Penerbit ADM RUMAH PENGETAHUAN
Jurnal KOMITEK
Jurnal Komputer, informasi Dan Teknologi

Implementation of Snort as a Wireless Network Security Detection Tool Using Linux Ubuntu

Implementasi Snort Sebagai Alat Pendeteksi Keamanan Jaringan Wireless Menggunakan Linux Ubuntu

Puteri Puji Insani [1]; Indra Kanedi [2]; Abdussalam Al Akbar [3]

[1] ***Universitas Dehasen Bengkulu***

Email: [1] puteripujiinsani12@gmail.com

How to Cite :

Insani, P,P. Kaned, I. Akbar, A, A. (2023). Implementation of Snort as a Wireless Network Security Detection Tool Using Linux Ubuntu. Jurnal Komputer, Informasi dan Teknologi, 3 (2). DO: https://do.org/10.53697/jkomitek.v3.2

ARTICLE HISTORY

Received [13 September 2023]
Revised [26 November 2023]
Accepted [15 Desember 2023]

KEYWORDS

Snort, Network Security, Linux Ubuntu

ABSTRAK

Implementasi snort sebagai alat pendeteksi keamanan jaringan wireless menggunakan linux ubuntu dengan menambahkan server yang digunakan untuk mengamati aktifitas pada jaringan wireless, jika terdapat suatu aktifitas yang dianggap membahayakan yang dilakukan oleh client, maka akan tersimpan informasi tersebut di dalam log snort dan database. 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. Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa implementasi snort sebagai alat pendeteksi keamanan jaringan wireless menggunakan linux ubuntu dapat membantu mendeteksi serangan yang terjadi dalam jaringan dan memberikan informasi terkait serangan tersebut

ABSTRACT

Implementation of snort as a wireless network security detection tool using linux ubuntu by adding a server that is used to observe activities on a wireless network, if there is an activity that is considered dangerous by the client, the information will be stored in the snort log and database. The web-based front-end uses BASE (Basic Analysis and Security Engine) which can be accessed through a browser with the url : IPaddressServer/base/. The information provided is related to attacks detected by snort that have been stored in the database. The information is in the form of source and destination IP addresses, the type of attack that occurred. Based on the tests carried out, it was found that the implementation of snort as a wireless network security detection tool using linux ubuntu can help detect attacks that occur on the network and provide information related to these attacks.

PENDAHULUAN

Suatu jaringan internet akan dapat memfasilitasi dan mewadahi pengguna untuk mengakses suatu situs, dan memanfaatkan informasi yang ada di situs tersebut. Saat mengakses suatu situs, pengguna akan mengalami suatu keadaan yang membuat pengguna tidak nyaman dalam melakukan aktifitas pengaksesan internet, misalnya pada saat akan mengakses link download atau membuka sebuah halaman dalam beberapa saat, akan terbuka suatu jendela-jendela baru di mana jendela-jendela tersebut berisikan konten-konten yang tidak diketahui dan tidak diinginkan oleh pengguna, konten tersebut bisa berisikan tentang media promosi, atau hal-hal yang bersifat pornografi yang apabila anak-anak dibawah usia 18 tahun mengaksesnya dan melihat hal tersebut tentu dapat memicu rusaknya perilaku perkembangan anak menjadi negatif. Permasalahan lain dengan adanya konten-konten yang tidak dinginkan oleh pengguna dapat mengakibatkan pemborosan kuota akses internet yang pada akhirnya pengguna akan merasa kuota dari akses internetnya lebih cepat habis dan menurunnya kecepatan untuk mengakses internet.

Hal lain yang sering dikhawatirkan pengguna saat melakukan aktifitas pengaksesan internet secara bebas ialah, pengguna tanpa sadar tidak memilah milih terlebih dahulu alamat website yang akan dituju apakah aman atau tidak dan dampak dari Malware yang bisa menginfeksi komputer sehingga mengakibatkan informasi-informasi yang bersifat privasi di suatu perusahaan ataupun personal yang apabila informasi tersebut dapat diakses dan disalahgunakan oleh malware atau orang lain secara umum, tentu dapat merugikan pemilik data tersebut ataupun perusahaan terebut.

Dari permasalahan yang telah penulis uraikan diatas, baik itu pengalaman pribadi penulis sendiri dan yang ada disekitar lingkungan penulis, maka penulis tertarik untuk membangun Network Security dengan menerapkan sistem operasi Linux Ubuntu Server dan Snort untuk memonitor keamanan jaringan, kenyamanan pengguna saat melakukan aktifitas akses internet dan keamanan informasi pengguna.

Linux Ubuntu adalah sistem operasi berbasis Linux (gratis) yang didesain khusus, mempunyai fitur - fitur untuk difungsikan sebagai firewall, sehingga Linux Ubuntu Server ini dilengkapi dengan aplikasi-aplikasi firewall seperti web filtering untuk mencegah akses ke situs web yang tidak diinginkan, spyware blocker melindungi komputer pengguna dari malware yang menginstal program sendiri tanpa izin dan kehendak user, dan Ad Blocker yang dapat membantu mengurangi tampilnya iklan-iklan online yang biasa terlihat di halaman suatu website yang akan menghabiskan lebih banyak kuota internet.

LANDASAN TEORI

Implementasi

Menurut Pertiwi (2021:43) Implementasi adalah penerapan dari sebuah desain sistem informasi yang telah diterapkan pada sebuah pemrograman komputer.

Implementasi mengacu pada tindakan untuk mencapai tujuan-tujuan yang telah ditetapkan dalam suatu keputusan. Tindakan ini berusaha untuk mengubah keputusan-keputusan tersebut menjadi pola-pola operasional serta berusaha mencapai perubahanperubahan besar atau kecil sebagaimana yang telah diputuskan sebelumnya. Implementasi pada hakikatnya juga merupakan upaya pemahaman apa yang seharusnya terjadi setelah program dilaksanakan.

Dalam tataran praktis, implementasi adalah proses pelaksanaan keputusan dasar. Proses tersebut terdiri atas beberapa tahapan yakni:

1.Tahapan pengesahan peraturan perundangan.
2.Pelaksanaan keputusan oleh instansi pelaksana.
3.Kesediaan kelompok sasaran untuk menjalankan keputusan.
4.Dampak nyata keputusan baik yang dikehendaki maupun tidak.
5.Dampak keputusan sebagaimana yang diharapkan instansi pelaksana.
6.Upaya perbaikan atas kebijakan atau peraturan perundangan.

Menurut Kamus Besar Bahasa Indonesia (2018:580) implementasi adalah pelaksanaan, yang jika penulis jabarkan pengertian implementasi dari kamus besar bahasa indonesia ialah melaksanakan konsep yang telah dirancang/didesain untuk kemudian dijalankan sepenuhnya agar tercapai tujuan yang diharapkan sebelumnya.

