. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam suatu sistem atau jaringan. *Snort* bekerja mirip dengan *TcpDump*, tetapi berfokus pada *sniffing* paket yang aman. Fitur utama yang membedakan *Snort* dari *TcpDump* adalah pemeriksaan muatan. *Snort* menganalisis kumpulan aturan muatan yang disediakan (Gunawan, et al., 2021). *Snort* merupakan sebuah aplikasi keamanan jaringan yang berfungsi dalam mendeteksi adanya ancaman dalam jaringan komputer, seperti penyusup, pemindaian, maupun penyerangan. *Snort* merupakan gabungan dari protokol analisis dan pendeteksi penyusupan yang berguna untuk merespon kejadian-kejadian yang sedang terjadi pada jaringan komputer secara *real-time*. *Snort* akan merespon kejadian yang terjadi dalam penyerangan *host-host* jaringan (Purba & Efendi, 2020). *Snort* merupakan sebuah aplikasi sekuriti yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Dalam praktiknya, *snort* sangat andal untuk membentuk *logging* paket-paket dan analisis trafik-trafik secara *real-time* dalam jaringan-jaringan berbasis *TCP*/*IP*. *Snort* ditulis oleh Martin Roesch dan sekarang dikelola oleh *Sourcefire*, dimana Roesch bertindak sebagai pendiri dan CTO (*Chief of Technical Officer*-Kepala Tim Teknis). *Snort* tersedia bebas dalam bentuk *source code* di bawah lisensi GNU General *Public License* (Dar & Harahap, 2018). *Snort* merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mampu menganalisis paket yang melintasi jaringan secara real *time traffic* dan *logging* ke dalam *database* serta mampu mengidentifikasi berbagai serangan yang berasal dari luar jaringan (Sutarti, et al., 2018). Untuk dapat menjalankan fungsinya, Snort memiliki 4 komponen utama pada arsitekturnya, yaitu (Sau & Siswantyo, 2021) :

1.*Sniffer*

Sniffer adalah perangkat yang berfungsi untuk masuk ke dalam jaringan. Tujuan utama dari komponen ini adalah

P-ISSN 1858-2680
E-ISSN 2723-4673

untuk melakukan *sniffing*, atau menangkap paket-paket yang sedang melintasi jaringan.

2. *Preprocessor*

Tugas utama dari komponen ini adalah untuk melakukan penyaringan atau pengecekan terhadap paket-paket yang telah ditangkap. Komponen ini akan menentukan jenis dari paket yang ditangkap, apakah berupa paket *HTTP*, paket hasil *scanning port* atau paket jenis lainnya.

3. *Detection Engine* (Mesin pendeteksi)

Pada tahap ini, mesin pendeteksi akan melakukan pencocokan antara paket dengan *rules* yang telah didefinisikan. Jika paket cocok dengan *rules* yang dibuat, maka paket tersebut akan diteruskan ke sistem *output* untuk menghasilkan alert.

4. Sistem *output*

Jika paket sesuai dengan *rules*, maka sistem *output* akan mengeluarkan peringatan atau *alert* dari *IDS*. Selain menghasilkan *alert*, *Snort* juga akan menghasilkan log berbentuk teks yang secara tetap tersimpan dalam *file* log pada direktori */var/log/snort*. Format *log* dari *IDS Snort* dapat disimpan dalam berbagai format, yaitu *tcpdump*, *csv*, dan *Unified2*.

