ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

IMPLEMENTASI KEAMANAN WIRELESS LAN MENGGUNAKAN SNORT DAN IPTABLES

Harri Agustian[(1)], Toibah Umi Kalsum[(2)], Hendri Alamsyah[(2)]

[1,2,3)]Study Program Of Computer Systems Engineering Faculty Of Computer UniversitasDehasen Bengkulu

Email:[1)]Harri Agustian@gmail.com);[2)]Cicik.umie@gmail.com;hendri.alamsyah@unived.ac.id

How to Cite :
Harri Agustian,Toibah Umi Kalsum, Hendri Alamsyah. 2020. IMPLEMENTASI KEAMANAN WIRELESS LAN MENGGUNAKAN SNORT DAN IPTABLES. GATOTKACA Journal.
*DOI:Https://Doi.Org/*10.37638/Gatotkaca.1.1.42-57

ARTICLE HISTORY
Received [12Januari 2020]
Revised [16 Februari 2020]
Accepted [20 Maret 2020]

KEYWORDS
Snort, Keamanan Jaringan, Ubuntu Server

ABSTRAK

Ringkasan,-Penelitian ini bertujuan untuk melakukan implementasi keamanan wireless LAN menggunakan snort dan iptables. Dan juga sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada jurusan rekayasa sistem komputer universitas Dehasen Bengkulu. Metode penelitian yang dilakukan adalah menggunakan perancangan sistem sampai dengan implementasi sistem. Perancangan sistem yaitu menggambarkan bagaimana melakukan implementasi keamanan jaringan wireless LAN menggunakan snort dan iptables dengan sistem operasi Linux Ubuntu Server 16.04, sesuai dengan sarana dan prasarana yang ada di laboratorium komputer Universitas Dehasen Bengkulu.Snort dan Iptables berjalan dengan baik sesuai dengan tugasnya untuk melakukan keamanan jaringan, baik itu dari penggunaan CPU Usage sangat kecil, kemampuan snort dalam melakukan deteksi dan melakukan pembatasab akses terhadap alamat-alamat yang melakukan ancaman, Yang berarti Snort dan Iptables sangat baik digunakan untuk melakukan keamanan jaringan.

ABSTRACT

-This study aims to implement wireless LAN security using Snort and Iptables. And also as one of the requirements to obtain a Computer Bachelor's Degree in computer systems engineering at Dehasen University of Bengkulu. The research method used is to use system design to system implementation. The system design is to describe how to implement the security of a wireless LAN network using Snort and Iptables with the Linux operating system of Ubuntu Server 16.04, in accordance with the facilities and infrastructure available in the computer laboratory of Dehasen University of Bengkulu. Snort and Iptables run well in accordance with their duties to perform network security, both from the use of CPU

Usage is very small, the ability of snort to detect and restrict access to addresses that pose a threat, which means Snort and Iptables are very well used to do network security.

PENDAHULUAN

Keamanan jaringan komputer merupakan suatu kebutuhan yang sangat vital untuk diimplementasikan didalam sebuah jaringan komputer, apabila jaringan komputer tersebut terhubung ke jaringan luar, yang secara teknis tentu siapa saja dapat mengakses jaringan milik suatu perusahaan tersebut. Hal ini menjadi kendala apabila user luar yang mengakses, mempunyai suatu niat yang buruk terhadap segala macam komponen jaringan perusahaan, mulai dari data, Operating sistem dan lainnya.

Sistem Keamanan Komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia jaringan Komputer, hal ini disebabkan tingginya ancaman yang mecurigakan (Suspicious Threat) dan serangan dari internet. Keamanan Komputer (Security) merupakan salah satu kunci yang dapat memperangaruhi tingkat Realiability (Termasuk Performance dan Availability) suatu internetwork. Jika kita lihat dan beranjak dari data CSI/FBI Survey, saat ini telah banyak perusahaan yang membelanjakan uangnya untuk terhindar dari masalah keamanan ini dan sementara itu juga untuk mengamankan sistemnya, banyak perusahaan tersebut telah menggunakan sistem dengan menkombinasikan beberapa teknologi sistem keamanan. Dimana hampir 69% nya menggunakan solusi dari Instrusion Prevention Sistem (IPS).

Berdasarkan penelitian yang saya lakukan di Pusat Komputer (PUSKOM) merupakan salah satu unit pelaksana teknis dalam lingkungan Universitas Dehasen Bengkulu yang menangani server jaringan, web, dan sistem informasi dosen dan mahasiswa. Puskom universitas Dehasen Bengkulu pernah mengalami serangan pada wireless dalam bentuk penyadapan aktivitas admin pada saat terhubung ke wireless LAN tersebut. Maka dari pada itu perlunya untuk melakukan keamanan jaringan wireless LAN.