Proses persiapan implementasi setidaknya menyangkut beberapa hal penting yakni:

1.Penyiapan sumber daya, unit dan metode.
2.Penerjemahan kebijakan menjadi rencana dan arahan yang dapat diterima dan dijalankan.
3.Penyediaan layanan, pembayaran dan hal lain secara rutin. Dapat penulis simpulkan dari beberapa sumber diatas, implementasi dalam laporan penulis ini ialah penerapan dari hasil pengamatan, proses rancangan baru yang diperoleh dari kegiatan seleksi agar mendapatkan hasil yang terbaik saat akan dilaksanakan nantinya.

Tinjauan Snort

Menurut Fathoni (2019:1170) Snort salah satu software keamanan jaringan berbasis IDS. Snort bersifat open-source sehingga boleh dimodifikasi sesuai dengan kebutuhan. Dalam pengoprasiannya Snort dapat berjalan pada mode Packet Sniffer, packet logger dan Network Intrusion Detection. Pada mode sniffer Snort hanya akan melihat jaringan yang sedang diawasi tanpa melakukan apapun, pada mode packet logger Snort akan mencatat semua paket yang lewat dan pada Network Intrusion Detection Snort hanya akan mendeteksi adanya tindakan ancaman sesuari dengan setting dan rule yang diimplementasikan, pencatatan hanya dilakukan hanya ketika Snort mendeteksi adanya tindakan ancaman.

Snort yang dapat diperoleh di www.snort.org biasanya di sebut sebagai Network Intrusion Detection System (NIDS). Snort sendiri adalah Open Source yang tersedia di berbagai variasi Unix (termasuk Linux) dan juga Microsoft Windows.

Sebuah NIDS akan memperhatikan seluruh segmen jaringan dimana dia berada, berbeda dengan host based IDS yang hanya memperhatikan sebuah mesin dimana software host based IDS tersebut di pasang. Secara sederhana, sebuah NIDS akan mendeteksi semua serangan yang dapat melalui jaringan komputer (Internet maupun IntraNet) ke jaringan / komputer yang kita miliki.

Menurut Miftahul (2020:8) Snort IDS merupakan IDS open source yang secara de facto menjadi standar IDS di industri. Dapat diimplementasikan dalam jaringan yang multi platform. Salah satu kelebihannya adalah mampu mengirimkan alert dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui Server Messager Block (SMB). Snort dapat bekerja dalam 3 mode, mode penyadap (sniffer), packet logger dan mode network intrusion detection.

Snort adalah NIDS yang bekerja dengan menggunakan signature detection, berfungsi juga sebagai sniffer dan packet logger. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah open source project. Versi komersial dari snort dibuat oleh Sourcefire. Snort memiliki karakteristik, sebagai berikut :

1.Berukuran kecil – Source code dan rules.
2.Portable untuk banyak OS – Telah diporting ke Linux, Windows, OSX, Solaris, BSD, dan lain lain.
3.Cepat – Snort mampu mendeteksi serangan pada network.
4.Mudah dikonfigurasi – Snort sangat mudah dikonfigurasi sesuai dengan kebutuhan network kita. Bahkan kita juga dapat membuat rule sendiri untuk mendeteksi adanya serangan baru.
5.Free – Kita tidak perlu membayar sepeser pun untuk menggunakan snort. Snort bersifat open source dan menggunakan lisensi GPL.

Komponen Snort

Snort merupakan packet sniffing yang sangat ringan. Snifing interface yang digunakan berbasis libpcap (pada Unix tersedia dengan tcpdump, www.tcpdump.org). Pembuat snort sangat fokus pada engine yang digunakan untuk mendeteksi serangan dan memanfaatkan tools tcpdump

untuk mengambil paket network. Salah satu keunggulan snort adalah bahwa snort memiliki plugin sistem yang sangat fleksibel untuk dimodifikasi.

Snort memiliki beberapa komponen yang tiap komponennya mempunyai tugas masing-masing. Pada saat ada paket network yang melewati Ethernet di tempat snort dipasang, maka ada beberapa hal yang dilalui:

1. Packet Capture Library (libpcap).
   Packet capture library – akan memisahkan paket data yang melalui ethernet card untuk selanjutnya digunakan oleh snort.
2. Packet decoder.
   Packet decoder – mengambil data di layer 2 yang dikirim dari packet capture library (proses 1). Pertama ia akan memisahkan Data link (seperti ethernet, TokenRing, 802.11) kemudian protokol IP, dan selanjutnya paket TCP dan UDP. Setelah pemisahan data selesai, snort telah mempunyai informasi protokol yang dapat diproses lebih lanjut.
3. Preprocessor.
   Selanjutnya dilakukan analisis (preprocessor) atau manipulasi terhadap paket sebelum dikirim ke detection engine. Manipulasi paket dapat berupa ditandai, dikelompokan atau malah dihentikan.
4. Detection Engine.
   Inilah jantung dari snort. Paket yang datang dari packet decoder akan ditest dan dibandingkan dengan rule yang telah ditetapkan sebelumnya. Rule berisi tanda-tanda (signature) yang termasuk serangan.
5. Output.
   Output yang dihasilkan berupa report dan alert. Ada banyak variasi output yang dihasilkan snort, seperti teks (ASCII), XML, syslog, tcpdump, binary format, atau Database (MySQL, MsSQL, PostgreSQL, dsb).

Jaringan Komputer

Menurut Pratama (2019:12) Jaringan Komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain (a network is a interconnection of a set of device capable of communication). Perangkat yang dimaksud adalah semua jenis perangkat komputer (komputer desktop, laptop, smartphone, pc tablet).

Network Security

Menurut Munawar (2020:32) Network Security atau keamanan jaringan sebagai segala bentuk proses atau teknologi yang dibuat untuk melindungi integritas, kerahasiaan, dan ketersediaan aksesibilitas data dan jaringan komputer.Network security bertugas untuk melindungi perangkat keras (hardware) ataupun perangkat lunak (software). Sistem ini menargetkan berbagai ancaman siber, kemudian menghalangi masuknya ancaman tersebut ke dalam jaringan. Singkatnya, network security berupa rangkaian aturan dan konfigurasi untuk meningkatkan perlindungan terhadap jaringan komputer.Keamanan jaringan sangat penting bagi perusahaan atau organisasi, terutama pada zaman serba digital ini. Ancaman di dunia siber terus berkembang dan mengintai sehingga berpotensi menyerang sistem komputer Anda. Hacker akan selalu mencari cara untuk membobol pertahanan jaringan demi kepentingan mereka sendiri. Kerumitan arsitektur jaringan pun menjadi alasan pentingnya penerapan network security dalam perusahaan.Sehingga menurut penulis Network Security merupakan sebuah topik dengan cakupan yang sangat luas dan komples, sebelum penulis menjabarkan tentang network security, penulis akan menjelaskan terlebih dahulu.

Menurut Sulaiman (2019:73) keamanan jaringan atau Network Security adalah segala aktifitas yang dilakukan untuk mengamankan network, khususnya untuk melindungi kegunaan, kehandalan, kualitas, dan keamanan dari network dan data dengan bertujuan untuk mencegah dan menghentikan berbagai threats (potensi serangan) dari luar ataupun dari jaringan lokal, agar tidak memasuki dan menyebar pada network.