Sistem Keamanan Jaringan, Keamanan merupakan aspek penting dalam membangun sebuah jaringan. Pada dasarnya keamanan yang ada pada sistem operasi belum cukup untuk mengamankan suatu jaringan komputer (Sihotang & Pangaribuan, 2023) Keamanan jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk ke dalam sistem jaringan komputer. Sistem harus tetap dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak memiliki hak. Langkah-langkah pencegahan dapat membantu administrator untuk menghentikan pengguna yang tidak sah untuk mengakses sistem jaringan komputer. Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-risiko yang akan terjadi pada jaringan komputer yang dapat menggangu aktivitas yang sedang terjadi pada sistem jaringan komputer. Ada tiga hal dalam konsep keamanan jaringan, yaitu ingkat bahaya, ancaman dan kerapuhan sistem (Purba & Efendi, 2020) Keamanan Jaringan dapat diartikan sebagai keadaan aman pada suatu susunan yang menjalankan sistem komputer. Keamanan jaringan juga dapat diartikan sebagai proses untuk mengidentifikasi dan mencegah adanya user yang tidak mempunyai izin (penyusup) dari sistem jaringan komputer. Tujuan dibangunnya suatu sistem keamanan jaringan adalah untuk menanggulangi dan mencegah ancaman dari jaringan luar yang dapat berupa ancaman logik atau fisik. Ancaman logik adalah sebauh ancaman yang berupa pengambilan data secara tidak saha atau pencurian data oleh penyusup dengan cara mencari celah yang terbuka pada sistem keamanan jaringan, sedangkan ancaman fisik yaitu sebuah ancaman yang berujuan untuk merusak sistem jaringan dari sisi *hardware* sebuah komputer (Anggraini, 2018). Secara umum, terdapat 3 hal dalam konsep keamanan jaringan, antara lain :

1. Resiko atau tingkat bahaya (risk) yaitu menyatakan besarnya kemungkinan gangguan yang muncul terhadap jaringan.
2. Ancaman (threat) yaitu menyatakan kemungkinan gangguan yang muncul terhadap jaringan.
3. Kerapuhan sistem (*vulnerability*) yaitu menyatakan kelemahan- kelemahan pada sistem yang memungkinkan terjadinya gangguan. Keamanan jaringan komputer itu sendiri menyangkut 3 elemen dasar yakni :

1. Keamanan jaringan (*network security*) : Upaya pengamanan atas jalur / media pengiriman data.
2.Keamanan aplikasi (*application security*) : Upaya pengamanan atas aplikasi-aplikasi dan layanan yang tersedia, contohnya DBMS.
3. Keamanan komputer (*computer security*) : Upaya pengamanan atas komputer yang digunakan untuk memakai aplikasi, termasuk di dalamnya adalah sistem operasi. Masalah keamanan jaringan komputer secara umum dibagi menjadi empat kategori yang saling berkaitan :

1. *Secrecy*/*confidentiality*: Informasi yang dikirim melalui jaringan komputer harus dijaga sedemikian rupa kerahasiaannya sehingga tidak dapat diketahui oleh pihak yang tidak berhak mengetahui informasi tersebut.

1. Authentication: Identifikasi terhadap pihak-pihak yang sedang melakukan komunikasi melalui jaringan harus dapat dilakukan. Pihak yang berkomunikasi melalui jaringan harus dapat memastikan bahwa pihak lain yang

P-ISSN 1858-2680
E-ISSN 2723-4673

diajak berkomunikasi adalah benar-benar pihak yang dikehendaki.

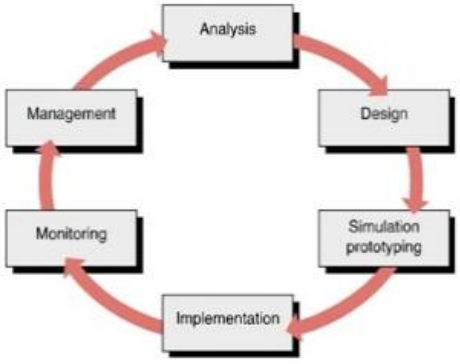
2. *Nonrepudiation*: Pembuktian korespondensi antara pihak yang mengirimkan informasi dengan informasi yang dikirimkan juga perlu dilakukan dalam komunikasi melalui jaringan komputer. Dengan pembuktian tersebut, identitas pengirim informasi dapat dipastikan dan penyangkalan pihak tersebut atas informasi yang telah dikirimnya tidak dapat dilakukan.