Dari uraian diatas maka peneliti tertarik untuk melakukan penelitian dengan judul yaitu "Implementasi Keamanan Wareless LAN Menggunakan Snort dan Iptables"

LANDASAN TEORI

Pengertian Implementasi

Menurut Cleaves (dalam wahab 2008;187), impelementasi itu mencakup proses bergerak menuju tujuan kebijakan dengan cara langkah administrative. Keberhasilan atau kegagalan impelementasi sebagai demikian dapat dievalusi dari sudut kemampuannya secara nyata dalam meneruskan atau mengoperasionalkan program-program yang telah dirancang sebelumnya.

Menurut Setiawan (2010:78) implementasi merupakan penerapan aplikasi dari hasil perancangan sistem yang ada untuk mencapai suatu tujuan yang didinginkan. Implementasi melaksanakan perintah-perintah yang secara terstruktur dari awal sampai akhir

Pengertian Komputer

Menurut Trisanjaya (2008:2) Keamanan komputer adalah bagian dari ilmu komputer yang bertugas untuk mengontrol resiko yang berhubungan dengan penggunaan komputer. Computer Security yang dimaksud adalah keamanan sebuah komputer yang terhubung ke dalam sebuah jaringan (Internet), dari akses yang tidak memiliki hak untuk mencoba masuk untuk memperoleh informasi dan service tertentu yang ada di dalam sistem.Usaha untuk mengakses paksa ini terdapat banyak macamnya, baik itu

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

intrusion (serangan dari luar organisasi) atau misuse (serangan dari dalam organisasi), dengan level hacker (hanya mencoba masuk ke dalam sistem komputer) atau bahkan cracker (mencoba masuk dan merusak untuk keuntungan pribadi).

Pengertian *Wireless*

Jaringan Wireless memiliki lebih banyak kelemahan dibandingkan dengan jaringan kabel (wired). Kelemahan jaringan wireless secara umum dapat konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karna saat ini untuk membangun sebuah jaringan wireless Cukup mudah (Pervaiz). Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor

Pengertian Snort

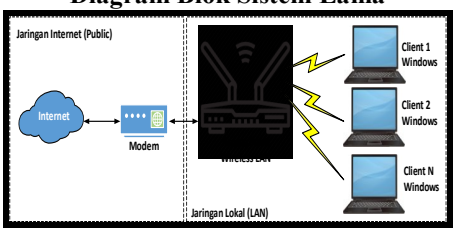
Menurut ariyus (2015:36) Snort merupakan suatu perangkat lunak untuk mendeteksi penyusup dan mempu menganalisis paket yang melintasi jaringan secara real time traffic dan logging kedalam database serta mampu mengidentifikasi berbagai serangan yang berasal dari luar jaringan. Program snort dapat dioprasikan dengan tiga mode, yaitu Paket Sniffer yang berfungsi untuk melihat paket yang lewat di jaringan, Paket Logger yang berfungsi untuk mencatat semua paket yang lewat di jaringan untuk dianalisis di kemudian hari dan NIDS (Network Intrusion Detection System), pada mode ini snort akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer

METODE PENELITIAN

Metode Pengumpulan Data

Menurut Azwar (2007: 110),Metode penelitian yang digunakan adalah metode eksprimen.

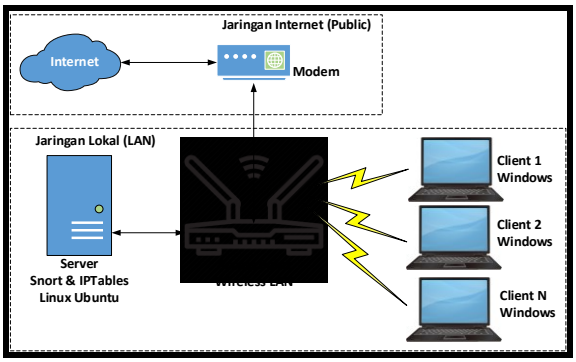
Diagram Blok Sistem Lama



Gambar 1 Blok Diagram Global Sistem Lama

Pada Gambar 1 Diagram Blok sistem lama diatas, client terkoneksi secara langsung ke access point yang menjadi sambungan wireless LAN tanpa adanya pengawasan dari pihak administrator dalam jaringan tersebut, sehingga apapun yang dilakukan oleh client yang terkoneksi di jaringan menggunakan wireless LAN didak dapat di batasi.