Keamanan komputer adalah bertujuan menjamin agar sumber daya informasi tidak digunakan atau dimodifikasi oleh orang yang tidak berhak. Pengamanan termasuk masalah teknis, manajerial, legalitas. Sistem keamanan terbagi menjadi tiga, yaitu:

a)Keamanan eksternal, adalah pengamanan yang berhubungan dengan fasilitas komputer dari penyusup dan bencana, seperti bencana alam.

b)Keamanan interface pemakai, berkaitan dengan indentifikasi pemakai sebelum pemakai diizinkan mengakses program dan data yang disimpan.

c)Keamanan internal, berkaitan dengan pengamanan beragam yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang andal dan tidak hilang untuk menjaga keutuhan program dan data.

Dari berbagai pengertian menurut para ahli, penulis mencoba menyimpulkan Network Security adalah perlindungan atau pengamanan jaringan beberapa komputer yang terhubung dengan kabel atau nirkabel baik itu server ataupun client terhadap serangan/kegagalan bertahan ketika ada celah-celah yang akan menggangu keamanan jaringan yang berkaitan dengan melindungi data, perangkat keras, dan perangkat lunak pada jaringan komputer baik itu dari keamanan luar atau dari dalam jaringan tersebut.

Pengertian Server

Menurut Kristiyanto (2021 :44) pada umumnya didalam sistem operasi terdapat berbagai macam service yang menggunakan arsitektur client/server. Contoh dari service ini adalah DHCP Server, Mail Server, Web Server, FTP server, DNS Server dan sebagainya. Setiap sistem operasi yang digunakan untuk server biasanya sudah disediakan layanan-layanan tersebut disamping layanan tersebut bisa didapatkan dari pihak ketiga. Sistem Operasi yang digunakan sebagai server, biasanya tidak memerlukan GUI dan bersifat psional, Namun saat ini banyak sekali komputer desktop dengan GUI dapat digunakan sebagai server namun sangat sedikit yang menggunakannya. Server biasanya terhubung dengan client dengan kabel UTP dan sebuah Network Card.

Pada komputerisasi, server merupakan kombinasi dari perangkat keras dan perangkat lunak yang dirancang untuk menyediakan layanan untuk klien pada sebuah jaringan komputer. Server didukung oleh prosesor yang bersifat scalable dan penggunaan ram yang besar, juga dilengkapi dengan sistem operasi khusus yang disebut sebagai sistem operasi jaringan. Server juga digunakan untuk menjalankan perangkat lunak administratif yang mengontrol akses terhadap jarngan dan sumber daya yang terdapat didalamnya.Menurut Nugroho (2020:22) Server bisa diartikan sebagai peladen atau pelayan dalam bahasa Indonesia. Pengertiannya adalah sistem komputer yang memiliki fitur khusus yaitu sebagai penyimpanan data. Di dalam server tersimpan data berupa informasi serta berbagai jenis dokumen yang sifatnya kompleks.

Fitur khusus tersebut ditujukan untuk memenuhi kebutuhan para pengguna. Pengguna membutuhkan informasi dan data secara langsung. Sehingga, server wajib menyajikan data sesuai dengan permintaan pengguna. Mengingat jumlah pengguna tidak hanya satu atau dua, server diwajibkan untuk bisa diakses dengan cepat, baik dalam menerima request atau mengirimkan data kepada user.

Linux

Menurut Hasibuan (2019:28) Linux merupakan sebuah nama sistem operasi berbasis Unix yang didistribusikan kepada publik dan memiliki GNU General Public License (GPL) secara gratis, yang berarti jika Linux dibagikan dengan source code-nya. Akses ke kode sumber memungkinkan pengguna untuk menyesuaikan sistem operasi ini, yang kemudian dapat digunakan kembali dan didistribusikan secara bebas.

Linux tidaklah menjadi hal yang awam untuk dibicarakan di dunia teknologi informasi. Linux adalah nama yang diberikan kepada sistem operasi komputer berbasis Unix. Linux merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama (Open

Source). Seperti perangkat lunak bebas dan sumber terbuka lain pada umumnya, kode sumber Linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapapun. Nama "Linux" berasal dari nama kernelnya (kernel Unux), yang dibuat tahun 1991 oleh Linus Torvalds. Sistemnya, peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU adalah dasar dari muneulnya nama alternatif GNU/Linux. Sistem operasi Linux yang dikenal dengan istilah distribusi Linux (Linux distribution) atau distro Linux umumnya sudah termasuk perangkat- perangkat lunak pendukung seperti server web, bahasa pemrograman, basisdata, tampilan desktop (desktop environment) (seperti GNOME dan KDE), dan paket aplikasi perkantoran (office suite) seperti OpenOffice.org, KOffice, Abiword, dan Gnumeric.

Menurut Onno (2019:41) Nama Linux sendiri diambil dari nama penciptanya, Linus Torvalds, untuk informasi lebih lanjut tentang sejarah Linux, yang akan dibahas pada artikel berikut. Kernel Linux merupakan perbedaan terbesar antara Linux dan sistem operasi populer lainnya dengan memiliki komponen yang tersedia yang bisa diakses secara terbuka dan juga bebas.

Sebuah sistem Linux umumnya menyediakan sebuah antarmuka baris perintah lewat sebuah shell, yang merupakan cara tradisional untuk berinteraksi dengan sebuah sistem Unix. Sebuah distro Linux yang dikhususkan untuk lingkungan server mungkin hanya memiliki CLI (Command Line Interface) sebagai satu-satunya antarmuka. Sebuah sistem yang tidak memiliki monitor hanya dapat dikontrol melalui baris perintah lewat protokol seperti SSH atau telnet. Kebanyakan komponen tingkat rendah Linux, termasuk GNU Userland, menggunakan ell secara ekslusif. CLI cocok untuk digunakan pada lingkungan otomasi tugas-tugas yang repetitif atau tertunda, dan menyediakan komunikasi interproses yang sangat sederhana. Sebuah program emulator terminal grafis sering digunakan untuk mengakses CLI dari sebuah Linux desktop. Perbedaan utama antara Linux dan sistem operasi popular lainnya terletak pada kernel Linux dan komponen-komponennya yang bebas dan terbuka. Linux bukan satu-satunya sistem operasi dalam kategori tersebut, walaupun demikian Linux adalah contoh terbaik dan terbanyak digunakan. Beberapa lisensi perangkat lunak bebas dan sumber terbuka berdasarkan prinsip-prinsip copyleft, sebuah konsep yang menganut prinsip: karya yang dihasilkan dari bagian copyleft harus juga merupakan copyleft. Lisensi perangkat lunak bebas yang paling umum, GNU GPL, adalah sebuah bentuk copyleft, dan digunakan oleh kernel Linux dan komponen-komponen dari proyek GNU.