III. METODOLOGI PENELITIAN

Metode Penelitian

Dalam melaksanakan penelitian ini, peneliti menggunakan metode *Network Development Life Cycle* (NDLC) yang merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup pengembangan aplikasi, dan analisis pendistribusian data. NDLC mendefinisikan siklus proses perancangan atau pengembangan suatu sistem jaringan komputer. NDLC mempunyai elemen yang mendefinisikan fase, tahapan, langkah atau mekanisme proses spesifik. Kata cycle merupakan kunci deskriptif dari siklus hidup pengembangan sistem jaringan yang menggambarkan secara keseluruhan proses dan tahapan pengembangan sistem jaringan yang berkesinambungan

Adapun tahapan yang dilakukan dalam NDLC terdiri dari *Analysis, Design, Simulation Prototyping, Implementation, Monitoring*, dan *Management*.



Gambar 2. Tahapan Metode *NDLC*

Keterangan :

1.*Analysis*

Tahap awal ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan pengguna, dan analisa topologi jaringan yang sudah ada saat ini.

2. *Design*

Membuat gambaran desain topologi jaringan yang akan dibangun sesuai dengan analisa kebutuhan yang telah dilakukan.

3.*Simulation Prototype*

Tahap dimana dilakukan simulasi dengan bantuan *tools* khusus di bidang jaringan yang digunakan untuk melihat kinerja awal jaringan yang akan dibangun.

4. *Implementation*

Tahap dimana akan dilakukan penerapan rancangan yang telah dibuat agar dapat diuji di lapangan agar dapat menyelesaikan masalah teknik dan non teknis.

5. *Monitoring*

Tahap dimana dilakukan pengamatan terhadap infrastruktur perangkat keras, dan memperhatikan jalannya aplikasi snort server di dalam jaringan yang telah dibangun

6. *Management*

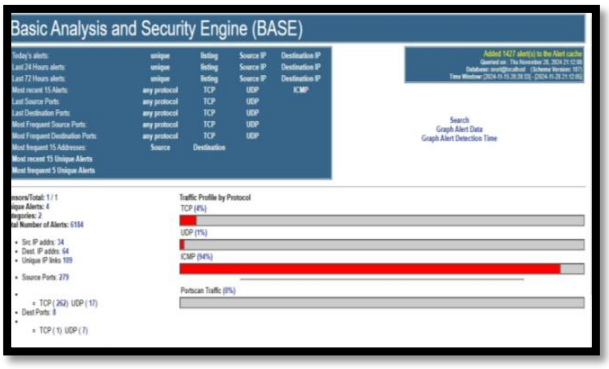
Tahap dimana menentukan kebijakan untuk membuat/mengatur agar sistem yang telah dibangun dapat berjalan dengan baik dan berlangsung lama.

IV. HASIL DAN PEMBAHASAN

Hasil Dan Impelementasi Aplikasi

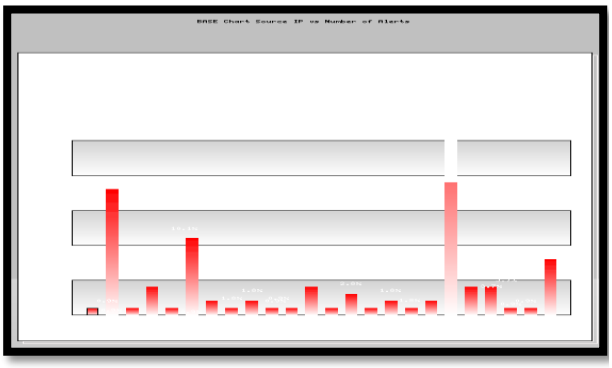
Implementasi *snort* sebagai alat pendeteksi keamanan jaringan di SMA Negeri 5 Bengkulu Selatan menggunakan *linux ubuntu server* dengan menambahkan server yang digunakan untuk mengamati aktifitas pada jaringan di SMA Negeri 5 Bengkulu Selatan, jika terdapat suatu aktifitas yang dianggap membahayakan yang dilakukan oleh *client*, maka akan tersimpan informasi tersebut di dalam log *snort* dan database. Untuk mempermudah dalam mengetahui informasi serangan yang terjadi tersebut, dibangun *front-end* berbasis *web* menggunakan *BASE* (*Basic Analysis and Security Engine*) yang dapat diakses melalui browser dengan url : IPaddressServer/base/, sehingga akan menampilkan halaman BASE.