Blok Diagram Sistem Yang Diusulkan



Gambar 2 Blok Diagram Global Sistem Baru

Pada Gambar 2 diagram blok sistem baru, penulis mencoba menambahkan server yang akan digunakan untuk mengamati aktivitas dalam suatu jaringan komputer menggunakan software aplikasi SNORT, jika terdapat suatu aktivitas yang dianggap membahayakan yang dilakukan oleh client, seperti adanya serangan Distributed Denial of Service (DDos) yang membanjiri lalu lintas jaringan internet/intranet pada server, sistem, atau jaringan akan dilakukan filter (penyaringan) terhadap traffic lalu lintas Data menggunakan IPTables

Prinsip Kerja Sistem

Prinsip kerja sistem disini bertujuan untuk memfokuskan kerja sistem yang akan di gunakan dari rancangan blok diagram yang akan dibuat dan di implementasikan sesuai dengan rancangan blok diagram dengan pokok kerja sistem. Sistem pengujian yang akan di lakukanmelalui proses persiapan alat alat yang di butuhkan, koneksi terhadap jaringan Lokal, koneksi terhadap jaringan internet global, menginstall software yang diperlukan serta menerapkan metode-metode yang digunkan untuk melakukan manajemen jaringan. Sampai pada akhir mendapat kesimpulan tentang kinerja dari ClearOS dalam melakukan manajemen dan keamanan jaringan.

HASILDAN PEMBAHASAN

Pembahasan

Dari serangkaian implementasi hingga pengujian terhadap sistem keamanan jaringan dengan menggunakan OS Linux Ubuntu *Server* dan Snort didapatkan hasil berupa sistem berjalan dengan baik sesuai dengan keinginan baik itu koneksi jaringan LAN, *Internet*, keamanan dan lain sebagainya.

Dari identifikasi masalah ditemukan masalah bagaimana merancang dan mengimplementasikan sistem keamanan jaringan dengan menggunakan Sistem Operasi Linux *Server* dan Snort sehingga akan menghasilkan sebuah jaringan dengan tingkat keamanan, kenyamanan dan kelancaran yang lebih baik dari sebelumnya. Berikut tampilan hasil deteksi Snort, seperti dapat dilihat pada tampilan dibawah ini :

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

Gambar 3. Tampilan Hasil Deteksi Snort

Hasil diatas merupakan hasil deteksi snort terhadap serangan yang terjadi sesuai dengan script yang telah di konfigurasi pada file *.rules snort. Hasil deteksi snort adalah sebagai berikut :

1. Terhadap ancaman *DDoS Attact*

Hasil deteksi snort untuk ancaman berupa *DDoS Attack* dapat dilihat pada tampilan gambar dibawah ini :

a. Serang pasif

Snort dapat mendeteksi serangan aktif dengan baik dengan *report* pada *Base* berupa (Gambar 4.1 dan 4.2) :*Alert ICMP DOS Detect 138*

Alert (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas DOS melalui protokol ICMP yang berhasil di detetksi snort.

b. Serangan aktif

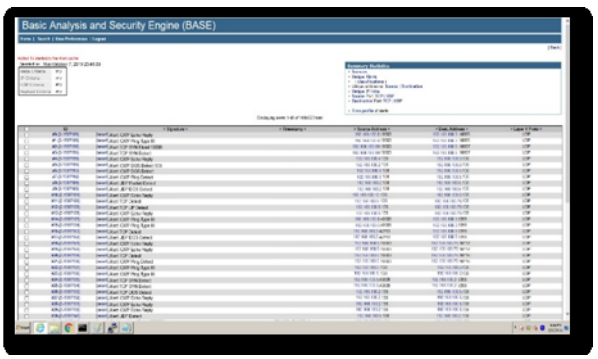
Snort dapat mendeteksi serangan Aktif dengan baik dengan *report* pada *Base* berupa (Gambar 4.1 dan 4.2) :*Alert ICMP Ping Detect*

Alert (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan kegiatan DOS dengan melakukan ping dengan menggunakan beban paket data.

c. Man in The Middle Attack

Snort dapat mendeteksi serangan Aktif dengan baik dengan *report* pada *Base* berupa (Gambar 4.1 dan 4.2) :*Alert ICMP DOS Detect*

Alert (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan kegiatan atau ancaman terhadap Protokol ICMP dengan menggunakan header paket data.



Gambar 4. Tampilan Report Log Ancaman DDoS

2. Terhadap ancaman *Ping Of Death*

Hasil deteksi snort untuk ancaman berupa *Ping of Death* dapat dilihat pada tampilan gambar dibawah ini :

a. Serang pasif

Snort dapat mendeteksi serangan aktif dengan baik dengan *report* pada *Base* berupa (Gambar 4.1 dan 4.3) :*Alert ICMP UDP DOS Detect*

Alert (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas atau ancaman pada jaringan melalui protokol UDP yang kalau di biarkan akan mengakibatkan server menjadi lambat karena menanggung beban kiriman paket data yang tidak berguna.

b. Serangan aktif

Snort dapat mendeteksi serangan Aktif dengan baik dengan *report* pada *Base* berupa (Gambar 4.1 dan 4.3) :*Alert ICMP Ping Detect Type II*