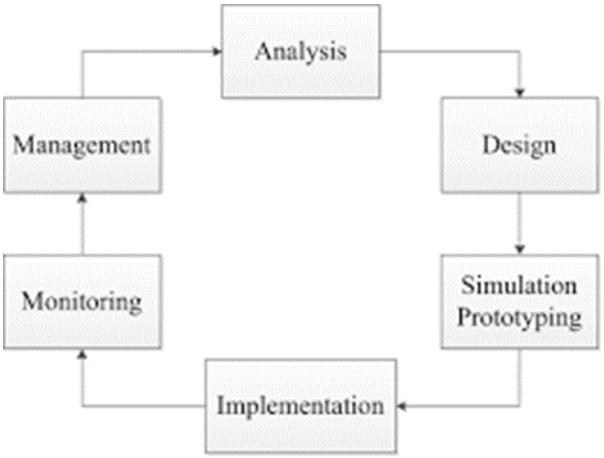
Linux dikendalikan oleh pengembang dan komunitas penggunanya. 8eberapa vendor mengembangkan dan mendanai distribusi mereka sendiri dengan dasar kesukarelaan. Debian merupakan contoh yang bagus. Yang lain memiliki versi komunitas dari versi komersialnya seperti yang Red Hat lakukan dengan Fedora. Di banyak kota dan wilayah, asosiasi lokal yang dikenal dengan nama Kelompok Pengguna Linux (Linux Users Group atau LUG) mempromosikan Linux dengan mengadakan pertemuan, demonstrasi, pelatihan, dukungan teknis dan instalasi sistem operasi Linux secara gratis. Ada banyak juga komunitas Internet yang menyediakan dukungan terhadap pengembang dan pengguna Linux. 8anyak proyek distribusi dan perangkat lunak sumber terbuka yang memiliki ruang percakapan IRe atau newsgroup. Forum daring merupakan bentuk lain untuk mendapatkan dukungan, contoh: Linux Questions.org dan forum Gentoo. Distribusi Linux memiliki [milis] dengan pembagian topik seperti penggunaan atau pengembangan

METODE PENELITIAN

Metode Analisis

Dalam melakukan pengembangan system, penulis akan menggunakan metode Network Development Life Cycle (NDLC) untuk implementasi Snort sevagai alat pendeteksi keamanan jaringan wireless menggunakan linux ubuntu. Metode tersebut terdiri dari analysis, design, simulation prototype, implementation, dan monitoring. Berikut merupakan tahapan dari metode NDLC sebagai berikut:

Gambar 1 Sirkulasi Metode NDLC



Adapun penjelasan dari tahapan diatas yaitu sebagai berikut;

1. Tahap Analysis, Tahapan awal yang dilakukan dalam menganalisis adalah analisa kebutuhan, analisa permasalahan yang ada, analisa keinginan user, dan analisa topologi jaringan yang sudah ada, bisa dibilang tahapan ini adalah tahapan pengumpulan data yang dibutuhkan untuk perumusan masalah dalam menyelesaikan kendala yang ada. Dengan mengidentifikasi sistem yang sedang berjalan lalu mencoba untuk menganalisa suatu pengembangan sistem seperti apa yang akan diterapkan pada sistem tersebut
2. Tahap Design, Tahap ini dari data-data yang didapatkan sebelumnya, tahapan desain ini penulis akan membuat desain gambar topologi jaringan yang akan dibangun, desain akses data dan sebagainya. Dalam penelitian ini penulis menggunakan aplikasi Microsoft Visio, GNS3 dan Corel Draw
3. Tahap Simulation Prototype, Tahap ini melakukan pengembangan jaringan yang akan membuat dalam bentuk simulasi dengan bantuan tools GNS3. Hal ini dimaksudkan untuk melihat kinerja dari network yang akan dibangun dan menjadi bahan presentasi dan sharing dengan pengembangan system jaringan,
4. Tahap Implementation, Tahap ini akan sedikit memakan waktu lama. Dalam melakukan implementasi, penulis telah menerapakan semua yang direncanakan dan dirancang sebelumnya. Pada tahapan ini akan terlihat bagaimana pengembangan yang akan dibangun akan memberikan pengaruh terhadap system (jaringan) yang ada,
5. Tahap Monitoring, Tahap ini Setelah diimplementasi, tahapan monitoring merupakan tahapan penting agar jaringan dan komunikasi dapat berjalan sesuai dengan keinginan dan tujuan penulis pada tahap awal analisis.
6. Tahap Management, Tahap ini salah satu yang menjadi perhatian khusus adalah masalah kebijakan, yaitu dalam dalam hal aktivitas, pemeliharaan dan pengelolahan dikategorikan pada tahap ini. Kebijakan perlu dibuat untuk membuat dan mengatur agar sistem yang telah dibangun dan berjalan dengan baik dapat berlangsung lama dan unsur reliability terjaga

HASIL DAN PEMBAHASAN

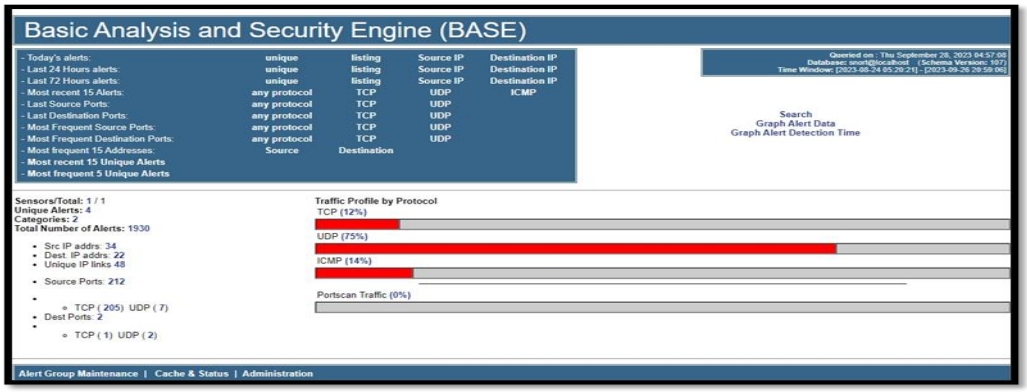
Hasil

Implementasi snort sebagai alat pendeteksi keamanan jaringan wireless menggunakan linux ubuntu dengan menambahkan server yang digunakan untuk mengamati aktifitas pada jaringan

wireless, jika terdapat suatu aktifitas yang dianggap membahayakan yang dilakukan oleh client, maka akan tersimpan informasi tersebut di dalam log snort dan database.

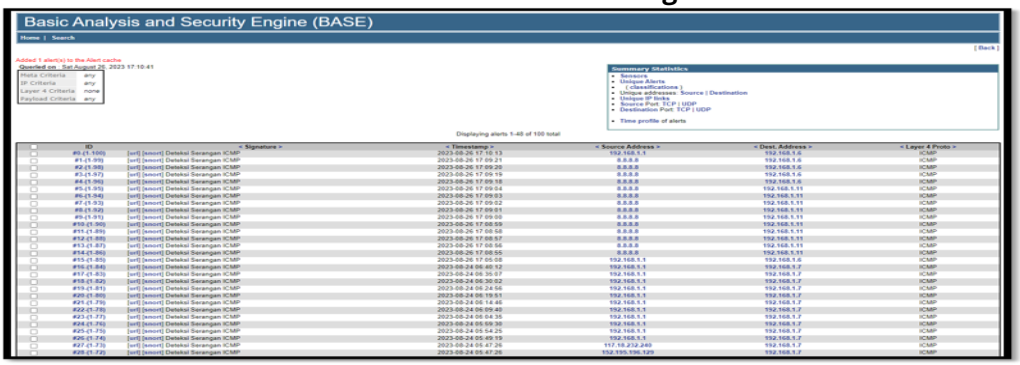
Untuk mempermudah dalam mengetahui informasi serangan yang terjadi tersebut, dibangun front-end berbasis web menggunakan BASE (Basic Analysis and Security Engine) yang dapat diakses melalui browser dengan url : IPaddressServer/base/, sehingga akan menampilkan halaman BASE seperti terlihat pada Gambar 2.