P-ISSN 1858-2680
E-ISSN 2723-4673



Gambar 3. *Front-End Web BASE*

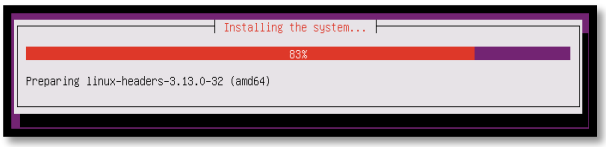
Terlihat bahwa terdapat informasi-informasi yang diberikan terkait serangan yang terdeteksi oleh *snort* yang telah tersimpan ke dalam database. Informasi tersebut berupa IP Address sumber dan tujuan, jenis serangan yang terjadi. Selain itu, pada *Front-End Web Base* tersebut menampilkan grafik yang diakumulasikan dari berapa banyak serangan yang terjadi berdasarkan jumlah serangan, *IP Address* sumber, *IP Address* Tujuan.



Gambar 4. Informasi Berupa Grafik

Dalam implementasi *snort* sebagai alat pendeteksi keamanan jaringan menggunakan *linux ubuntu server*, terdapat beberapa tahapan yang dilakukan, diantaranya :

1.Menyiapkan Server dan instalasi sistem operasi linux ubuntu server pada server tersebut, sehingga terlihat seperti Gambar 4.3.



Gambar 4.3. Instalasi Linux Ubuntu Server

2.Instalasi dan Konfigurasi Snort pada Linux Ubuntu Server Pada tahap ini terdapat beberapa service prerequisites yang digunakan sebelum menginstal snort pada linux ubuntu server. Adapun service prerequisites tersebut yaitu dengan mengetik perintah :

apt-get install build-essential libpcap-dev libpcre3-dev libdumbnet-dev bison flex zlib1g-dev liblzma-dev openssl libssl-dev

Setelah itu instalasi snort dengan perintah sebagai berikut :

wget https://snort.org/downloads/snort/snort-2.9.20.tar.gz

tar -xvzf snort-2.9.9.0.tar.gz

cd snort-2.9.9.0

./configure --enable-sourcefire

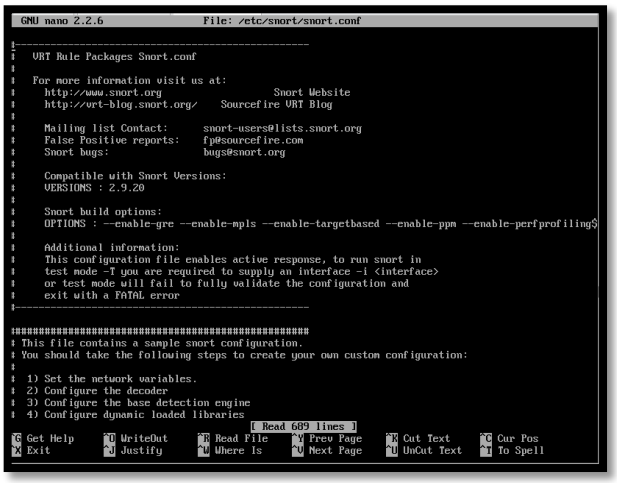
make

make install

Kemudian melakukan konfigurasi snort dengan perintah :

nano /etc/snort/snort.conf

sehingga menampilkan informasi.



Gambar 4.4. Konfigurasi Snort

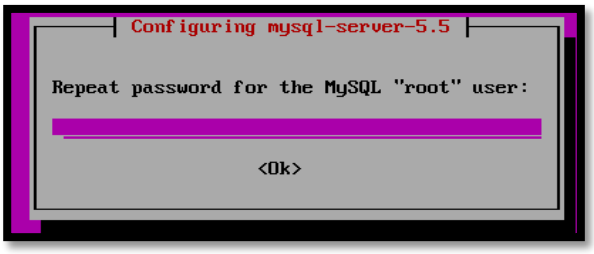
3. Instalasi Apache, PHP, dan MySQL

Untuk instalasi apache, PHP dan MySQL dengan cara mengetik perintah sebagai berikut :

apt-get install apache2 libapache2-mod-php5 php5 php5-mysql php5-common php5-gd php5-cli php-pear mysql-server libmysqlclient-dev mysql-client autoconf libtool

Pada saat instalasi mysql, terdapat pop-up yang digunakan untuk mengisi password root database MySQL, seperti Gambar 4.5.