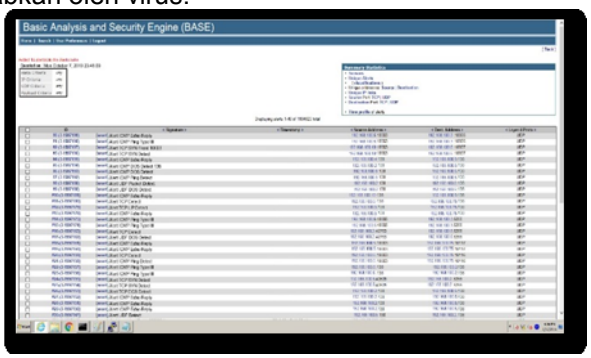
Alert (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan

kegiatan ping ping ke server atau pada jaringan dengan interval waktu yang cepat.

c. *Man in The Middle Attack*

Snort dapat mendeteksi serangan Aktif dengan baik dengan *report* pada *Base* berupa (Gambar 4.1 dan 4.3) :*Alert ICMP TCP UP Detect*

Alert (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan kegiatan atau ancaman terhadap *Protokol* TCP melalui kiriman *header* paket data biasanya ini disebabkan oleh virus.



Gambar 5. Tampilan *ReportLog* Ancaman *Ping Of Death*

Hasil Pengujian *SYN Flood*

Hasil deteksi snort untuk ancaman berupa *SYN Flood* dapat dilihat pada tampilan gambar dibawah ini :

a. Serang pasif

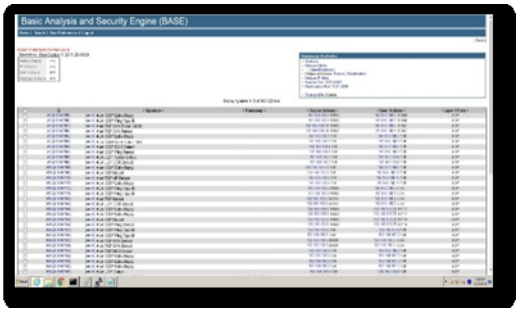
Snort dapat mendeteksi serangan Aktif dengan baik dengan *report* pada *Base* berupa *Alert TCP SYN Flood 10003 Alert* (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan kegiatan kiriman paket yang berulang-ulang melalui *port* 10003.

b. Serang pasif

Snort dapat mendeteksi serangan Pasif dengan baik dengan *report* pada *Base* berupa (Gambar 5 dan 6) :*Alert TCP SYN Flood Detect Alert* (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan kegiatan kiriman paket yang berulang-ulang.

c. *Man in The Middle Attack*

Snort dapat mendeteksi *Man in The Middle Attack* dengan baik dengan *report* pada *Base* berupa (Gambar 4 dan 5) :*Alert TCP SYN Flood Detect Alert* (pemberitahuan) diatas merupakan pemberitahuan adanya aktifitas melakukan kegiatan kiriman paket yang berulang-ulang.



Gambar 5. Tampilan Report Log Ancaman SYN Flood

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

Persiapan Alat Dan Bahan (*Hardware* dan *Software*)

a. Persiapan *Hardware*

Untuk melakukan analisa implementasi keamanan wireless LAN menggunakan snort dan iptbles ini yang perlu dipersiapkan antara lain :

1. Laptop untuk *Server*

Spesifikasi laptop Acer yang digunakan pada penelitian ini adalah *ProcessorIntel P6200*, *Memory* 1 GB, *Harddisk* 500 GB serta perlatan lainnya bawaan laptop.

2. Laptop untuk klien
3. Kabel LAN
4. RJ 45
5. Tang *Crimping*

b. Persiapan *Sofware*

Software-software yang digunakan dalam penelitian ini adalah :

1. Linux Ubuntu Server 16.04
2. Snort
3. IPTables
4. Web Browser (Google Chrome dan Mozilla)
5. Putty

Installasi Ubuntu Server

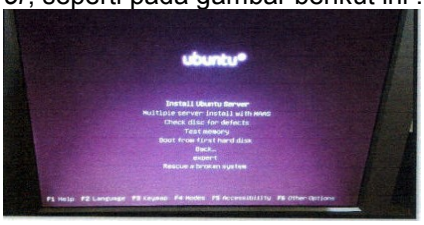
a. Pilihan Bahasa

Pada awal *booting* terdapat pilihan bahasa yang ingindigunakan, seperti pada gambar dibawah ini :