Gambar 2 Front-End Web BASE



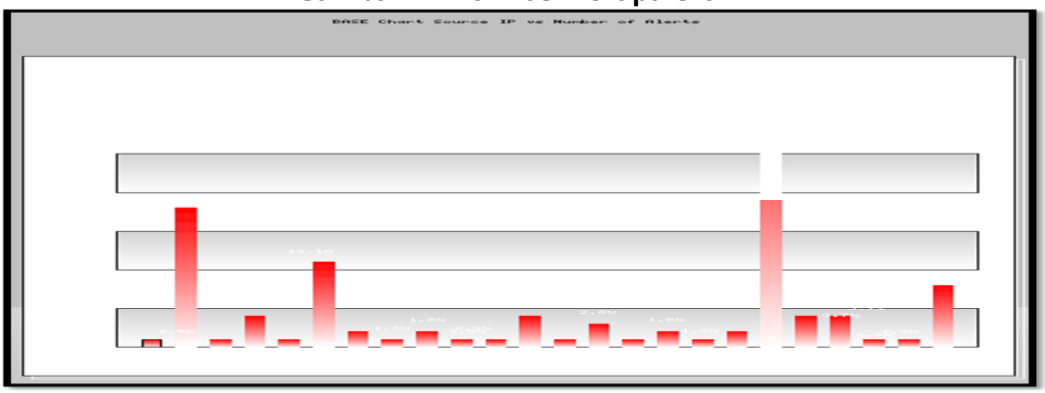
Pada Gambar 2 tersebut terlihat bahwa terdapat informasi-informasi yang diberikan terkait serangan yang terdeteksi oleh snort yang telah tersimpan ke dalam database. Informasi tersebut berupa IP Address sumber dan tujuan, jenis serangan yang terjadi, seperti Gambar 3.

Gambar 3 Informasi Serangan



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, seperti terlihat pada Gambar 4.

Gambar 4 Informasi Berupa Grafik



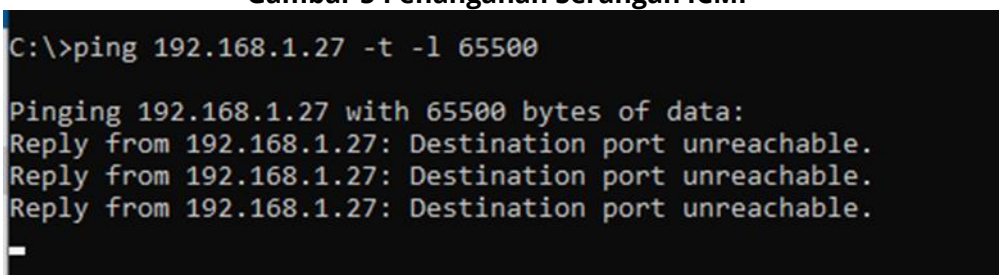
Setelah snort mendeteksi serangan seperti terlihat pada BASE, maka administrator dapat melakukan blokir serangan tersebut melalui iptable, dengan menambahkan rules sebagai berikut :

1.Penanganan Serangan ICMP

Iptables -A INPUT -s IP Penyerang -p icmp --icmp-type 8 -m conntrack --ctstate NEW -j DROP

Dengan rule tersebut, IP penyerang tidak dapat melakukan ping seperti terlihat pada Gambar 5.

Gambar 5 Penanganan Serangan ICMP



2.Penanganan Serangan TCP

Iptables -A INPUT -s IP Penyerang -p tcp --dport 80 -j DROP Dengan rule tersebut, IP penyerang tidak dapat melakukan serangan TCP, seperti terlihat pada Gambar 6.

Gambar 6 Penanganan Serangan TCP

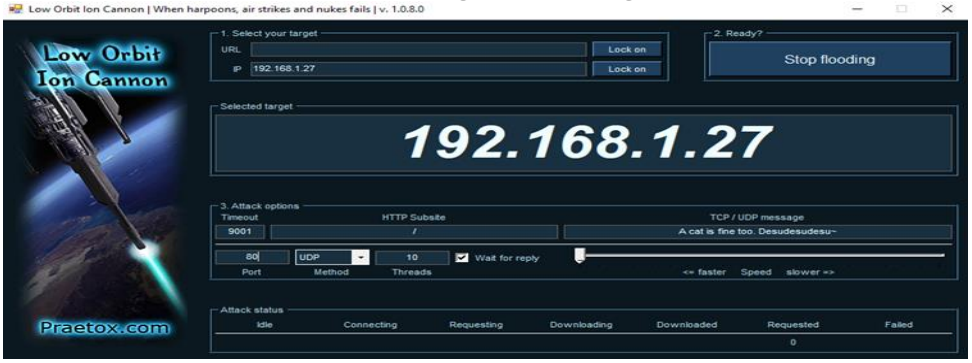
3.Penanganan Serangan UDP

Iptables -I INPUT -s IP Penyerang -p udp --dport 80 -j DROP

Iptables -I INPUT -s IP Penyerang -p udp --dport 53 -j DROP

Dengan rule tersebut, IP penyerang tidak dapat melakukan serangan TCP, seperti terlihat pada Gambar 7.

Gambar 7 Penanganan Serangan UDP



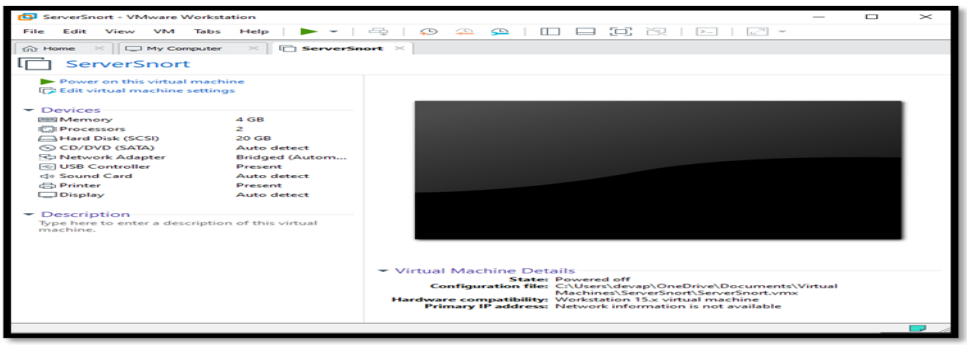
Pembahasan

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

1.Menyiapkan Server

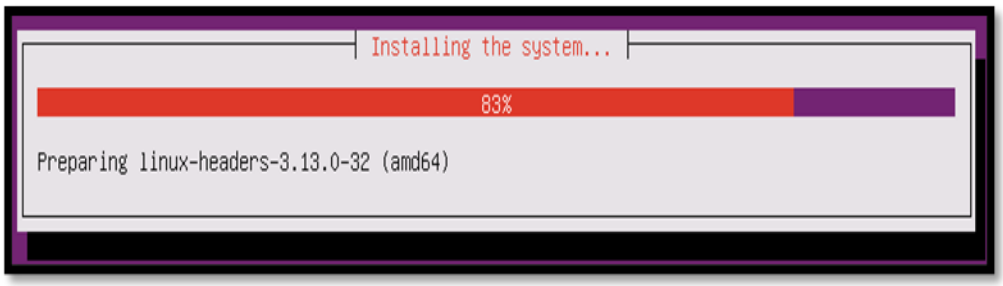
Tahap ini server yang digunakan berupa Virtual Machine yang dapat diakses melalui VMWare dimana jaringan dibuat brigde sehingga dapat terkoneksi dengan jaringan luar, seperti Gambar 8.