P-ISSN 1858-2680
E-ISSN 2723-4673



Gambar 4.5. Password Root Database MySQL

4. Instalasi Barnyard2

Barnyard2 digunakan untuk memproses paket-paket yang telah terdeteksi oleh snort yang kemudian menyimpannya ke dalam database MySQL. Adapun perintah yang digunakan untuk instalasi Barnyard2 seperti :

cd ~/snort_src

wget https://github.com/firnsy/barnyard2/archive/master.tar.gz -O barnyard2-Master.tar.gz

tar zxvf barnyard2-Master.tar.gz

cd barnyard2-master

autoreconf -fvi -I ./m4

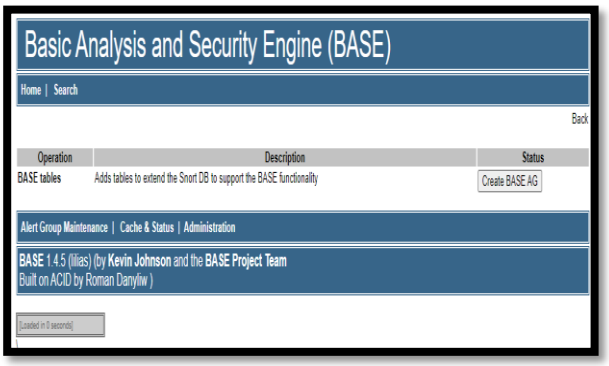
./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu

make

make install

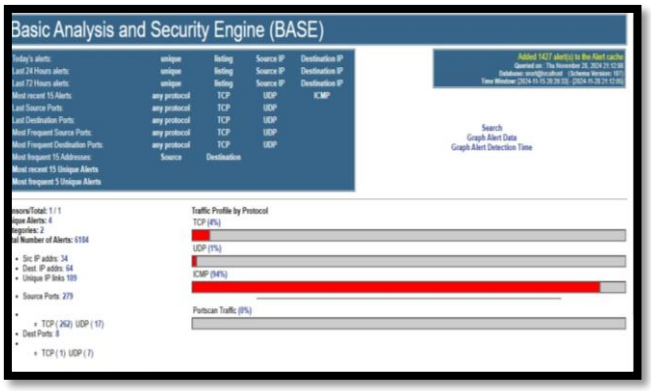
5. Instalasi BASE

Pada tahap ini dilakukan instalasi BASE dengan cara membuka browser melalui client kemudian ketik IPAddressServer/base/, sehingga akan menampilkan halaman setup page BASE, seperti Gambar 4.6.



Gambar 4.6. Setup Page BASE

Setelah berhasil, masuk ke main page untuk melihat informasi-informasi serangan yang terjadi pada jaringan, seperti terlihat pada Gambar 4.7.



Gambar 4.7. Main Page Front-End Web Base

6. Konfigurasi Rule/Aturan Snort

Rule/aturan snort digunakan untuk mendeteksi serangan-serangan yang terjadi sesuai dengan aturan yang telah dibuat. Konfigurasi rule snort dengan perintah :

nano /etc/snort/rules/local.rules

Setelah selesai membuat rule, ketik perintah untuk melakukan verifikasi terhadap rule yang telah dibuat :

snort -T -i eth0 -c /etc/snort/snort.conf

1. Menjalankan Service Snort dan Barnyard2 dengan perintah :

service snort start

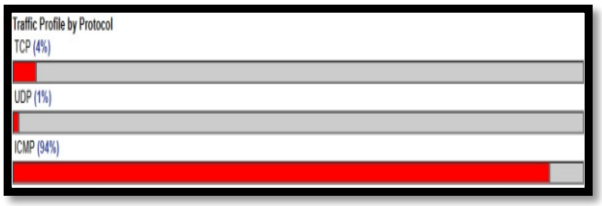
sevicer barnyard2 start

Hasil Pengujian

Pada tahap ini dilakukan pengujian terhadap infrastruktur jaringan yang telah diimplementasikan apakah berjalan dengan baik atau tidak. Pengujian implementasi *snort* sebagai alat pendeteksi keamanan jaringan *wireless* menggunakan *linux ubuntu* antara lain :