Gambar 6. Tampilan Pilihan Bahasa

b. Pilihan Model *Install*

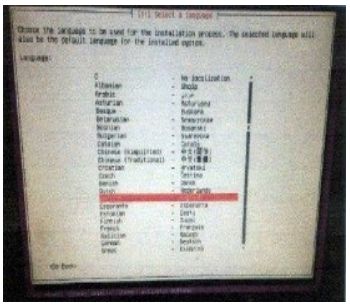
Setelah itu dilanjutkan ke pilihan model *Installasi* yang diinginkan, dalam hal ini penulis memilih *InstallUbuntuServer*, seperti pada gambar berikut ini :



Gambar 7. Tampilan Pilihan Model Install

c. Tampilan Pilihan Bahasa

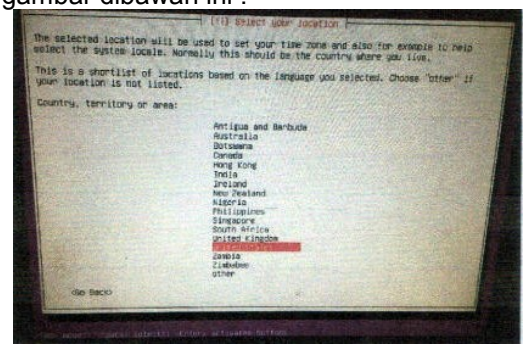
Tampilan pilihan bahasa yang ingin di install kedalam sistem ubuntu yang diinginkan, adapun tampilan dari halaman ini dapat dilihat pada tampilan dibawah ini :



Gambar 8. Tampilan Pilihan Bahasa

d. Pilihan Lokasi

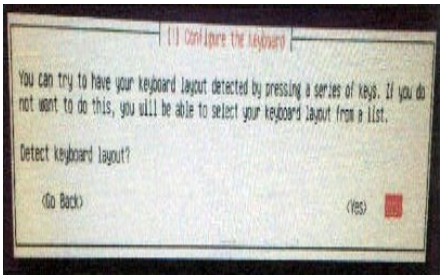
Pilihan ini berfungsi untuk pengaturan model lokasi kita. Tampilan dari pada halaman ini dapat dilihat pada gambar dibawah ini :



Gambar 9. Tampilan Pilihan Lokasi

e. Tampilan Konfigurasi *Keyboard*

Proses ini berfungsi untuk memillih atau mendeteksi *keybooard* yang digunakan daiam hal ini penulis memilih pilihan *default* yaitu dengan pilihan No. Tampilan halaman ini dapat dilihat pada gambar dibawah ini :

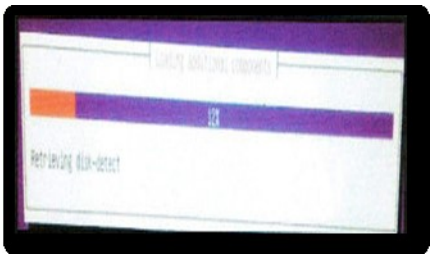


Gambar 10. Tampilan Pilihan Keyboard

f. Tampilan *LoadingAdditionalComponen*

Proses ini berfungsi melakukan deteksi semua komponen yang ada pada PC. Tampilan dari pada halaman ini dapat dilihat pada gambar dibawah ini :

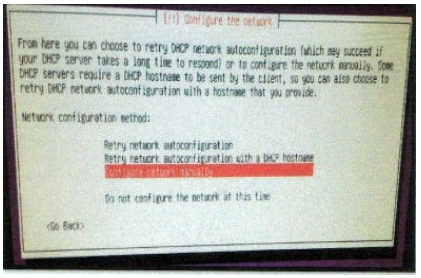
ISSN: XX32-XXX5 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa



Gambar 11. Tampilan *Loading Additional Component*

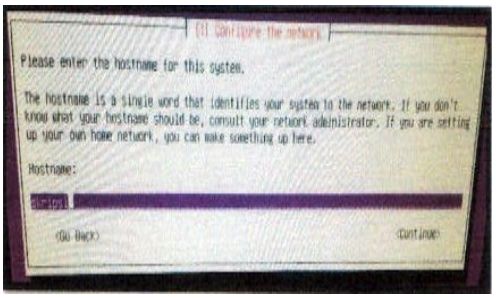
g. Tampilan Konfigurasi *Network*

Pada tahap ini kita akan mengatur konfigurasi *network*, disini penulis memilih pilihan pengaturan manual, yaitu dengan melakukan input IP *Address*, *Netmask* dan *Gateway* secara manual sesuai dengan yang ada pada jaringan. Tampilan dari pada halaman ini dapat dilihat pada gambar dibawah ini :