Gambar 8 Virtual Machine Server



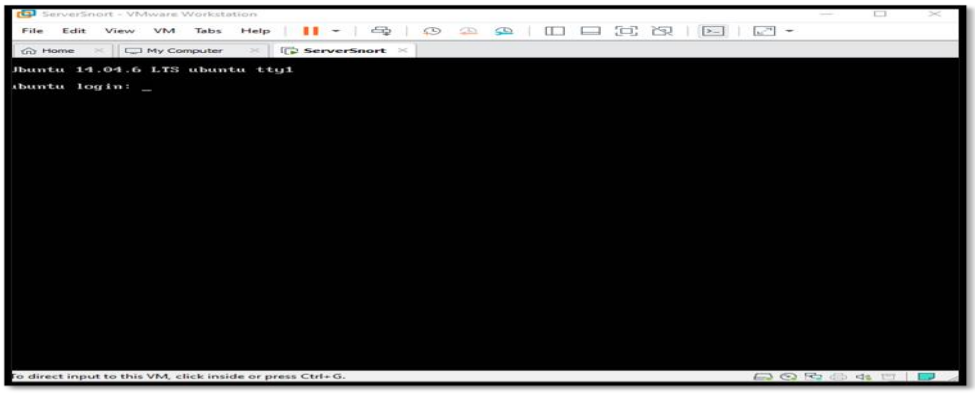
2.Instalasi sistem operasi linux ubuntu server pada Virtual Machine server tersebut, sehingga terlihat seperti Gambar 9.

Gambar 9 Instalasi Linux Ubuntu Server



Setelah instalasi linux ubuntu server selesai, maka akan menampilkan halaman utama dari linux ubuntu server seperti terlihat pada Gambar 10.

Gambar 10 Linux Ubuntu Server



3.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.gzcd snort-2.9.9.0./configure --enable-sourcefiremake make install
Kemudian melakukan konfigurasi snort dengan perintah :
nano /etc/snort/snort.conf sehingga menampilkan informasi seperti Gambar 11.

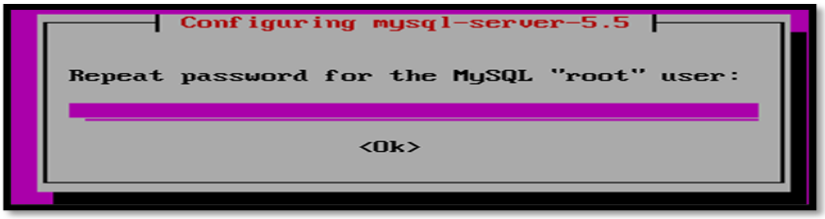
Gambar 11 Konfigurasi Snort

4.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 12.

Gambar 12 Password Root Database MySQL



5.Instalasi Barnyard2

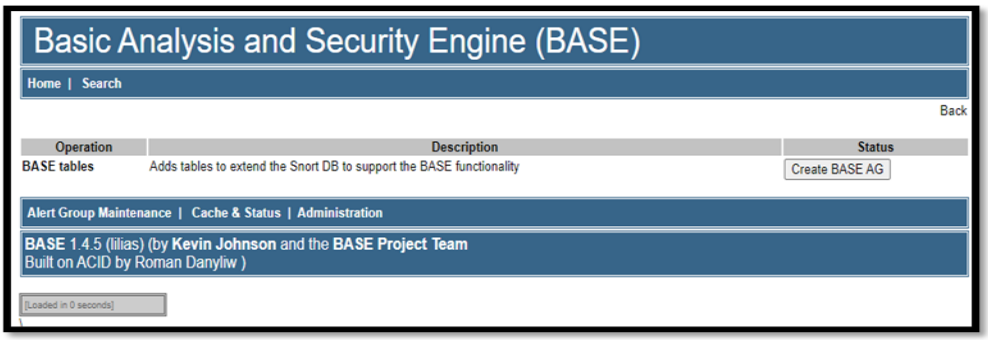
Barnyard2 digunakan untuk memproses paket-paket yang telah terdeteksi oleh snort yang kemudian menyimpannya ke dalam database MySQL. Adapun perintah yang digunakan untuk instalasi Barnyard2 seperti :

cd ~/snort_srcwget https://github.com/firnsy/barnyard2/archive/master.tar.gz -O barnyard2-Master.tar.gztar zxvf barnyard2-Master.tar.gzcd barnyard2-masterautoreconf -fvi -I ./m4./configure --with-mysql --with-mysql-libraries=/usr/lib/x86_64-linux-gnu make make install

6.Instalasi BASE

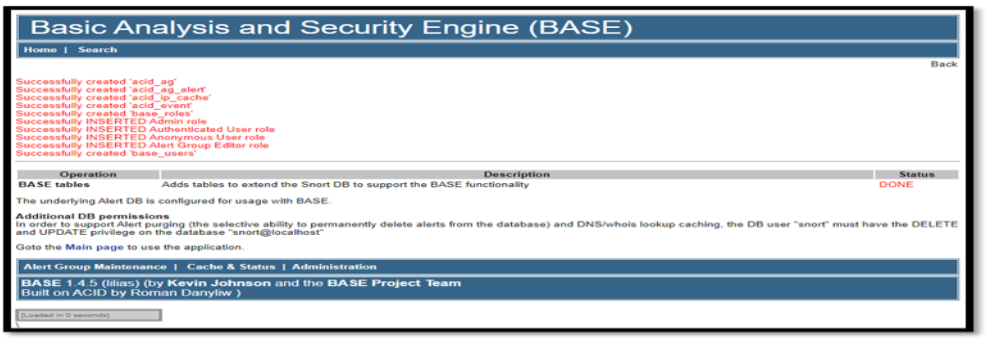
Pada tahap ini dilakukan instalasi BASE dengan cara membuka browser melalui client kemudian ketik IPAddressServer/base/, sehingga akan menampilkan halaman setup page BASE, seperti Gambar 13.