1. Pengujian ICMP

Pengujian ICMP dilakukan dengan perintah ping secara terus menerus pada IP Address tujuan. Pengujian ICMP tersebut di deteksi oleh snort dengan memberikan informasi traffic profile by protocol pada ICMP berupa grafik dan tingkat persentase serangan yang, seperti terlihat pada Gambar 4.8.

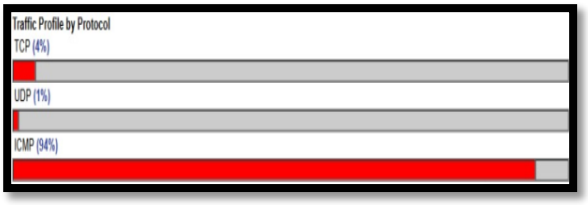


Gambar 4.8. Deteksi Snort Melalui Base

P-ISSN 1858-2680
E-ISSN 2723-4673

2. Pengujian TCP Flooding

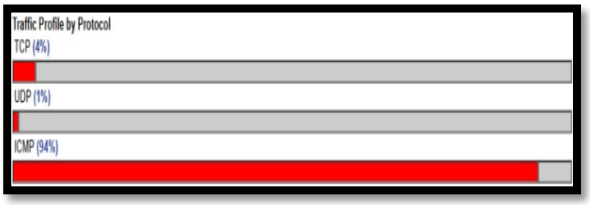
Pengujian TCP Flooding dilakukan menggunakan tools LOIC dengan memasukkan IP Address dan tipe serangan TCP Flooding pada LOIC. Pengujian TCP Flooding tersebut di deteksi oleh snort dengan memberikan informasi traffic profile by protocol pada TCP berupa grafik dan tingkat persentase serangan yang, seperti terlihat pada Gambar 4.9.



Gambar 4.9. Deteksi Snort Melalui Base

3. Pengujian UDP Flooding

Pengujian UDP Flooding dilakukan menggunakan tools LOIC dengan memasukkan IP Address dan tipe serangan UDP Flooding pada LOIC. Pengujian UDP Flooding tersebut di deteksi oleh snort dengan memberikan informasi traffic profile by protocol pada UDP berupa grafik dan tingkat persentase serangan yang, seperti terlihat pada Gambar 4.10.



Gambar 4.10. Deteksi Snort Melalui Base

Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa implementasi *snort* sebagai alat pendeteksi keamanan jaringan menggunakan *linux ubuntu* dapat membantu mendeteksi serangan yang terjadi dalam jaringan dan memberikan informasi terkait serangan tersebut, selain itu dengan Web UI Base Snort dapat mempermudah mendapatkan informasi berupa IP addrees sumber dan IP address tujuan serta jenis serangan yang telah dilakukan.

V. PENUTUP

A. Kesimpulan

Berdasarkan hasil dan pembahasan serta pengujian, maka dapat disimpulkan bahwa :

1. Pengamanan terhadap jaringan komputer di SMA Negeri 5 Bengkulu Selatan untuk menghindari hal-hal yang tidak diinginkan dengan menerapkan *Snort* di dalamnya yang akan mendeteksi apabila terdapat ancaman serangan-serangan. *Snort* akan bertugas untuk mendeteksi serangan-serangan yang terjadi jika ada *client* yang melakukan penyerangan terharap server berupa melakukan *ping of death* ataupun serangan *DDos*.
2. *Front-end* berbasis *web* menggunakan *BASE* (*Basic Analysis and Security Engine*) yang dapat diakses melalui browser dengan url : IPaddressServer/base/. Informasi-informasi yang diberikan terkait serangan yang terdeteksi oleh *snort* yang telah tersimpan ke dalam database. Informasi tersebut berupa IP Address sumber dan tujuan, jenis serangan yang terjadi
3. Berdasarkan hasil pengujian yang telah dilakukan penerapan snort dapat membantu pihak sekolah dalam mengetahui informasi sistem keamanan pada jaringan komputer di sekolah, serta mengamankan jaringan komputer di Sekolah.