Gambar 12. Tampilan Halaman Cek HDD dan *Memory*

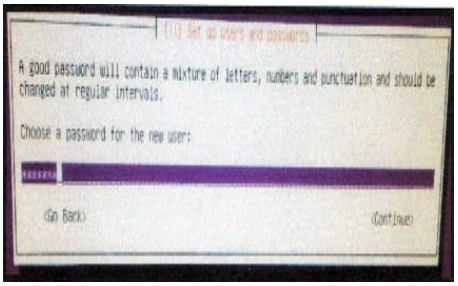
h. Input *Hostname*



Gambar 13. Tampilan *InputHostname*

i. Tampilan InputPassword

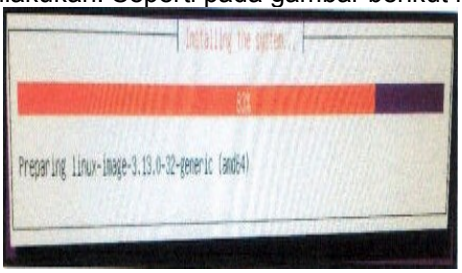
Pada proses *ini kita diminta untuk memasukan* password*,hendaknya* password *yang di gunakan yaitu* password *yang kita ingat karena akan digunakan untuk masuk kedalam system Linux* Server*. Tampilan proses installasi dapat dilihat pada gambar dibawah ini :*



Gambar 14. Tampilan *InputPassword*

j. Tampilan *InstallasiSystem*

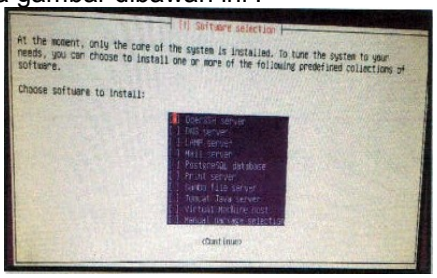
Proses installasi mulai dilakukan. Seperti pada gambar berikut ini :



Gambar 15. Tampilan *Installasi Paket System*

k. Tampilan Pilihan Paket Installasi

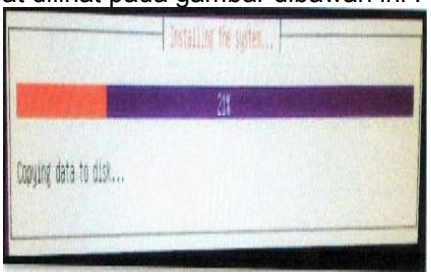
Proses ini merupakan pilihan paket aplikasi yang ingin di gunakan. Tampilan halaman *Booting* dapat dilihat pada gambar dibawah ini :



Gambar 16. Tampilan Pilihan Paket

l. Tampilan Proses Installasi Paket yang dipilih

Pada tahap ini system akan melakukan installasi paket-paket sistem yang dipilih. Tampilan halaman ini dapat dilihat pada gambar dibawah ini :



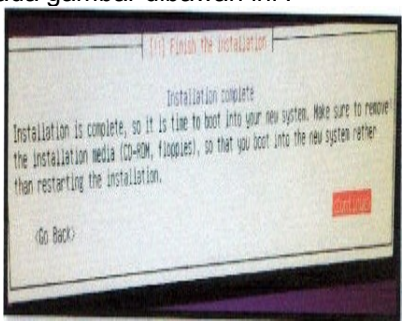
Gambar 17. Tampilan Installasi Paket Yang Dipilih

m. Tampilan Proses Installasi Selesai

Sampai tahap ini proses installasi Linux Ubuntu *Server* selesai dilakukan. Tampilan

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

halaman ini dapat dilihat pada gambar dibawah ini :



Gambar 18 Tampilan Installasi Paket Yang Dipilih

n. Tampilan Proses *Booting*

Setelah installasi selesai dilakukan maka sistem utama linux *server*akan melakukan *booting*. Tampilan halaman ini dapat dilihat pada gambar dibawah ini :

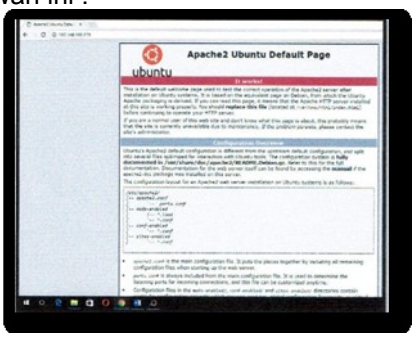
Gambar 19. Tampilan Proses Booting

Instailasi Paket-paket pendukung

Paket-paket aplikasi atau sistem yang dibutuhkan untuk Snort yaitu Apache, PHP5 dan MySql. Setelah semua paket selesai di install baru bisa kita melakukan instailasi Snort. Adapun tampilan paket selesai diinstall dapat dilihat pada gambar dibawah ini ;

a. Apache2

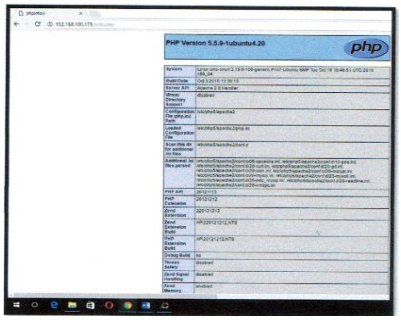
Paket apache2 selesai di install ditandai dengan bisa dilakukan *browsing* dari *explorer*yaitu dengan cara mengetikan alamat IP dari server linu. Adapun tampilannya seperti pada gambar dibawah ini :