Gambar 13 Setup Page BASE



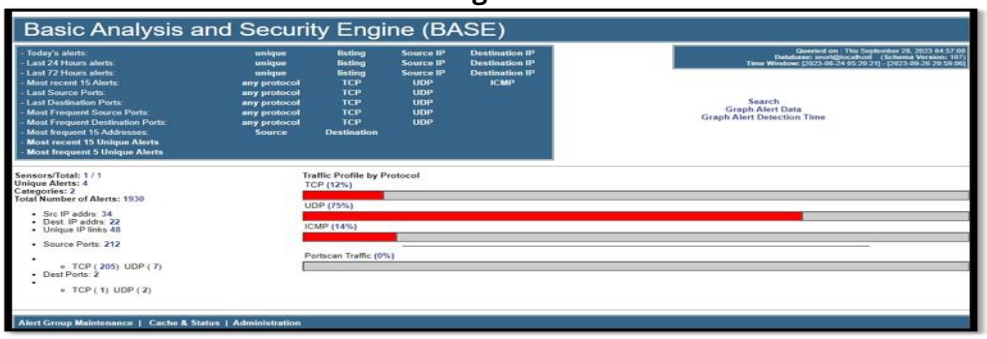
Create Base AG untuk instalasi front-end web BASE, sehingga menampilkan informasi seperti Gambar 14.

Gambar 14 Instalasi Front-End Web Base



Setelah berhasil, masuk ke main page untuk melihat informasi-informasi serangan yang terjadi pada jaringan, seperti terlihat pada Gambar 15.

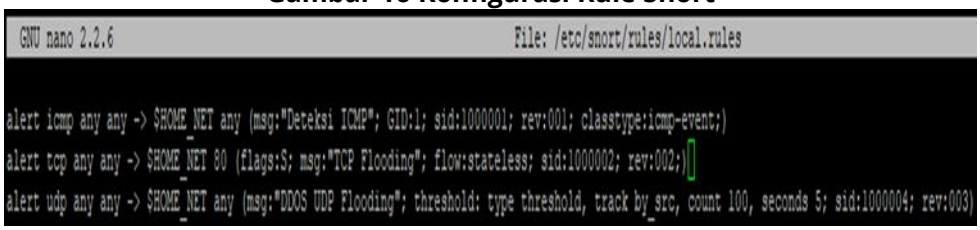
Gambar 15 Main Page Front-End Web Base



7.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 dan menampilkan rule-rule yang telah dibuat seperti Gambar 16.

Gambar 16 Konfigurasi Rule Snort



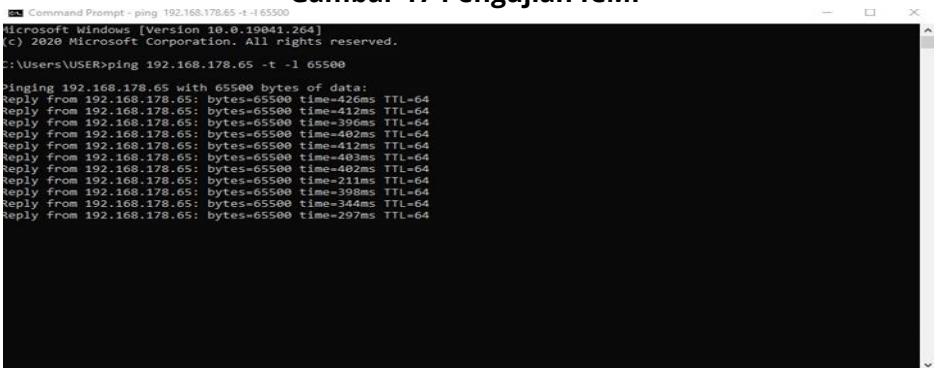
Setelah selesai membuat rule, ketik perintah untuk melakukan verifikasi terhadap rule yang telah dibuat :snort -T -i eth0 -c /etc/snort/snort.conf

8.Menjalankan Service Snort dan Barnyard2 dengan perintah :
service snort start
sevicer barnyard2 start

Pengujian ICMP

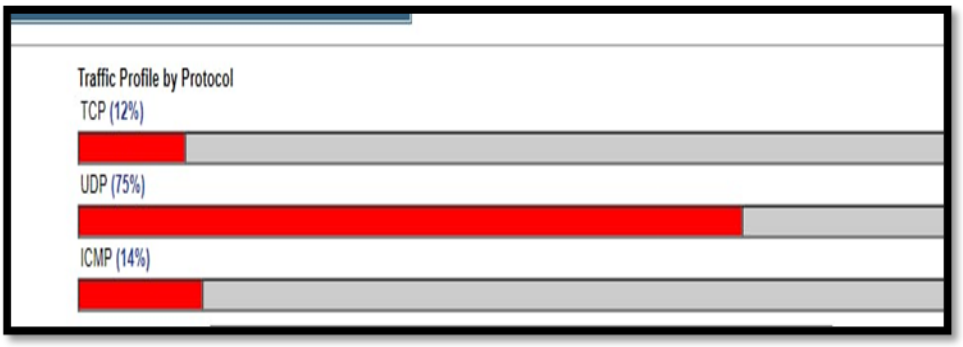
Pengujian ICMP dilakukan dengan perintah ping secara terus menerus pada IP Address tujuan, seperti terlihat pada Gambar 17.

Gambar 17 Pengujian ICMP



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 18.

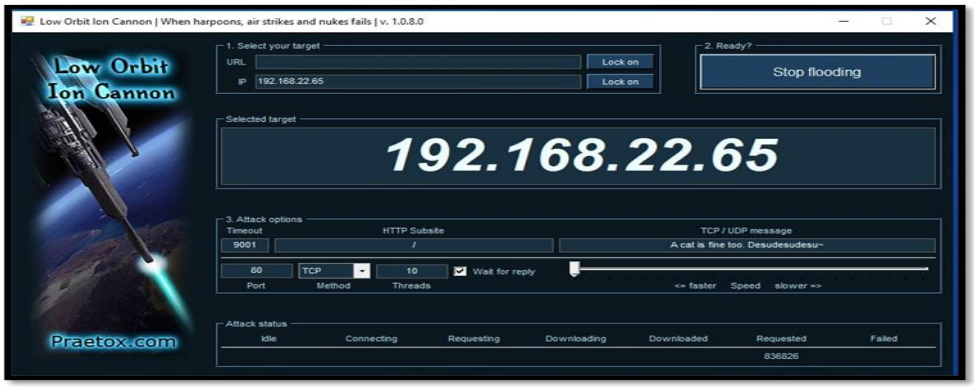
Gambar 18 Deteksi Snort Melalui Base



5.Pengujian TCP Flooding

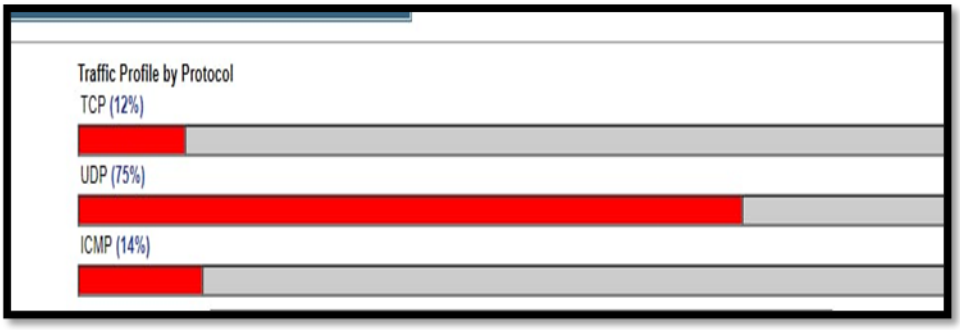
Pengujian TCP Flooding dilakukan menggunakan tools LOIC dengan memasukkan IP Address dan tipe serangan TCP Flooding pada LOIC, seperti terlihat pada Gambar 19.

Gambar 19 Pengujian TCP Flooding



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 19.

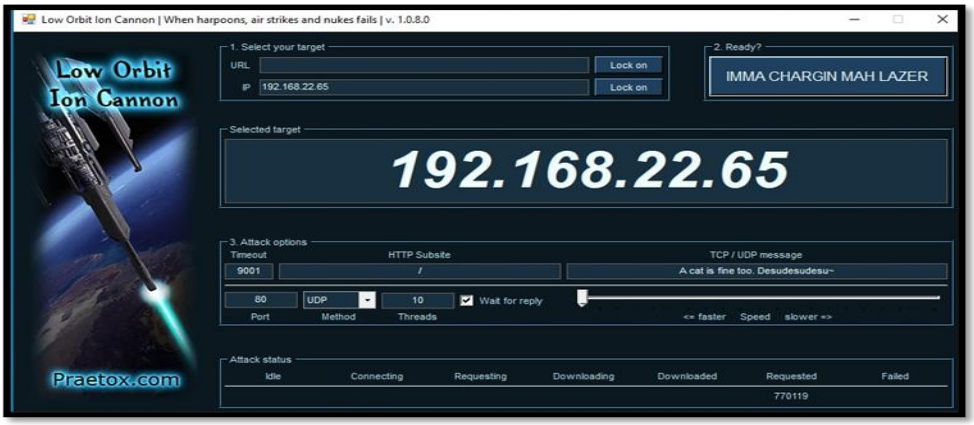
Gambar 20 Deteksi Snort Melalui Base



6.Pengujian UDP Flooding

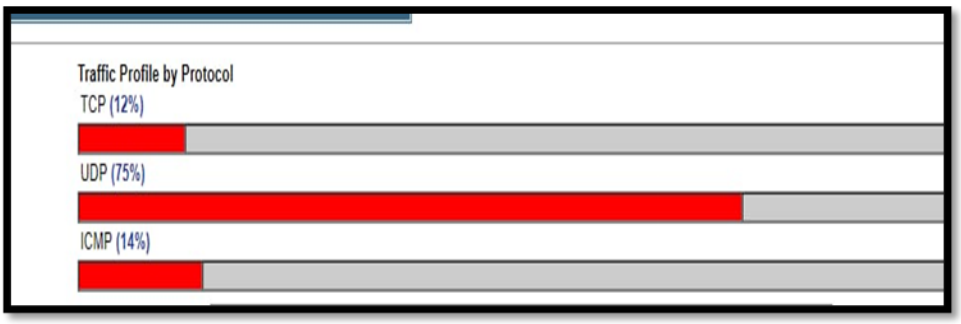
Pengujian UDP Flooding dilakukan menggunakan tools LOIC dengan memasukkan IP Address dan tipe serangan UDP Flooding pada LOIC, seperti terlihat pada Gambar 21.

Gambar 21 Pengujian UDP Flooding



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 22.

Gambar 22 Deteksi Snort Melalui Base



Berdasarkan pengujian yang dilakukan, didapatkan hasil bahwa implementasi snort sebagai alat pendeteksi keamanan jaringan wireless 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.

KESIMPULAN DAN SARAN

Kesimpulan

1. Implementasi snort sebagai alat pendeteksi keamanan jaringan wireless menggunakan linux ubuntu dengan menambahkan server yang digunakan untuk mengamati aktifitas pada jaringan wireless, jika terdapat suatu aktifitas yang dianggap membahayakan yang dilakukan oleh client, maka akan tersimpan informasi tersebut di dalam log snort dan database.
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 pengujian yang dilakukan, didapatkan hasil bahwa implementasi snort sebagai alat pendeteksi keamanan jaringan wireless menggunakan linux ubuntu dapat membantu mendeteksi serangan yang terjadi dalam jaringan dan memberikan informasi terkait serangan tersebut.

Saran

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

DAFTAR PUSTAKA

Fathoni, Medy Wisnu. 2019. Perbandingan Nilai Akurasi Snort dan Suricata dalam Mendeteksi Intrusi Lalu Lintas di Jaringan. Jurnal Info Kripto. Program Studi Sistem Informasi STMIK Profesional Makassar

Hasibuan, Doli. 2019. Analisis Dan Implementasi Jaringan Thin Client Menggunakan Linux Terminal Server Project Pada Jaringan LAN. Jurnal METHODIKA. Fakultas Ilmu Komputer, Universitas Methodist Indonesia

Kamus Besar Bahasa Indonesia (2018:580) Edisi Revisi. Kementrian Pendidikan dan Kebudayaan

Kristiyanto, Ari. 2019. Virtualisasi menggunakan Xen Hypervisor seebagai efisiensi penggunaan server (PT. Smart Intermedia Solusindo). Fakultas Sains Dan Teknologi UIN Syarif Hidayatullah Jakarta

Miftahul Jannah. 2020. Implementasi Intrusion System (IDS) Snort Pada Laboratorium Jaringan Komputer. UG Jurnal. Fakultas Teknik Informatika Universitas Gunadarma

Munawar, Zen. 2020. Keamanan Jaringan Komputer Pada Era Big Data. Jurnal Sistem Informasi – J-SIKA. Teknik Informatika, Fakultas Teknologi Informasi Universitas Bale Bandung

Nugroho, Anggun. 2020. Perancangan Sistem Informasi Pengelolaan Aset UKM (Unit Kegiatan Mahasiswa) STMIK STIKOM Bali Berbasis Client Server. Konferensi Nasional Sistem & Informatika 2020. Program Studi Sistem Komputer STMIK STIKOM Bali

Pratama, Aditya Wisnu. 2019. Konfigurasi Inter-Vlan Pada Cisco Berbasis Graphics User Interface (GUI) Sebagai Pembelajaran Peralatan Jaringan Komputer Cisco. Jurusan Teknik Informatika. Sekolah Tinggi Teknologi Adisutjipto Yogyakarta

Pertiwi, Dini Hari. 2021. Implementasi Program Tahfidz Dalam Pembinaan Kecerdasan Spiritual Peserta Didik Di Madrasah Aliyah Negeri 2 Jember Tahun Pelajaran 2021/2022. Fakultas Tarbiyah Dan Ilmu Keguruan. Universitas Islam Negeri Kiai Haji Achmad Siddiq Jember.

Sulaiman, Oris Krianto. 2019. Analisis Sistem Keamanan Jaringan Dengan Menggunakan Switch Port Security. CESS (Journal Of Computer Engineering, System And Science). Universitas Islam Sumatera Utara