B. Saran

Berdasarkan kesimpulan, maka peneliti menyarankan agar dapat menerapkan *snort* sebagai alat pendeteksi keamanan jaringan menggunakan *linux ubuntu*, sehingga menghindari hal-hal yang tidak diinginkan karena terdapat fitur deteksi dini yang telah disematkan pada server.

DAFTAR PUSTAKA

[1] Amaludin, L., 2022. *Model Pembelajaran Problem Base Leanning Penerapan dan Pengaruhnya Terhadap Keterampilan Berpikir Kritis dan Hasil Belajar*. Tangerang: Pascal Books.

[2] Switri, E., Apriyanti & Zaimuddin, 2021. *Penerapan Metode Manhaji Pada Pembelajaran Bahasa Arab*. Pasuruan Jawa Timur: Penerbit Qiara Media.

[3] Dasmen, R. N., Ariyanto, C., Surya, M. H. & Ramadhan, H., 2022. Penerapan Snort Sebagai Sistem Pendeteksi Serangan Keamanan Jaringan. *Jurnal Riset Sistem Informasi dan Teknik Informatika (JURASIK)*, Volume Vol.7 No.1 ISSN.2527-5771.

[4] Sau, W. M. & Siswantyo, S., 2021. Analisis Penggunaan Hasil Deteksi IDS Snort Pada Tools RITA Dalam Mendeteksi Ativitas Beacon. *Jurnal Info Kripto*, Volume Vol.15 No.2.

[5] Gunawan, A. R., Sastra, N. P. & Wiharta, D. M., 2021. Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware. *Majalah Ilmiah Teknologi Elektro*, Volume Vol.20. No.1 e-ISSN:2503-2372.

P-ISSN 1858-2680
E-ISSN 2723-4673

[6] Purba, W. W. & Efendi, R., 2020. Perancangan dan Analisis Sistem Keamanan Jaringan Komputer Menggunakan Snort. *Aiti Jurnal Teknologi Informasi*, Volume Vol.17 No.2 e-ISSN:2615-7128.

[7] Dar, M. H. & Harahap, S. Z., 2018. Implementasi Snort Intrusion Detection System (IDS) Pada Sistem Jaringan Komputer. *Jurnal Informatika*, Volume Vol.6 No.3 e-ISSN:2615-1855.

[8] Sutarti, Pancaro, A. P. & Saputra, F. I., 2018. Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal Prosisko* , Volume Vol.5 No.1 e-ISSN:2597.9922.

[9] Sihotang, S. & Pangaribuan, H., 2023. Rancang Bangun Instrusion Detection System (IDS) Menggunakan Snort (Studi Kasus : PT. PLN Batam). *Jursima (Jurnal Sistem Informasi Dan Manajemen)*, Volume Vol.11 No.1 ISSN:2338-1523.

[10] Anggraini, M. A. N., 2018. Uji Fitur Intrusion Prevention Pada Firewall Untangle Dengan Pengujian DOS dan SSH Brute Force. *Jurnal Manajemen Informatika*, Volume Vol.9 No.1.

[11] Simargolang, M. Y., Widarma, A. & Irawan, M. D., 2021. *Jaringan Komputer*. Medan: Yayasan Kita Menulis.

[12] Husen, Z. & Surbakti, M., 2020. *Membangun Server dan Jaringan Komputer Dengan Linux Ubuntu*. Aceh: Syiah Kuala University Press.

[13] Hanafi, M. & Habibi, R., 2020. *Cara Mudah Desain Sistem Operasi Linux Ubuntu 16.04 LTS Edition Dalam 5 Jam*. Bandung: Kreatif Industri Nusantara.

[14] Anggrawan, A., 2018. *Algoritma dan Pemrograman Implementasi Pada VB.Net dan Java*. Pertama penyunt. Yogyakarta: Andi Publisher.

P-ISSN 1858-2680
E-ISSN 2723-4673