Gambar 20 Tampilan Apache

b. PHP

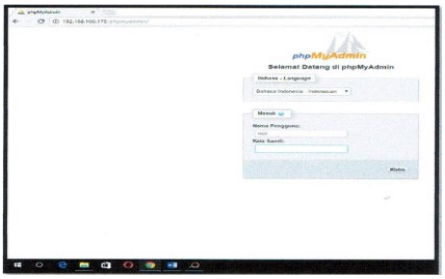
Paket PHP selesai di install ditandai dengan bisa dilakukan *browsing* dari *explorer* yaitu dengan cara mengetikan alamat IP dari *server* linux. Adapun tampilannya seperti pada gambar dibawah ini :



Gambar 21. Tampilan PHP

c. **MySql**

Paket MySql selesai di *install* ditandai dengan bisa dilakukan *browsing* dari *explorer* yaitu dengan cara mengetikan alamat IP dari server linu. Adapun tampilannya seperti pada gambar dibawah ini :



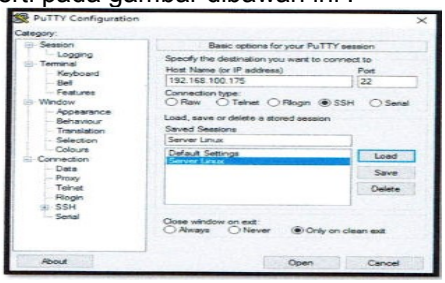
Gambar 22. Tampilan MySql

Installasi dan Konfigurasi Snort dan IPTables

Untuk melakukan installasi snort kita bisa melakukan dari komputer lain dengan menggunakan aplikasi-aplikasi *remote*, disini penulis menggunakan Putty. Adapun langkah-langkah install snort pada *server*yaitu :

a. *Login* ke *server*

Tahap ini yaitu melakukan login ke *Server* Linux Ubuntu dengan menggunakan Putty. Adapun tampilannya seperti pada gambar dibawah ini :

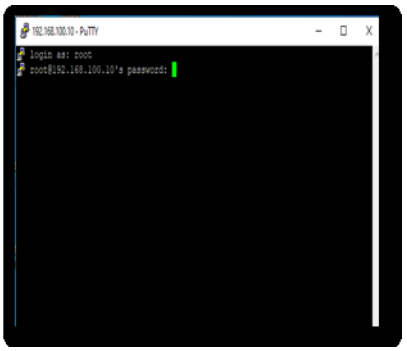


Gambar 23. Tampilan *Login* Putty

b. *InputUsername* dan *Password*

ISSN: XX32-XX45 GATOT KACA JOURNAL e-ISSN : XX67-XX89
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

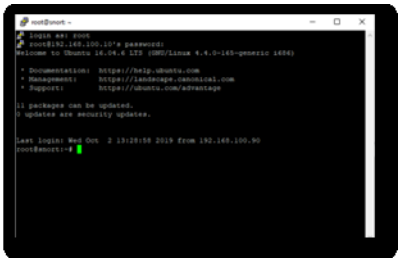
Selanjutnya melakukan *inputUsername* dan *Password*, silakan isikan *Username* dan *password* sesuai dengan yang di input waktu installasi. Adapun tampilannya seperti pada gambar dibawah ini :



Gambar 24. Tampilan *InputUsername* dan *Password*

c. Berhasil *Login*

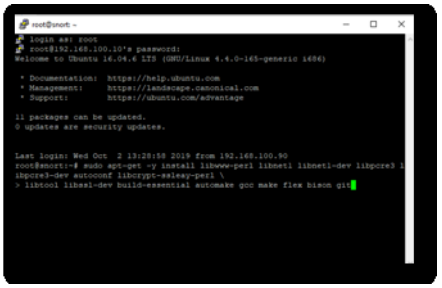
Setelah berhasil login kita masuk kedalam sistem linux. Adapun tampilannya seperti pada gambar dibawah ini :



Gambar 25. Tampilan Berhasil *Login* ke Server

d. Install Snort

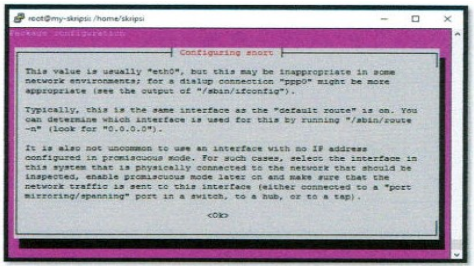
Untuk melakukan install snort pada server dapat dilakukan dengan perintah “apt-get install snort snortcommon snort-common-libraries snort-rules-default”, seperti tampilan dibawah ini :



Gambar 26. Tampilan Perintah Install *Library* Snort

e. Konfigurasi Snort

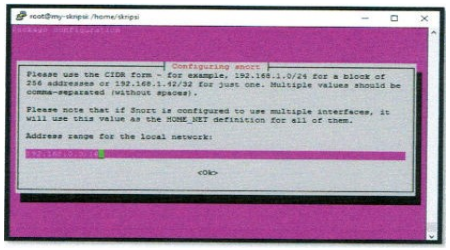
Tahap ini mulai melakukan konfigurasi snort, seperti tampilan dibawah ini :



Gambar 27. Tampilan Konfigurasi Snort

f. IP Yang Dilindungi

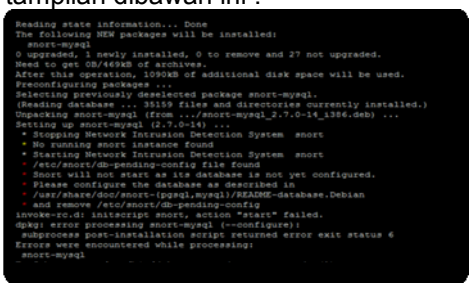
Tahap ini melakukan konfigurasi snort untuk pemilihan ip yang diingin dilindungi, seperti tampilan dibawah ini :



Gambar 28. Tampilan Konfigurasi IP Yang Dilindungi

i. Snort berhasil diinstall

Setelah semua , seperti tampilan dibawah ini :



Gambar 29. Tampilan Snort Berhasil Diinstall

KESIMPULAN DAN SARAN

A. Kesimpulan

Dari hasil penelitian maka dapat ditarik kesimpulan sebagai berikut:

1. Linux Ubuntu Server sangat baik digunakan untuk keperluan server, baik itu dari segi kemampuan, biaya dan konfigurasi-konfigurasinya.

2. Sistem Snort sangat sangat baik digunakan untuk keperluaan keamanan jaringan karena snort memiliki pilihan dan kemampuan untuk mengamankan jaringan dan yang lebih utama snort sangat ringan untuk digunakan.

3. Dalam melakukan keamanan jaringan Linux Ubuntu Server dan Snort dapat melakukan sesuai dengan keiinginan penguna

B. Saran

Setelah dilakukan pengujian terhadap Sistem Snort, maka penulis menyarankan.

1. Kedepannya Sistem ini sebaiknya digabungkan dengan firewalfirewall lainnya seperti Jupiter, Mikrotik dan sebagainya, untuk mendapatkan hasil yang lebih maksimal.
2. Dalam melakukan keamanan jaringan sebaiknya dilakukan sesuai dengan kebutuhan seperti jaringan mana yang ingin dilakukan pengamanan

DAFTAR PUSTAKA

Desmon Sharon, 2014, Membangun jaringan Wireless Local Area Network (WLAN) CV. BIQ BENGKULU Jurnal Media Infotama.

Ery setiyawan Jullev Atmaji. Bekti Maryuni Susanto. 2016. Monitoring Keamanan Jaringan Komputer Menggunakan Network Intrussion Detection System (NIDS.) Seminar penelitian tegnologi informasi.

Putu Agus Eka Pratama, 2014, Handbook Jaringan Komputer. Informatika Bandung.

Jarot Setyaji, 2010, Buku Pintar Menguasai Komputer Dan Laptop. Media Kita.Jakarta Selatan.

Jufriadif Na'am, 2012, Teknik Keamanan Jaringan Dan Data Dengan Linux Demilitarized Zone U. Jurnal Processor, (2) 7 hal

Kristoko Dwi Hartomo, 2007, Analisis Perancangan perangkat Lunak Instrusion Detection Sistem (IDS) pada jaringan komputer berbasis teknologi Mobile. Jurnal sistem dan informatika.

Muhammad Satria Nugraha. 2010, Implementasi instrusion detection sistem untuk Filtering paket data.skripsi yayasan pembinaan pendidikan Nusantara.

Rian adi Wibowo. Melwin Syafrizal, 2014. Analisis dan implementasi IDS menggunakan Snort pada Cloud Server di jogja digital valley. Jurnal Teknik Informatika.

Slamet, 2014, Intrusion Preventing Sistem pada jaringan Wireless STIKOM Surabaya menggunakan SNORT dan IPTables. Jurnal Teknik Infortamika.

Tri Wahyu W, Aidil Sanjaya. 2008 Studi Sistem Keamanan Komputer.Jurnal Artifical.

Tuxkeren, 2013, Ubuntu Server Panduan Singkat dan Cepat Jasakom batam

GATOT KACA
JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa