PENDETEKSIAN DAN PENCEGAHAN SERANGAN PADA JARINGAN MENGGUNAKAN SNORT PADA LINUX UBUNTU

Diajukan kepada Program D.III Manajemen Informatika

Untuk Memenuhi Salah Satu Syarat Guna Mencapai Gelar Ahli Madya dalam Bidang Ilmu Manajemen Informatika

OLEH:

RAFLI RAZAK

14 205 087

JURUSAN MANAJEMEN INFORMATIKA
FAKULTAS EKONOMI DAN BISNIS ISLAM
INSTITUT AGAMA ISLAM NEGERI BATUSANGKAR

2018

Saya yang bertanda tangan dibawah ini:

Nama	: RAFLI RAZAK
NIM	: 14 205 087
Tempat, Tanggal Lahir	: Bangko, 21 Juni 1996
Fakultas	: Ekonomi Dan Bisnis Islam
Jurusan	: Manajemen Informatika

Menyatakan dengan sesungguhnya bahwa Tugas Akhir saya yang berjudul: **"PENDETEKSIAN DAN PENCEGAHAN SERANGAN PADA JARINGAN MENGGUNAKAN SNORT PADA LINUX UBUNTU"** adalah **benar karya saya sendiri bukan plagiat** kecuali yang tercantum sumbernya.

Apabila dikemudian hari terbukti bahwa karya ilmiah ini plagiat, maka saya bersedia menerima sanksi sesuai dengan ketentuan perundang-undangan yang berlaku. Demikian surat pernyataan ini saya buat dengan sebenarnya untuk digunakan sebagaimana mestinya.

Batusangkar, Februari 2018

Saya yang Menyatakan

RAFLI RAZAK

NIM. 14 205 087

PERSETUJUAN PEMBIMBING

Pembimbing Penulisan Tugas Akhir atas Nama : Rafli Razak, NIM : **14 205 087** dengan Judul : **"PENDETEKSIAN DAN PENCEGAHAN SERANGAN PADA JARINGAN MENGGUNAKAN SNORT PADA LINUX UBUNTU"** memandang bahwa Tugas Akhir yang bersangkutan telah memenuhi persyaratan Ilmiah dan dapat disetujui untuk dilanjutkan ke Sidang Munaqasyah.

Demikianlah persetujuan ini diberikan untuk dapat dipergunakan sebagaimana mestinya.

Batusangkar, Februari 2018

Ketua Jurusan
Manajemen Informatika

Iswandi, M.Kom
NIP. 19700510 200312 1 004

Pembimbing

Zikrawahyu, M.Kom
NIP. 19740507 20051 1 006

Mengetahui,
Dekan Fakultas Ekonomi dan Bisnis Islam
IAIN Batusangkar

Dr. Ulya Afsani, S.H., M.Hum
NIP. 19750303 199903 1 004

PENGESAHAN TIM PENGUJI

Tugas Akhir yang berjudul **"ANALISA PENDETEKSIAN DAN PENCEGAHAN SERANGAN PADA JARINGAN BERBASIS SNORT PADA LINUX UBUNTU "** oleh **RAFLI RAZAK,** NIM. **14 205 087,** telah diajukan pada sidang munaqasyah Institut Agama Islam Negeri (IAIN) Batusangkar, Senen 19 Februari 2018 dan dinyatakan telah diterima sebagai salah satu syarat untuk mencapai gelar Ahli Madya Program Diploma III (D.III) Manajemen Informatika.

No.	Nama Penguji	Jabatan	Tanda Tangan	Tanggal
1.	Zikrawahyu, M.Kom NIP. 19740507 200501 1 006	Ketua Sidang		23/2-18
2.	Iswandi, M.Kom NIP. 19700510 200312 1 004	Anggota		22/2-18
3.	Lita Sari Muchlis, M.Kom NIP. 19780122 200801 2 017	Anggota		21/02-2018

Mengetahui,

Dekan Fakultas Ekonomi dan Bisnis Islam

IAIN Batusangkar

Dr. Ilya Atsani, S.H., M.Hum

Nip. 19750303 199903 1 004

Allah tidak akan membebani seseorang melainkan dengan kesanggupannya"

(Al-Baqarah: 286)

Setapak langkah ku ayun dengan tertatih-tatih "asa" di pundak mesti ku raih perjuangan yang melelahkan. Terkadang aku harus mengeluh, merintih dan menangis. Tetapi bendera telah ku kembangkan. Berpantang mundur kebelakang. Akupun menjejaki tingginya pendakian "asa" telah membasahi jiwaku yang dahaga. Tertunduk ribuan cita-cita yang menertawaiku, yang harus ku kibarkan demi kebahagian orang tuaku.

YA ALLAH.....

Tidak ada sesuatu yang mudah kecuali memang engkau yang memudahkannya dan engkau yang menjadikan segala sesuatu yang sulit itu menjadi mudah jika memang engkau berkehendak.

ALHAMDULILLAH YA ALLAH.....

Hari ini atas izin Mu dan rahmat Mu, tak ada yang bisa ku ucap, selain rasa syukur yang teramat dalam, betapa besar kasih sayang Mu menyertaiku. Ku berdoa, bersimpuh dan mengadahkan tangan pada Mu ya Allah. Aku tidak ingin kebahagiaan ini hanya jadi milikku, tapi juga dirasakan bagi orang-orang yang ku sayangi dan menyayangiku. Terimakasih Ya Allah.

Seiring rasa syukurku kepada Mu.

Aku persembahkan karya kecil ini sebagai tanda bakti dan hormatku yang tiada tara.

KEPADA KEDUA ORANG TUA KU.

Ibunda Hermailis dan ayahanda Hermanto

Terima kasih banyak, berkat semua dorongan dan jerih payah ibu dan ayah selama ini. Dukungan, motivasi dan nasehat yang selalu kalian berikan.

Tetes keringatmu yang membasahi demi masa depan kami.

Ibuku tercinta, "Hermailis"

Ibu,… berkat doamu, tetes air mata dan pengorbananmu , ibu telah banyak berkorban buatku demi meraih cita-cita ini. Akhirnya sebongkah cita-cita kita raih juga, terwujud keinginan untuk melihat anakmu jadi sarjana bu….

Aku menyadari apa yang ku perbuat sampai hari ini belum bisa membalas walau setetes dari keringat orang tuaku dan keluargaku…

Ya Allah limpahkanlah segala kemuliaan kepadaku dan keluargaku serta tuntunlah setiap langkahku hingga akhir pencapaian cita-citaku….

Ayah…Ibu…semoga ini menjadi awal dalam pencapaian hari esok yang lebih baik. Bagiku tidak ada yang lebih baik selain membuatmu bahagia, dimana perjalanan masih panjang dan perjuanganku belum selesai.

Semoga dengan rahmat dan ridho Mu mengiringi setiap langkahku untuk masa yang akan datang….

Terima kasih juga aku ucapkan kepada My Brother & My Sister

(Robby Akbar Prasetyo,Rahmat Fahrozi,Annisa Maharani)

Terima kasih untuk doanya, pengorbananya sehingga abang bisa meraih gelar sarjana ini.

Keluarga Besar ku…

Selalu memberikan semangat dan dukungan untukku, terima kasih untuk kasih sayang kalian yang tiada tara untuk slalu mendidik dan menyayangi ku.

Buat semua teman-teman pada jurusan Manajemen Informatika yang tidak mungkin disebutkan satu persatu. khususnya teman-temanku :

"Muslimin" Gak terasa udah 3 Tahun setengah aja kita dirantau orang ya bro. biasanya kita selalu gaje-gajean, masak berdua di kost. Sekarang aku harus duluan pergi dari Batusangkar. Wah nampaknya awet terus nih sama Hayatun Nisa. Hehe ditunggu undangannya bro.

"M. RIdho" yang terobsesi jadi polisi dari kecil. Semangat dhok mengejar cita2nya.

"M. Alda Yoga P" hahaha kawanku yang paling gendut dan suka makan. Namun berpikir kreatif namun selalu tertawa meskipun ada masalah.

"Heri Candra " yang selalu menemaniku dan membantuku,yang selalu memberi support terhadap ku jika aku dalam keadaan terpuruk dalam frustasi dan banyak hal lainnya,sankyu ri,akhirnya kita bisa wisuda bareng juga ri ☺.

"Lamboyni Alias Boy" teman kost tapi selalu mendengarkan dan melantunkan ayat2 suci Al-Qur'an setiap paginya. Semangat boy meskipun belum menemukan judul untuk skripsinya.

"Helmi Antoni" teman yang bersuara merdu yang selalu enak untuk didengar dan terobsesi jadi penyanyi. Semoga cita2mu dapat tercapai my.

"Putri Wiyana" teman seperjuangan,terimakasih banyak atas bantuannya selama ini dari tugas kuliah bahkan dalam banyak hal lainnya, semangat ya pw biar bisa nyusul kami wisuda nantinya ☺.

"Melly Marlina" biasa dipanggil cebol ☺,jangan main game mulu bol,kerjain tuh Tugas Akhirnya biar bisa wisuda nanti.

"Richi Oktariandi" teman dekat ku,orangnya yang nyantai aja, hokinya tinggi ☺semangat ya mas bro semoga sukses.

"Ikhsan Oktavio & Julius Roliat Sihotang" biasa dipanggil gaek ☺ terimakasih banyak gaek atas supportnya selama ini, terimakasih banyak atas bantuannya gaek, semoga panjang umur mu gaek dan julius jangan main game mulu jul ☺.

"Ramadhan Saputra" terimaksih bang don udah bantuin banyak hal selama perkuliahan ☺ dan akhirnya bisa wisuda bareng ☺.

"Marya Giptia" terimakasih marya yang juga selalu membantu ku dalam perkuliahan,bahkan sampe akhir sidang pun dan bisa wisuda bareng.

"Eka Dwi Sari Ningsih,Desi,Devi" kalian apakabar,maaf jika aku jarang mengabari kalian,oh ya semangat ya yang mau ngajukan judul,semoga cepat wisuda ya ☺,jangan main game mulu eka ☺ jangan galau mulu desi ☺,semangat devi buat kuliahnya dan jangan sering bawa hewan sebagai praktikumnya ke kost,kasian desi takut dianya☺.

Jika memang membaca itu adalah hal yang paling membosankan dalam belajar, maka carilah tutor yang bisa mengajarkan banyak hal secara langsung.

Good Luck All…

Wassalam

By : Rafli Razak, A.Md

ABSTRAK

Judul Tugas Akhir	**:**	**Pendeteksian Dan Pencegahan Serangan Pada Jaringan Menggunakan Snort Pada Linux Ubuntu**
Nama Mahasiswa	**:**	**Rafli Razak**
Nomor Induk Mahasiswa	**:**	**14 205 087**
Jurusan	**:**	**Manajemen Informatika**
Fakultas	**:**	**Ekonomi Dan Bisnis Islam**
Dosen Pembimbing	**:**	**Zikrawahyu, M.Kom**

Penelitian ini dilakukan bertujuan untuk mempermudah admin dalam memonitoring jaringan. Penulis menemukan adanya beberapa masalah dalam memonitoring jaringan yaitu banyaknya para user yang mencoba meretas kedalam server untuk mencuri database atau merusak sistem kinerja suatu server jaringan. Dengan menggunakan OS linux diharapkan dapat membantu kinerja snort dalam memonitoring jaringan. Perangkat lunak yang digunakan dalam sistem adalah snort yang berfungsi untuk memproteksi jaringan dan linux sebagai OS untuk menjalankan snort. Dengan memanfaatkan sistem proteksi yang terdapat pada snort diharapkan dapat membantu memproteksi adanya gangguan serangan terhadap jaringan.

Kata kunci :*Snort, Linux Ubuntu, DDoS, Pingflood, Portscanning*

KATA PENGANTAR

Puji dan syukur Penulis ucapkan kehadirat Allah SWT yang selalu melipahkan kesehatan dan kesempatan kepada Penulis sehingga pembuatan Tugas Akhir ini dapat terselesaikan. Shalawat dan Salam Penulis sampaikan kepada Nabi Muhammad SAW yang telah membawa Umat Islam yang penuh dengan Ilmu Pengetahuan bagi seluruh Umat Manusia untuk kemaslahatan hidup di Dunia dan Akhirat.

Maksud dan Tujuan pembuatan Tugas Akhir ini adalah untuk memberikan sumbangan pemikiran kepada Almamater serta untuk memenuhi sebagian persyaratan untuk mencapai gelar Diploma III Jurusan Manajemen Informatika Institut Agama Islam Negeri (IAIN) Batusangkar.

Dalam penulisan Tugas Akhir ini penulis banyak mendapat bimbingan dan bantuan baik Moril maupun Materil dari berbagai pihak. Oleh karena itu pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Dr. H. Kasmuri, M.A selaku Rektor IAIN Batusangkar.
2. Bapak Dr. Ulya Atsani, S.H., M.Hum. selaku Dekan Ekonomi dan Bisnis Islam Institut Agama Islam Negeri (IAIN) Batusangkar.
3. Bapak Iswandi, M.Kom selaku ketua Jurusan Manajemen Informatika IAIN Batusangkar yang telah memberikan bimbingan kepada penulis dalam pembuatan Tugas Akhir ini.
4. Bapak Zikrawahyu, M.Kom selaku Dosen Pembimbing yang telah memberikan banyak arahan dan nasehat kepada penulis dalam penyelesaian Tugas Akhir ini.
5. Bapak Gampito, S.E., M.Si selaku Dosen Pembimbing Akademik yang telah bersedia membimbing akademik selama 3 tahun serta telah memberikan semangat dan motivasi.
6. Orang Tua dan Keluarga yang telah memberikan bantuan baik moril maupun materil untuk penyelesaian Tugas Akhir ini.

7. Serta seluruh rekan-rekan MI angkatan ’14 yang selalu membangun kebersamaan dan saran dalam menyelesaikan Tugas Akhir tahun ini.
8. Juga kepada Pihak-pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan Motivasi dan semangat serta sumbangan pemikirannya kepada penulis sehingga selesainya Tugas Akhir ini.

Penulis sadar bahwasanya Tugas Akhir ini jauh dari kesempurnaan, oleh karena itu kritikan dan saran yang sifatnya membangun sangat penulis harapkan untuk kesempurnaan Tugas Akhir ini. Penulis juga berharap semoga penulisan Tugas Akhir ini memberikan manfaat kepada kita semua. Amin…

Akhirnya kepada Allah SWT jualah penulis bermohon dan bersujud semoga keikhlasan yang diberikan akan dibalas-Nya. ***Amin Ya Robbal'alamin***.

Batusangkar, Februari 2018

Penulis

DAFTAR ISI

ABSTRAK ..... **i**
KATA PENGANTAR ..... **ii**
DAFTAR ISI ..... **iv**
DAFTAR GAMBAR ..... **vi**
BAB I PENDAHULUAN **1**
A. Latar Belakang Masalah 1
B. Identifikasi Masalah 3
C. Rumusan Masalah 3
D. Batasan Masalah 3
E. Tujuan Penelitian 4
F. Manfaat Penelitian 4
G. Metode Penelitian 4
H. Sistematika Penulisan 5
BAB II LANDASAN TEORI **6**
A. Jaringan Komputer 6
1. Pengertian Jaringan Komputer 6
2. Perangkat Keras Jaringan Komputer 7
3. Jenis Jaringan Komputer 12
4. Topologi Jaringan Komputer 13
B. Konsep Dasar IP Address Dan Subnething 17
1. Konsep Dasar IP Address 17
2. Pengertian Subnetting 19
3. Pengertian Subnet Mask 20
C. Keamanan Jaringan 20
1. Kebijakan Keamanan 22
2. Mengenali ancaman terhadap network security 23
3. Serangan Pada Jaringan Komputer 23
D. Pengenalan Linux 30

1. Sejarah Linux 30
2. Pengertian Linux 31
3. Kelebihan dan Kekurangan Linux 31
4. Macam-Macam Distro Linux 33
E. PENGENALAN LINUX UBUNTU 35
1. Pengertian Linux Ubuntu 35
2. Sejarah Linux Ubuntu 36
3. Perbedaan Linux *Ubuntu* dan *Windows* 37
4. Kelebihan Linux Ubuntu 38
5. Kelemahan Linux Ubuntu 39
6. Fitur – fitur Linux Ubuntu. 39
7. Penginstalan Linux Ubuntu 40
F. *SNORT Intrusion Detection System* (IDS) 44
1. Komponen Snort 44
2. Supported Platforms 46
3. Mode Kerja 47
BAB III ANALISA DAN PERANCANGAN SISTEM 49
A. Analisa dan Kebutuhan Sistem 49
B. Perancangan Sistem Keamanan Jaringan 50
C. Penginstallan Aplikasi 52
D. Pengujian Dan Hasil 58
BAB IV PENUTUP 62
A. Kesimpulan 62
B. Saran 62
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR GAMBAR

Gambar 2. 1 *topologi bus* 14
Gambar 2. 2 *Topologi Ring* 15
Gambar 2. 3 *Topologi Star* 16
Gambar 2. 4 *Pemilihan Bahasa* 40
Gambar 2. 5 *Penginstalan Paket Ubuntu* 41
Gambar 2. 6 *Menghapus Disk dan Install Ubuntu* 41
Gambar 2. 7 *Konfirmasi Instalan* 42
Gambar 2. 8 *Pemilihan Lokasi Waktu* 42
Gambar 2. 9 *Pemilihan mode keyboard* 43
Gambar 2. 10 *User* 43
Gambar 3. 1 *Skema Simulasi Jaringan* 51
Gambar 3. 2 *Versi snort* 54
Gambar 3. 3 *Penginstalan Bernyard* 56
Gambar 3. 4 *IP Scan* 59
Gambar 3. 5 *perbobaan Ping* 59
Gambar 3. 6 *serangan DDoS* 60
Gambar 3. 7 *Snort Alert* 60
Gambar 3. 8 *Jumlah Baris ditable serangan* 61
Gambar 3. 9 *Table statistic penyerang* 61

DAFTAR TABEL

Tabel 3. 1 *IP Address* 52

BAB I
PENDAHULUAN

A. Latar Belakang Masalah

Seiring berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya yang mempermudah pekerjaan-pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Manusia sudah sangat tergantung dengan sistem informasi, akan tetapi statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang. Sistem pelaporan pertahanan terhadap aktivitas gangguan yang ada saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator.

Seorang Adiministrator jaringan bertanggung jawab penuh atas segala sesuatu ketersedian dan kerahasiaan informasi. Tidak hanya itu, pemeliharaan perangkat keras maupun perangkat lunak, analisis masalah, pemantauan kinerja jaringan. Sehingga dibutuhkan sebuah sistem *security* yang bisa membantu kerja sang administrator.

Menurut Monika Kusumawati (2010) "Snort merupakan bagian dari IDS dan merupakan sebuah perangkat lunak *open source"*. Snort merupakan sebuah aplikasi yang sangat bermanfaat bagi keamanan suatu jaringan yang memberi laporan secara detail, dan *up to date* sehingga segala kegiatan penyerangan dapat dideteksi/ diketahui secara dini, kelemahan sistem ini adalah pada bagian pengoperasian cukup rumit, butuh kejelian dan kecepatan pembacaan packet.

Ubuntu adalah salah satu distribusi Linux yang berbasiskan Debian dan didistribusikan menjadi perangkat lunak sistem operasi yang bebas. Secara singkat dan jelasnya yaitu Ubuntu adalah sejenis sistem operasi yang berbasiskan Linux Debian. Ubuntu ditujukan untuk penggunaan secara pribadi, namun ubuntu juga disediakan dalam bentuk sistem operasi ubuntu server.

Sudah ada beberapa penelitian karya ilmiah yang membahas tentang keamanan jaringan diantaranya :

Denny Wijanarko (2015) melakukan uji coba penerapan Snort sebagai sistem keamanan Jaringan Komputer, penelitian tersebut membuat sistem keamanan dengan menggunakan Snort dan menghubungkannya dengan Sms *Gateway*. Pada penelitian sistem yang dibuat bertujuan untuk memberikan *notifikasi* peringatan kepada *admin* apabila terjadi pencatatan sebuah *event alert*, sehingga *admin* dapat melakukan tindakan berdasarkan jenis *alert* yang teridentifikasi oleh program snort. Zilza Triani (2017) melakukan penelitian tentang Keamanan Jaringan Berbasis *Intrusion Detection System (Ids)* Dan *Intrusion Prevention System (Ips)* Menggunakan *Suricata*. Sistem ini dapat mendeteksi sebuah serangan intruksi yang dilakukan penyusup. pencegahan dilakukan dengan *drop* pada paket-paket yang dianggap tindak penyusupan. Mohammad Affandi (2012) melakukan penelitian tentang keamanan jaringan dengan judul Implementasi Snort sebagai alat pendeteksi intrusi menggunakan linux, disini peneliti melakukan pendeteksian menggunakan snort yang hanya sebagai mentedeksi adanya serangan. Miftahul Jannah (2012) melakukan penelitian tentang keamanan jaringan berbasis snort pada laboratorium jaringan komputer, disini peneliti menggunakan snort sebagai intrusion system atau sebagai pendeteksi serangan tetapi peneliti juga menambahkan Acibase sebagai pendukung snort, dimana acidbase sendiri berfungsi sebagai membuat table database yang akan digunakan oleh acid.

Pada tugas akhir ini peneliti mencoba melakukan sebuah penelitian dengan membuat sistem keamanan dan menganalisa sistem keamanan menggunakan Snort pada Linux Ubuntu. Hal ini lah yang melatarbelakangi penulis untuk menganalisa dan mengimplementasikan suatu sistem deteksi serangan pada jaringan yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan seperti *DDoS, Sniffing, Port Scanning* dan melaporkan pelaporan dengan notifikasi menggunakan Snort pada linux ubuntu sebagai firewall.

Oleh karena itu, sesuai dengan permasalah yang telah dikemukakan, maka penulis mencoba membahas suatu masalah dengan judul **"Analisa Pendeteksian Dan Pencegahan Serangan pada Jaringan Berbasis Snort pada Linux Ubuntu".**

B. Identifikasi Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan di atas, maka penulis dapat mengidentifikasikan masalah yang akan dijadikan sebagai acuan dalam pendeteksian serangan pada jaringan, sebagai berikut:

1. Sulitnya mengetahui penyusupan dan serangan yang sering terjadi di dalam jaringan internet.
2. Seringnya terjadi serangan pada jaringan seperti pingflood, port scanning, dan DDoS.

C. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan di atas, maka dapat dibuat perumusan masalah yaitu "sistem yang bagaimana yang bisa mengamankan jaringan dari serangan terhadap jaringan".

D. Batasan Masalah

Agar penelitian lebih terarah dan tidak menyimpang dari pokok permasalahan dan tujuan yang hendak dicapai, maka penulis membatasi ruang lingkup :

1. Jaringan yang diuji berupa *Local Area Network* (LAN).
2. Sistem operasi yang digunakan adalah *Linux Ubuntu 16.0.4*.
3. Terdapat 3 *host* yang terdiri dari 1 *server*,1 penyerang,dan 1 sebagai firewall.
4. Serangan yang akan digunakan dalam pengujian berupa *pingflood* dan *DDoS.*

E. Tujuan Penelitian

Sesuai permasalahan yang dihadapi, tujuan penelitian adalah :

1. Mengetahui penyusupan dan serangan yang sering terjadi di dalam jaringan internet.
2. Mengatasi serangan pada jaringan seperti *pingflood, dan DDoS*.
3. Untuk menghasilkan informasi serangan pada jaringan dan meningkatkan mutu pengawasan terhadap praktek kejahatan yang terjadi pada jaringan internet.
4. Untuk membantu admin dalam pengawasan pada sebuah jaringan sehingga tidak terjadinya hal-hal yang tidak diinginkan seperti pencurian data.

F. Manfaat Penelitian

Adapun manfaat penelitian ini dilakukan, yaitu:

1. Sebagai masukan bagi penulis sendiri untuk memperluas cakrawala berpikir setelah mendapatkan suatu perbandingan teori dengan aplikasinya.
2. Sebagai informasi untuk mengetahui penyusupan yang terjadi pada komputer atau laptop kita melalui jaringan internet.
3. Mencegah penyusup yang hendak menerobos masuk ke sistem komputer kita.

G. Metode Penelitian

Dalam penulisan ini penulis menggunakan beberapa metode penelitian antara lain :

1. Penelitian Pustaka (*Library Research*)

   Penelitian ini dilakukan untuk mencari data, mengumpulkan data dan mempelajari data dari buku-buku serta literatur-literatur yang berhubungan dengan permasalahan yang dibahas dalam penelitian.

2. Penelitian Labor (*Laboratory Research*)

   Dalam penelitian ini penulis melakukan pengolahan data dengan menggunakan alat bantu dalam pembuatan Tugas Akhir ini. Ditinjau dari penggunaan *hardware* dan *software* yang digunakan pada saat penulis melakukan proses penulisan tugas akhir ,sebagai berikut :

a. *Hardware*

Spesifikasi Perangkat Lunak yang digunakan terdiridari:

1) *3 unit Laptop*
2) *USB Lan Card*
3) *2 kabel LAN*

b. *Software*

1) *Snort*
2) *Linux Ubntu*

H. Sistematika Penulisan

Dalam penulisan ini penulis menggunakan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini menguraikan tentang latar belakang masalah, identifikasi masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, sistematika penulisan

Bab II Landasan Teori

Bab ini berisi teori yang di ambil dari buku-buku panduan dan referensi lain yang terkait dengan penelitian yang dilakukan oleh penulis.

Bab III Analisa dan Perancangan

Bab ini membahas analisa sistem pendeteksian serangan pada jaringan.

Bab IV Penutup

Bab ini berisi kesimpulan yang didapat selama pembuatan laporan tugas akhir serta saran-saran yang akan menjadi masukan bagi penulis serta bisa berguna bagi orang yang membaca

BAB II
LANDASAN TEORI

A. Jaringan Komputer

1. Pengertian Jaringan Komputer

Menurut Deny Purwanto (2015:1)"jaringan komputer adalah hubungan antar dua buah komputer atau lebih yang dapat berkomunikasi satu sama lain sehingga dapat saling berbagi data atau sumber dan dapat memindahkannya dengan mudah".

Menurut Muhammad Zunaidi (2013:107)mendefinisikan"jaringan komputer adalah kumpulan sistem-sistem yang terhubung dan saling berinteraksi menggunakan jalur komunikasi untuk berbagi sumber daya".

Adapun jalur yang digunakan dalam komunikasi jaringan dapat berbentuk media kabel (*Wired Network*), maupun non kabel (*Wireless Network*). Jaringan komputer yang dibentuk menggunakan media kabel, dapat memanfaatkan berbagai jenis kabel,diantara kabel yang sering digunakan dalam membentuk sebuah jaringan adalah kabel *coaxial*, kabel *UTP*, kabel *STP* dan kabel *Fiber Optic*.

Berdasarkan teori di atas dapat disimpulkan bahwa jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lainnya yang terhubung dalam satu kesatuan. Jaringan dan konektor yang digunakan adalah konektor tipe DIX. Panjang kabel *transceiver* maksimum 50 m, panjang kabel *Thick Ethernet* maksimum 500 m dengan maksimum 100 *transceiver* terhubungi. Informasi dan data bergerak melalui kabel-kabel atau tanpakabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan. Setiap komputer, printer atau periferal yang terhubung dengan jaringan disebut node.

Tujuan dari jaringan komputer adalah untuk melakukan komunikasi data, sharing data maupun pemakaian resource bersama seperti printer dan

media penyimpanan sekunder. Komunikasi data sendiri memiliki tujuan yang lebih khusus, yaitu:

a. Memungkinkan pengiriman data dalam jumlah besar efisien, ekonomis, dan tanpa kesalahan dari suatu tempat ke tempat yang lain.
b. Memungkinkan penggunaan sistem komputer dan peralatan pendukung dari jarak jauh (*remote*).
c. Memungkinkan penggunaan komputer secara terpusat maupun secara tersebar sehingga mendukung manajemen dalam hal kontrol, baik desentralisasi ataupun sentralisasi.
d. Mempermudah kemungkinan pengelolaan dan pengaturan data yang ada dalam berbagai macam sistem komputer.
e. Mengurangi waktu untuk pengelolaan data.
f. Mendapatkan data langsung dari sumbernya.
g. Mempercepat penyebarluasan informasi.
h. Komunikasi data berkaitan dengan pertukaran data diantara dua perangkat yang terhubung secara langsung yang memungkinkan adanya pertukaran data antar kedua pihak.

2. Perangkat Keras Jaringan Komputer

Prihanto (2003) Perangkat jaringan merupakan alat atau piranti yang digunakan untuk membangun suatu sistem jaringan. Masing-masing perangkat jaringan memiliki fungsi dan tujuan tersendiri didalam suatu sistem jaringan. Pemilihan perangkat-perangkat jaringan yang diperlukan dapat disesuaikan dengan kebutuhan sistem jaringan yang akan dibangun. Meskipun terdapat aneka ragam jenis jaringan komputer yang berbeda, tapi tetap memiliki perangkat keras yang umum seperti kabel atau perangkat *Wi-Fi, ethernet card,hub* atau *switch, repeater, bridege* dan lain-lain.

a. Router

Router sering digunakan untuk menghubungkan beberapa *network*. Baik network yang sama maupun yang berbeda dari segi teknologinya. Seperti menghubungkan network yang menggunakan topologi *Bus, Star, dan Ring*. Router juga digunakan untuk membagi network besar menjadi beberapa buah subnetwork (network-network kecil). Setiap subnetwork seolah-olah terisolir dari *network* lain.Hal ini dapat membagi-bagi traffic yang akan berdampak positif pada performa network. Sebuah router memiliki kemampuan routing.Artinya router secara langsung dapat mengetahui kemana rute perjalanan informasi (yang disebut packet) akan dilewatkan. Apakah ditujukan untuk host lain dalam satu network ataukah berbeda network. Jika paket-paket ditujukan untuk host pada network yang sama maka router akan menghalangi paket-paket keluar, sehingga paket-paket tersebut tidak membanjiri network yang lain.

Ada beberapa jenis router yaitu :

1) Mikrotik

Mikrotik adalahsebuah perusahaan yang bergerak di bidang produksi perangkat keras *(hardware)* dan perangkat lunak (*Software)* yang berhubungan dengan sistem jaringan komputer yang berkantor pusat di Latvia, bersebelahan dengan Rusia. Mikrotik didirikan pada tahun 1995 untuk mengembangkan router dan sistem *ISP (Internet Service Provider) nirkabel*. Mikrotik dibuat oleh MikroTikls sebuah perusahaan di kota Riga, Latvia. Latvia adalah sebuah negara yang merupakan pecahan dari negara Uni Soviet dulunya atau Rusia sekarang ini. Mikrotik awalnya ditujukan untuk perusahaan jasa layanan Internet (PJI) atau *Internet Service Provider (ISP)* yang melayani pelanggannya menggunakan teknologi nirkabel atau wireless. Saat ini *MikroTikls* memberikan layanan kepada banyak ISP nirkabel untuk layanan akses Internet dibanyak negara di dunia dan juga sangat populer di Indonesia. MikroTik sekarang menyediakan

hardware dan software untuk konektivitas internet di sebagian besar negara di seluruh dunia. Produk hardware unggulan Mikrotik berupa Router, *Switch*, Antena, dan perangkat pendukung lainnya. Sedangkan produk *Software* unggulan Mikrotik adalah MikroTik RouterOS.

2) RouterOS

RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer manjadi router *network* yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan *wireless*, cocok digunakan oleh ISP dan *provider hotspot.*

3) Routerboard

Router embedded produk dari mikrotik.Routerboard seperti sebuah pc mini yang terintegrasi karena dalam satu board tertanam *prosesor, ram, rom,* dan *memori flash. Routerboard* menggunakan *os RouterOS* yang berfungsi sebagai router jaringan, *bandwidth management, proxy server, dhcp, dns server* dan bisa juga berfungsi sebagai *hotspot server*. Mikrotik pada standar perangkat keras berbasiskan *Personal Computer* (PC) dikenal dengan kestabilan, kualitas kontrol dan *fleksibilitas* untuk berbagai jenis paket data dan penanganan proses rute atau lebih dikenal dengan istilah *routing*. Mikrotik yang dibuat sebagai router berbasiskan PC banyak bermanfaat untuk sebuah ISP yang ingin menjalankan beberapa aplikasi mulai dari hal yang paling ringan hingga tingkat lanjut. Contoh aplikasi yang dapat diterapkan dengan adanya Mikrotik selain routing adalah aplikasi kapasitas akses *(bandwidth) manajemen, firewall, wireless access point (WiFi), backhaul link*, sistem *hotspot*, *Virtual Private Netword (VPN)server* dan masih banyak lainnya.

b. Bridge

Bridge atau kadangkala disebut transparent bridge merupakan perangkat network yang digunakan untuk menghubungkan dua buah *LAN* atau membagi sebuah *LAN* menjadi dua buah segmen. Tujuannya adalah

untuk mengurangi *traffic* sedemikian rupa sehingga dapat meningkatkan performa *network*.

c. Repeater

Repeater termasuk satu dari perangkat keras jaringan komputer yang dipasang di titik-titik tertentu dalam jaringan untuk memperbaharui sinyal yang ditransmisikan agar mencapai kembali kekuatan dan bentuknya semula guna memperpanjang jarak tempuh. *Repeater* berfungsi untuk menguatkan sinyal.

1) Network Interface Card

Kartu Jaringan (*NIC*) merupakan salah satu dari perangkat keras yang menyediakan media untuk menghubungkan antar komputer. Kebanyakan kartu jaringan adalah kartu internal, yaitu kartu jaringan yang di pasang pada slot ekspansi di dalam komputer. Kartu jaringan yang banyak terpakai saat ini adalah: kartu jaringan *Ethernet*, *LocalTalk konektor*, dan kartu jaringan *Token Ring*.

d. Kabel

Setiap jenis kabel mempunyai kemampuan dan spesifikasinya yang berbeda, oleh karena itu dibuatlah pengenalan tipe kabel. Ada beberapa jenis kabel yang dikenal secara umum,*yaitu twisted pair (UTP / unshielded twisted pair*dan*STP/shieldedtwisted pair), coaxial cable* dan *fiber optic*. Berikut akan dijelaskan beberapa macam kabel yang serring digunakan dalam jaringan.

1) *Thin Ethernet (Thinnet)*

Thin Ethernet atau *Thinne*t memiliki keunggulan dalam hal biaya yang relatif lebih murah dibandingkan dengan tipe pengkabelan lain, serta pemasangan komponennya lebih mudah. Panjang kabel *thin coaxial*/RG-58 antara 0.5 – 185 m dan maksimum 30 komputer terhubung.

2) *Thick Ethernet (Thicknet)*

Dengan *thick Ethernet* atau *thicknet*, jumlah komputer yang dapat dihubungkan dalam jaringan akan lebih banyak dan jarak antara komputer dapat diperbesar, tetapi biaya pengadaan pengkabelan ini lebih mahal serta pemasangannya relatif lebih sulit dibandingkan dengan *Thinnet*. Pada *Thicknet* igunakan *transceiver* untuk menghubungkan setiap komputer dengan sistemaringan dan konektor yang digunakan adalah konektor tipe DIX. Panjang kabel *transceiver* maksimum 50 m, panjang kabel *Thick Ethernet* maksimum 500m dengan maksimum 100 *transceiver* terhubung.

3) *Twisted Pair Ethernet*

Kabel *Twisted Pair* ini terbagi menjadi dua jenis yaitu *shielded* dan *unshielded*. *Shielded* adalah jenis kabel yang memiliki selubung pembungkus (*Shielded Twisted Pair*) sedangkan *unshielded* tidak mempunyai selubung pembungkus (*Unshielded Twisted Pair*). Untuk koneksinya kabel jenis ini menggunakan konektor RJ-11 atau RJ-45. Pada *twisted pair network*, komputer disusun membentuk suatu pola *star*. Setiap PC memiliki satu kabel *twisted pair* yang tersentral pada HUB. *Twistedpair* umumnya lebih handal dibandingkan dengan *thin coax* karena HUB mempunyai kemampuan *data error correction* dan meningkatkan kecepatan transmisi Saat ini ada beberapa grade, atau kategori dari kabel *twisted pair.* Kategori 5 adalah yang paling reliable dan memiliki kompabilitas yang tinggi, dan yang paling disarankan. Berjalan baik pada 10Mbps dan *FastEthernet* (100Mbps). Kabel kategori 5 dapat dibuat *straight-through* atau *crossed*.

4) *Fiber Optic*

Jaringan yang menggunakan *Fiber Optic (FO)* biasanya perusahaan besar,dikarenakan harga dan proses pemasangannya lebih sulit. Namun demikian, jaringan yang menggunakan FO dari segi kehandalan dan kecepatan tidakdiragukan. Kecepatan pengiriman data dengan media FO lebih dari 100Mbps dan bebas pengaruh lingkungan.

3. Jenis Jaringan Komputer

Menurut Gilang (2010) Secara umum jaringan komputer dibagi atas lima jenis, yaitu:

a. Local Area Network (LAN)

Local Area Network (LAN), merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer) dan saling bertukarinformasi.

b. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN), pada dasarnya merupakan versi LAN yang berukuran lebih besar dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.

c. Wide Area Network (WAN)

Wide Area Network (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua.WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program(aplikasi) pemakai.

d. Internet

Sebenarnya terdapat banyak jaringan didunia ini, seringkali menggunakan perangkat keras dan perangkat lunak yang berbeda-beda. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kampatibel dan berbeda. Biasanya untuk melakukan hal ini diperlukan sebuah mesin yang disebut gateway guna melakukan hubungan dan melaksanakan terjemahan yang diperlukan, baik perangkat keras maupun perangkat lunaknya.Kumpulan jaringan yang terinterkoneksi inilah yang disebut dengan internet.

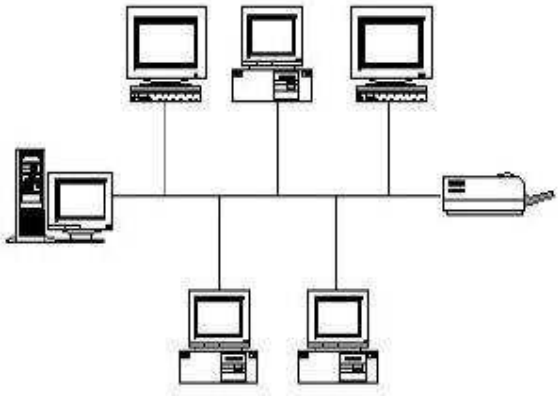
e. Jaringan Tanpa Kabel

Jaringan tanpa kabel merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Misalnya orang yang ingin mendapat informasi atau melakukan komunikasi walaupun sedang berada diatas mobil atau pesawat terbang, maka mutlak jaringan tanpa kabel diperlukan karena koneksi kabel tidaklah mungkin dibuat di dalam mobil atau pesawat. Saat ini jaringan tanpa kabel sudah marak digunakan dengan memanfaatkan jasa satelit dan mampu memberikan kecepatan akses yang lebih cepat dibandingkan dengan jaringan yang menggunakan kabel.

4. Topologi Jaringan Komputer

Menurut Fadel (2010) Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, *token-ring*,*star* dan *peer-to-peer network*. Masing-masing topologi ini mempunyai ciri khas, dengan kelebihan dan kekurangannya sendiri.

a. Topologi BUS



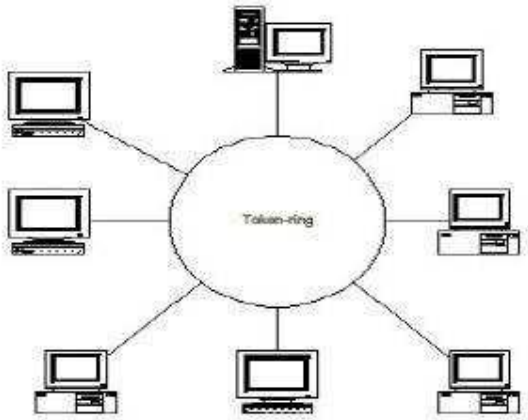
Gambar 2. 1 *topologi bus*

Topologi *bus* terlihat pada skema di atas. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1) Keuntungan
   a) Hemat kabel
   b) Layout kabel sederhana
   c) Mudah dikembangkan
   d) Jarak *LAN* tidak terbatas.
   e) Kecepatan pengiriman tinggi.
   f) Jumlah terminal dapat ditambah ataupun dikurangi tanpa menggangu operasi yang telah berjalan.
   g) Tidak diperlukan pengendalian pusat.
2) Kerugian
   a) Deteksi dan isolasi kesalahan sangat kecil
   b) Kepadatan lalu lintas
   c) Bila salah satu client rusak maka jaringan tidak dapat berfungsi
   d) Diperlukan repeater jarak jauh.
   e) Jika lalu lintas data terlalu banyak dan tinggi dapat terjadi kemacetan pada pengiriman data.
   f) Operasional jaringan *LAN* bergantung pada setiap terminal.

g) Jika terjadi gangguan atau kerusakan pada salah satu lokasi (titik) dalam jaringan maka akan mempengaruhi jaringan secara keseluruhan, bahkan ada kemungkinan jaringan akan terhenti sama sekali.

b. Topologi RING



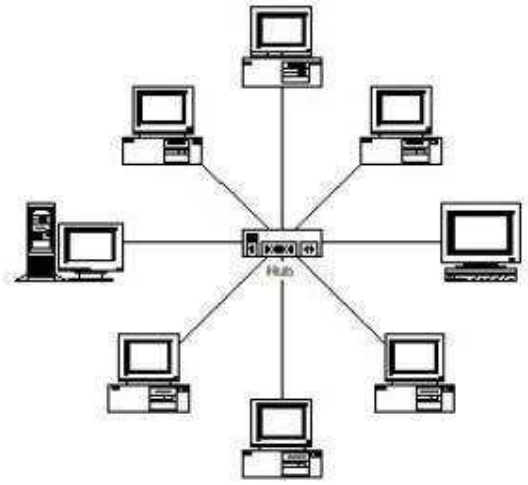
Gambar 2. 2 *Topologi Ring*

Topologi RING terlihat pada skema berikut ini.Metode *token-ring* (sering disebut ring saja) adalah cara menghubungkan komputer sehingga berbentuk ring (lingkaran). Setiap simpul mempunyai tingkatan yang sama. Jaringan akan disebut sebagai *loop*, data dikirimkan kesetiap simpul dan setiap informasi yang diterima simpul diperiksa alamatnya apakah data itu untuknya atau bukan.Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1) Keuntungan:
   a) Hemat kabel
   b) Laju data *(transfer rate)* tinggi.
   c) Dapat melayani lalu lintas data yang padat.
   d) Tidak diperlukan host,relatif lebih murah.
   e) Dapat melayani berbagai media pengiriman.
   f) Komunikasi antar terminal mudah.
   g) Waktu yang diperlukan untuk mengakses data optimal.

2) Kerugian:
   a) Peka pada masalah
   b) Pengembangan jaringan lebih kaku
   c) Penambahan atau pengurangan terminal sangat sulit.
   d) Kerusakan pada media pengiriman dapat menghentikan kerja seluruh jaringan.

c. Topologi STAR



Gambar 2. 3 *Topologi Star*

Merupakan kontrol terpusat, semua link harus melewati pusat yang menyalurkan data tersebut kesemua simpul atau client yang dipilihnya.Simpul pusat dinamakan stasium primer atau *server* dan lainnya dinamakan stasiun sekunder atau client server.Setelah hubungan jaringan dimulai oleh *server* maka setiap *client server* sewaktu-waktu dapat menggunakan hubungan jaringan tersebut tanpa menunggu perintah dari server. Terdapat keuntungan dan kerugian dari tipe ini yaitu:

1) Keuntungan:
   a) Paling fleksibel
   b) Pemasangan/perubahan stasiun sangat mudah dan tidak mengganggu bagian jaringan lain
   c) Kontrol terpusat
   d) Kemudahan deteksi dan isolasi kesalahan/kerusakan

e) Kemudahaan pengelolaan jaringan

2) Kerugian:

a) Boros kabel

b) Perlu penanganan khusus

c) Kontrol terpusat (HUB) jadi elemen kritis

d. Topologi peer – to – peer

Peer artinya rekan sekerja. *Peer-to-peer network* adalah jaringan komputer yang terdiri dari beberapa komputer (biasanya tidak lebih dari 10 komputer dengan 1-2 *printer*).Dalam sistem jaringan ini yang diutamakan adalah penggunaan program, data dan printer secara bersama-sama.

B. Konsep Dasar IP Address Dan Subnething

1. Konsep Dasar IP Address

Dalam konsep jaringan komputer, dimana di dalamnya adalah koneksi antar komputer yang dihubungkan dengan menggunakan perangkat penghubung. Diperlukan mekanisme pengalamatan agar antar komputer bisa saling berkomunikasi atau saling bertukar data. Untuk itu dunia jaringan komputer tidak dapat terlepas dari yang namanya protokol.

Menurut Kukuh Nugroho (2016:30) “protokol yang paling banyak digunakan sebagai sarana untuk melakukan pengalamatan dalam sebuah jaringan adalah IP (*Internet Protocol*)”.

Pada dasarnya IP merupakan sebuah identitas untuk jalur bukan menunjuk kepada sebuah komputer atau router. Apabila perangkat komputer atau router dipindah, tidak menggunakan jalur yang sama, kemungkinan besar IP sudah berubah lagi. Untuk lebih memahami konsep dasar IP penulis menjabarkan beberapa hal yang terkait dalam konsep dasar ini.

a. TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar menukar data dari satu komputer ke komputer lain di dalam suatu jaringan. Prinsip pembagian lapisan pada TCP/IP menjadi protokol komunikasi data yang fleksibel dan dapat diterapkan dengan mudah di setiap jenis komputer dan antarmuka jaringan. Oleh karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu.

b. *IP Address*

IP address adalah metode pengalamatan pada jaringan komputer dengan memberikan sederet angka pada komputer *(host)*, *router* atau peralatan jaringan lainnya. *IP address* sebenarnya bukan diberikan kepada komputer (*host*) atau *router*, melainkan pada *interface* jaringan dari *host / router* tersebut. IP (*Internet protocol*) sendiri di desain untuk interkoneksi sistem komunikasi komputer pada jaringan paket *switched*. Pada jaringan TCP/IP, sebuah komputer diidentifikasi dengan alamat IP. Tiap-tiap komputer memiliki alamat IP yang unik, masing-masing berbeda satu sama lainnya. Hal ini dilakukan untuk mencegah kesalahan pada transfer data. Terakhir, protokol data akses berhubungan langsung dengan media fisik. Secara umum protokol ini bertugas untuk menangani pendeteksian kesalahan pada saat transfer data, namun untuk komunikasi datanya, IP mengimplementasikan dua fungsi dasar yaitu *addressing* dan *fragmentasi*.

e. IPv4

IPv4 adalah sebuah jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjangnya adalah 32-bit, dan secara teoritis dapat mengalamati hingga 4 miliar *host* komputer di seluruh dunia.

Alamat *IPv4* umumnya ditulis dalam notasi desimal bertitik (*dotted-desimal notation)*, yang dibagi ke dalam empat buah oktet berukuran 8-bit. Karena setiap oktet berukuran 8-bit, maka nilainya berkisar antara 0 hingga 255. Pengalamatan *IPv4* menggunakan 32 bit yang setiap bit dipisahkan dengan notasi titik.

2. Pengertian Subnetting

Subnetting adalah upaya / proses untuk memecah sebuah network dengan jumlah host yang cukup banyak, menjadi beberapa network dengan jumlah host yang lebih sedikit. Teknik subnetting membuat skala jaringan lebih luas dan tidak dibatas oleh kelas-kelas IP (IP Classes) A, B, dan C yang sudah diatur. Dengan subnetting, anda bisa membuat network dengan batasan host yang lebih realistis sesuai kebutuhan. Subnetting menyediakan cara yang lebih fleksibel untuk menentukan bagian mana dari sebuah 32 bit IP adddress yang mewakili netword ID dan bagian mana yang mewakili host ID. Dengan kelas-kelas IP address standar, hanya 3 kemungkinan network ID yang tersedia; 8 bit untuk kelas A, 16 bit untuk kelas B, dan 24 bit untuk kelas C. Subnetting mengizinkan anda memilih angka bit acak (arbitrary number) untuk digunakan sebagai network ID. Dua alasan utama melakukan subnetting:

a. Mengalokasikan IP address yang terbatas supaya lebih efisien. Jika internet terbatas oleh alamat-alamat di kelas A, B, dan C, tiap network akan memliki 254, 65.000, atau 16 juta IP address untuk host devicenya. Walaupun terdapat banyak network dengan jumlah host lebih dari 254, namun hanya sedikit network (kalau tidak mau dibilang ada) yang memiliki host sebanyak 65.000 atau 16 juta. Dan network yang memiliki lebih dari 254 device akan membutuhkan alokasi kelas B dan mungkin akan menghamburkan percuma sekitar 10 ribuan IP address.

b. Alasan kedua adalah, walaupun sebuah organisasi memiliki ribuan host device, mengoperasikan semua device tersebut di dalam network ID yang sama akan memperlambat network. Cara TCP/IP bekerja mengatur agar

semua komputer dengan network ID yang sama harus berada di physical network yang sama juga. Physical network memiliki domain broadcast yang sama, yang berarti sebuah medium network harus membawa semua traffic untuk network. Karena alasan kinerja, network biasanya disegmentasikan ke dalam domain broadcast yang lebih kecil bahkan lebih kecil dari Class C address.

3. Pengertian Subnet Mask

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada angka biner 32 bit yang digunakan untuk membedakan network ID dengan host ID, menunjukkan letak suatu host, apakah berada di jaringan lokal atau jaringan luar.

RFC 950 mendefinisikan penggunaan sebuah subnet mask yang disebut juga sebagai sebuah address mask sebagai sebuah nilai 32-bit yang digunakan untuk membedakan network identifier dari host identifier di dalam sebuah alamat IP. Bit-bit subnet mask yang didefinisikan, adalah sebagai berikut:

a. Semua bit yang ditujukan agar digunakan oleh network identifier diset ke nilai 1.
b. Semua bit yang ditujukan agar digunakan oleh host identifier diset ke nilai 0. Setiap host di dalam sebuah jaringan yang menggunakan TCP/IP membutuhkan sebuah subnet mask meskipun berada di dalam sebuah jaringan dengan satu segmen saja. Entah itu subnet mask default (yang digunakan ketika memakai network identifier berbasis kelas) ataupun subnet mask yang dikustomisasi (yang digunakan ketika membuat sebuah subnet atau supernet) harus dikonfigurasikan di dalam setiap node TCP/IP.

C. Keamanan Jaringan

Menurut Ri2M (2010) Keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringan yang lebih banyak mempunyai ancaman keamanan dari pada komputer yang tidak

terhubung ke mana-mana. Namun dengan adanya pengendalian maka resiko yang tidak diinginkan dapat dikurangi. Adanya keamanan jaringan maka para pemakai berharap bahwa pesan yang dikirim dapat sampai dengan baik ke tempat yang dituju tanpa mengalami adanya kecacatan yang diterima oleh si penerima, misalnya saja adanya perubahan pesan. Di dalam keamanan jaringan terdapat pula resiko jaringan komputer yang merupakan segala bentuk ancaman bauk fisik maupun logic yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan. Resiko dalam jaringan komputer disebabkan oleh beberapa faktor yaitu:

1. Kelemahan manusia
2. Kelemahan perangkat keras computer
3. Kelemahan sistem operasi jaringan
4. Kelemahan sistem jaringan komnikasi

Keamanan jaringan juga mempunyai tujuan yang dapat membuat kemanan jaringan lebih ditingkatkan lagi, yaitu :

a) *Confidentiality* : Adanya data - data yang paling penting yang biasanya tidak boleh di akses oleh seseorang, maka dilakukan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Biasanya confidentiality ini berhubungan dengan informasi yang diberikan ke pihak lain
b) *Integrity* : Bahwa pesan yang disampaikan tetap orisinil yang tidak diragukan keaslianya, tidak dimodifikasi selama dalam perjalanan dari sumber ke penerimanya.
c) *Avaibility* : Dimana user yan mempunyai hak akses diberi akses tepat pada waktunya, biasanya ini berhubungan dengan ketersediaan informasi atau data ketika dibutuhkan. Apabila sistem informasi ini diserang maka akan menghambat bahkan menyebabkan tidak dapat mengakses informasi tersebut.

Tujuan keamanan jaringan dapat dicapai dengan suatu metode keamanan jaringan yang dapat melindungi sistem baik dari dalam maupun dari luar jaringan, namun bukan hanya melindungi tetapi harus

dapat bertindak apabila terjadi serangan yang ada di dalam jaringan. Namun dibutuhkan juga suatu pemahaman tentang menentukan kebijakan keamanan *(security policy*) dalam keamanan jaringan. Jika ingin menentukan apa saja yang harus dilindungi maka harus mempunyai perencanaan keamanan yang matang dan baik berdasarkan pada prosedur dan kebijakan keamanan jaringan, karena apabila tidak direncanakan maka tidak akan sesuai dengan yang diharapkan dalam perindungan jaringan.

1. Kebijakan Keamanan

Salah satu problem *network security* yang paling penting adalah menentukan kebijakan dalam *network security* (Ri2M, 2010). Kebanyakan orang menginginkan solusi soluteknis untuk setiap masalah yaituk dapat berupa program yang dapa tmemperbaiki masalah-masalah *network security*. Padahal, perencanaan keamanan yang matang berdasarkan prosedur dan kebijakan dalam network security akan membantu menentukan apa-apa yang harus dilindungi, berapa besar biaya yang harus ditanamkan dalam melindunginya, dan siapa yang bertanggung jawab untuk menjalankan langkah-langkah yang diperlukan untuk melindungi bagiantersebut.

Di dalam keamanan jaringan,peran manusia memegang tanggung jawab keamanan yang cukup berperan. Keamanan jaringan tidak akan efektif kecuali orang-orangnya mengetahui tanggung jawabnya masing-masing. Dalam menentukan *network security policy*, diperlukan adanya kebijakan apa yang diharapkan Selain itu, kebijakan ini harus mencangkup:

a. Tanggung jawab *network user*, meliputi Antara lain keharusan user untuk mengganti *password*nya dalam periode tertentu, atau memeriksa kemungkinan *password* yang kita buat bisa diakses oleh orang lain.
b. Langkah-langkah yang harus di perbuat bila terdeteksi masalah keamanan,siapa yang harus diberitahu. Hal ini harus dijelaskan dengan lengkap,bahkan hal-hal yang sederhana sepert user untuk tidak mencoba

melakukan apa-apa atau mengatasi sendiri bila masalah terjadi,dan segera memberitahu sistem administrator.

Adanya kebijakan tersebut maka manusia merupakan salah satu faktor yang sangat penting, namun sering dilupakan dalam pengembangan teknologi informasi, begitu juga dengan pengembangan di bidang keamanan jaringan. salah satu contohnya adalah dalam penggunaan *password* yang sulit justru menyebabkan pengguna menuliskanya pada kertas yang ditempelkan pada komputer atau meja. Selain faktor dari manusia, faktor yang dibutuhkan juga tergantung dari organisasi, keputusan yang di ambil merupakan keputusan tentang keamanan komputer, dan juga masalah biaya dari suatu sistem keamanan.

2. Mengenali ancaman terhadap network security

Langkah awal dalam mengembangkan rencana *network security network security* yang efektif adalah dengan mengenali ancaman yang mungkin datang.

a. Akses tidak sah, oleh orang yang tidak mempunyai wewenang.
b. Kesalahan informasi, segala masalah yang dapat menyebabkan diberikanya informasi yang penting atau sesitif kepada orang yang salah, yang seharusnya tidak boleh mendapatkan informasi tersebut.
c. Penolakan terhadap *service*, segala masalah mengenai *security* yang menyebabkan sistem mengganggu pekerjaan-pekerjaan yang produktif.

3. Serangan Pada Jaringan Komputer

Jaringan komputer merupakan kumpulan dimana komputer saling terhubung satu dengan yang lainnya.Dengan adanya jaringan komputer ini pengguna dapat saling berinteraksi dengan pengguna lainnya.Seperti mengirim file,foto,video,chating dan lainnya.Tetapi disamping itu ada beberapa ancaman yang sering terjadi berupa serangan pada jaringan komputer.

Adapun jenis dan teknik serangan yang mengganggu jaringan komputer beraneka jenis, diantaranya adalah :

a. Port Scanning

Merupakan suatu proses untuk mencari dan membuka *port* pada suatu jaringan komputer. Dari hasil *scanning* akan didapat letak kelemahan sistem tersebut. Pada dasarnya sistem *port scanning* mudah untuk dideteksi, tetapi penyerang akan menggunakan beberapa cara metode untuk menyembunyikan serangan.

b. Teardrop

Teknik penyerangan dengan mengeksploitasi proses *disassembly reassembly* paket data. Dalam jaringan internet sering kali data harus dipotong menjadi paket yang lebih kecil untuk menjamin *reliabilitas* dan proses *multiple* akses jaringan.Pada proses pemotongan data paket yang normal, setiap potongan diberi informasi *offset* data yang berbunyi "Potongan *byte* ini merupakan potongan 600 *byte* dari total 800 *byte* paket yang dikirimkan".

c. IP spoofing

Teknik ini bekerja dengan mengganti alamat IP pengguna yang lain yang bukan penyerang sebenarnya. Hal ini terjadi karena salah rancang *(design flaw)* bagian urutan nomor *(sequence number)* dari paket *TCP/IP*. Dalam beberapa kasus,penyerang menggunakan satu alamat IP sumber yang spesifik pada semua paket IP yang keluar untuk membuat semua pengembalian paket IP dan pesan ICMP ke pemilik alamat tersebut.

d. ICMP flood

Penyerang melakukan eksploitasi dengan tujuan untuk membuat target host menjadi terganggu, yang disebabkan oleh pengiriman sejumlah paket yang besar ke arah target *host. Eksploitasi* sistem ini dilakukan dengan mengirimkan suatu perintah "ping" dengan tujuan *broadcast a*tau multicast dimana pengirim dibuat seolah-olah adalah target host. Semua balasan dikembalikan ke target host. Hal inilah yang menyebabkan host target menjadi terganggu dan menurunkan kinerja jaringan bahkan dapat menyebabkan *denial of service.*

e. UDP flood UDP flood

Dengan cara *spoofing,User Datagram Protocol (UDP) flood attack* akan menempel pada servis *UDP chargen* di salah satu mesin, yang untuk keperluan“percobaan” akan mengirimkan sekelompok karakter ke mesin lain, yang diprogram untuk mengecho setiap kiriman karakter yang diterima melalui *servis chargen.* Karena paket *UDP* tersebut di-spoofing diantara ke dua mesin tersebut maka yang terjadi adalah “banjir” tanpa henti paket kiriman karakter yang tidak berguna diantara diantara kedua mesin tersebut. Untuk menanggulangi *UDP flood,disable* semua *servis UDP* di semua mesin di jaringan, atau dengan menyaring semua *servis UDP* yang masuk pada *firewall*.

f. Packet interception

Gangguan jenis ini dilakukan dengan membaca paket di saat paket tersebut sedang mengalami *packet sniffing*. *Packet interception* merupakan cara penyerang untuk mendapatkan informasi yang ada di dalam paket tersebut.Hal ini dapat dicegah dengan mengenkripsi terlebih dahulu,sehingga penyerang akan mengalami kesulitan untuk membuka paket tersebut.

g. Smurf attack

Gangguan jenis ini biasanya dilakukan dengan menggunakan IP *spoofing,*yaitu mengubah nomor IP dari datangnya *request*.Dengan menggunakan *IPspoofing,respons* dari ping tadi dialamatkan ke komputer yang IP-nya di *spoof*. Akibatnya, komputer tersebut akan menerima banyak paket. Hal ini dapat mengakibatkan pemborosan penggunaan *bandwidth* jaringan yang menghubungkan komputer tersebut.

h. Ddos (Distributed Denial of Service) Serangan DDOS

Serangan DOS (*Denial-Of-Service attacks*) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat

menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Dalam sebuah serangan *Denial of Service*,si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai *traffic flooding.*
2. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga *request* yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut.Teknik ini disebut sebagai request *flooding*.
3. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara,termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server.

Bentuk serangan *Denial of Service* awal adalah serangan *SYN Flooding Attack*, yang pertama kali muncul pada tahun 1996 dan mengeksploitasi terhadap kelemahan yang terdapat di dalam protokol *Transmission Control Protocol (TCP*). Serangan-serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat di dalam sistem operasi,layanan jaringan atau aplikasi untuk menjadikan sistem, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami crash.

Beberapa contoh Serangan DDOS lainnya adalah:

a) Serangan *Buffer Overflow*, mengirimkan data yang melebihi kapasitas sistem,misalnya paket *ICMP* yang berukuran sangat besar.
b) Serangan *SYN*, mengirimkan data *TCP SYN* dengan alamat palsu.

c) Serangan *Teardrop*, mengirimkan paket IP dengan nilai *offset* yang membingungkan.
d) Serangan Smurf, mengirimkan paket *ICMP* bervolume besar dengan alamat *host* lain.
e) *ICMP Flooding*

i. Ping of death

Ping Kematian (*Ping of death* disingkat ***POD***) adalah jenis serangan pada komputer yang melibatkan pengiriman ping yang salah atau berbahaya ke komputer target. Sebuah ping biasanya berukuran 56 i (atau 84 *bytes* ketika header IP dianggap). Dalam sejarahnya, banyak sistem komputer tidak bisa menangani paket ping lebih besar daripada ukuran maksimum paket IP, yaitu 65.535 *byte*. Mengirim ping dalam ukuran ini (65.535 *byte*) bisa mengakibatkan kerusakan (*crash*) pada komputer target.

Secara tradisional, sangat mudah untuk mengeksploitasi bug ini.Secara umum,mengirimkan paket 65.536 *byte* ping adalah illegal menurut protokol jaringan, tetapi sebuah paket semacam ini dapat dikirim jika paket tersebut sudah terpecah-pecah, Ketika komputer target menyusun paket yang sudah terpecah-pecah tersebut, sebuah *buffer overflow* mungkin dapat terjadi,dan ini yang sering menyebabkan sistem crash.

j. Sniffer

Sniffer Paket atau penganalisa paket (arti tekstual:pengendus paket dapat pula diartikan (‘penyadap paket’) yang juga dikenal sebagai *Network Analyzers* atau *Ethernet Sniffer* ialah sebuah aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Dikarenakan data mengalir secara bolak-balik pada jaringan,aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari *RFC*(*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti *hub* atau *switch*), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu

lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (*promiscuous mode*) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel).

Sniffer paket dapat dimanfaatkan untuk hal-hal berikut:

1. Mengatasi permasalahan pada jaringan komputer.
2. Mendeteksi adanya penyelundup dalam jaringan (*Network Intusion*).
3. Memonitor penggunaan jaringan dan menyaring isi isi tertentu.
4. Memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya (misalkan *password*).
5. Dapat digunakan untuk *Reverse Engineer* pada jaringan.

k. DNS Poisoning

DNS *Poisoning* merupakan sebuah cara untuk menembus pertahanan dengan cara menyampaikan informasi *IP Address* yang salah mengenai sebuah host, dengan tujuan untuk mengalihkan lalu lintas paket data dari tujuan yang sebenarnya. Cara ini banyak dipakai untuk menyerang situs-situs *e-commerce* dan banking yang saat ini bisa dilakukan dengan cara online dengan pengamanan Token. Teknik ini dapat membuat sebuah server palsu tampil identik dengan dengan server online banking yang asli. Oleh karena itu diperlukan digital cerficate untuk mengamankannya,agar server palsu tidak dapat menangkap data otentifikasi dari nasabah yang mengaksesnya. Jadi dapat disimpulkan cara kerja DNS (Domain Name System) poisoning ini adalah dengan mengacaukan DNS *Server* asli agar pengguna Internet terkelabui untuk mengakses web site palsu yang dibuat benar-benar menyerupai aslinya tersebut, agar data dapat masuk ke server palsu.

l. Trojan Horse

Trojan *horse* atau Kuda Troya atau yang lebih dikenal sebagai Trojan dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (malicious

software/malware) yang dapat merusak sebuah sistem atau jaringan.Tujuan dari Trojan adalah memperoleh informasi dari target (password, kebiasaan user yang tercatat dalam system log, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target).

Cara Kerja Trojan berbeda dengan jenis perangkat lunak mencurigakan lainnya seperti virus komputer atau worm karena dua hal berikut:

1. Trojan bersifat "stealth" (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau worm bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi crash.
2. Trojan dikendalikan dari komputer lain (komputer attacker).

Ada beberapa jenis Trojan yang beredar antara lain adalah:

a) Pencuri password: Jenis Trojan ini dapat mencari password yang disimpan di dalam sistem operasi (/etc/passwd atau /etc/shadow dalam keluarga sistem operasi UNIX atau berkas *Security Account Manager (SAM)* dalam keluarga sistem operasi Windows NT) dan akan mengirimkannya kepada si penyerang yang asli. Selain itu, jenis Trojan ini juga dapat menipu pengguna dengan membuat tampilan seolah-olah dirinya adalah layar login (/sbin/login dalam sistem operasi UNIX atau *Winlogon.exe* dalam sistem operasi Windows NT) serta menunggu pengguna untuk memasukkan passwordnya dan mengirimkannya kepada penyerang. Contoh dari jenis ini adalah Passfilt Trojan yang bertindak seolah-olah dirinya adalah berkas Passfilt.dll yang aslinya digunakan untuk menambah keamanan password dalam sistem operasi *Windows NT*,tapi disalah gunakan menjadi sebuah program pencuri *password*.

b) Pencatat penekanan tombol (*keystroke logger/keylogger*):Jenis Trojan ini akan memantau semua yang diketikkan oleh pengguna dan akan mengirimkannya kepada penyerang. Jenis ini berbeda dengan spyware, meski dua hal tersebut melakukan hal yang serupa (memata-matai pengguna).

c) *Tool* administrasi jarak jauh *(Remote Administration Tools/RAT*): Jenis Trojan ini mengizinkan para penyerang untuk mengambil alih kontrol secara penuh terhadap sistem dan melakukan apapun yang mereka mau dari jarak jauh, seperti memformat hard disk, mencuri atau menghapus data dan lain-lain. Contoh dari Trojan ini adalah *Back Orifice,Back Orifice* 2000,dan SubSeven.

d) DDoS Trojan atau Zombie Trojan: Jenis Trojan ini digunakan untuk menjadikan sistem yang terinfeksi agar dapat melakukan serangan penolakan layanan secara terdistribusi terhadap *host* target.

e) Ada lagi sebuah jenis Trojan yang mengimbuhkan dirinya sendiri ke sebuah program untuk memodifikasi cara kerja program yang diimbuhinya. Jenis Trojan ini disebut sebagai *Trojan virus.*

*f) Cookies Stuffing,*ini adalah script yang termasuk dalam metode *blackhat,* gunanya untuk membajak *tracking code* penjualan suatu produk,sehingga komisi penjualan diterima oleh pemasang *cookies stuffing,* bukan oleh orang yang terlebih dahulu mereferensikan penjualan produk tersebut di *internet.*

D. Pengenalan Linux

1. Sejarah Linux

Ali Akbar (2006) Sejarah linux dimulai dari dua orang tokoh yang bernama Richard Stallman dan Linus Torvalds. Richard Stallman yang memiliki pandangan unik bahwa hak seorang programer adalah mendapatkan source code yang gratis untuk aplikasi yang didapatkannya, maka Richard Stallman menginisialisasi sebuah gerakan yang dinamakan

Free Software Movemant, gerakan ini berkembang hingga akhirnya berdiri organisasi bernama GNU *Fondation.* GNU *Fondation* juga menghasilkan banyak *software* yang dilisensikan menggunakan aturan GPL sehingga pengguna dari program tersebut bebas menggunakannya secara free.

Linux versi 0.01 dikerjakan sekitar bulan Agustus 1991. Kemudian pada tanggal 5 Oktober 1991, Linus mengumumkan versi resmi Linux, yaitu versi 0.0.2 yang hanya dapatmenjalankan *Shell bash (GNU Bourne Again Shell)* dan *GCC(GNU C Compiler).*

Saat ini Linux adalah sisitem UNIX yang sangat lengkap,bisa digunakan untuk jaringan,pengembangan *software* dan bahkan untuk pekerjaan sehari-hari. Linux memiliki perkembangan yangs angat cepat. Hal ini dapat terjadi karena Linux dikembangkan oleh beragam kelompok orang. Keragaaman ini termasuk tingkat pengetahuan pengalaman serta *geografis*. Agar kelompok ini dapat berkomunikasi dengan cepat dan efisien, internet menjadi pilihan yang sangat tepat.

2. Pengertian Linux

Ali Akbar (2006) Linux secara istilah merupakan kata yang mengacu pada sebuah sistem operasi yang dilisensikan dengan sistem GPL (GNU *General Public License* atau *Guaranteed Public for Life).* Dalam arti sempit yang dinamakan linux hanyalah kernelnya saja.

Linux adalah sebuah software sistem operasi open source yang gratis untuk disebarluaskan dibawah lisensi GNU. Linux merupakan turunan dari UNIX dan dapat bekerja pada berbagai macam perangkat keras kompter. Dengan lisensi *GNU (Gnu Not Unix)* kita dapat memperoleh program, lengkap dengan kode sumbernya (*source code*).

3. Kelebihan dan Kekurangan Linux

a. Kelebihan

1) Bersifat *Open source*,bebas dan terbuka. Sehingga tidak perlu biaya untuk mendapatkannya.

2) Linux sekarang sudah mudah untuk dioperasikan,kalau dulu penggunaan linux diidentik dengan para hacker. Sekarang orang awam seperti saya pun sudah banyak yang menggunakannya.
3) Hampir semua aplikasi yang digunakan di windows sudah ada aplikasi linuxnya yang dikembangkan oleh komunitas linux atau bisa juga menggunakan *software emulator*.
4) Memiliki keamanan yang lebih unggul karena didedain *multiuser* sehingga apabila *virus* menyerang user tertentu, akan sangat sulis untuk menyebar ke *user* yang lain.
5) Cocok untuk *PC* yang memiliki spesifikasi minimum karena linux membutuhkan *resource* yang lebih kecil dibandingkan dengan *windows*.
6) Linux dapat dijalankan di dua mode.
7) Jarang *crash* atau hang yang mengharuskan kita untuk merestart komputer karena linux lebih stabil.
8) Memiliki komunitas diberbagai penjuru dunia.
9) Terdapat beragam pilihan seperti Uuntu, Fedora, Debian, Centos, RedHat, Opensuse, Mandriva, dan sebagainya.

b. Kekurangan Linux

1) Banyak *user* yang belum terbiasa menggunakan linux.
2) Dukungan hardware dari vendor tertentu yang tidak terlalu baik pada linux.
3) Proses instalasinya tidak semudah windows.
4) Aplikasi di linux belum sebagus aplikasi *windows.*
5) Bagi *administrator* sistem yang belum terbiasa dengan Unix atau Linux ya mau atau tidaknya harus belajar dulu memahami tentang linux
6) Struktur *directori* dan hak akses yang membingungkan bagi *user* yang terbiasa menggunakan *windows*.

4. Macam-Macam Distro Linux

a. *Xandros*

Xandros adalah sebuah Distro Linux yang berdasarkan pada KDE. Tampilannya mirip dengan *Microsoft windows*, sehingga mengoperasikannya sangat mudah.

b. *Ubuntu*

Ubuntu adalah Distro Linux yang berbasis Debian.*Canonical Ltd* (Perusahaan milik mark shuttleworth) yang menyeponsori proyek Ubuntu. Nama Ubuntu sendiri diambil dari konsep ideologi afrika selatan. Ubuntu berasal dari bahasa kuno afrika yang berarti "rasa keperimanusiaan terhadap sesama manusia".

c. *CentOS*

CentOS adalah distro linux yang bebas,yang didasarkan pada *Red Hatt Enterprise Linux* (RHEL). *ChentOS* sendiri.

d. Debian

Debian adalah sistem operasi yang berbasis kernel Linux. Debian adalah "*Kernel Independen*", yaitu sistem operasi debian yang dikembangkan dengan murni tanpa mendasarkan pada sistem operasi yang telah ada.

e. Fedora

Fedora adalah sebuah distro Linux yang berbasis RPM dan Yum, distro fedora sendiri dikembangkan oleh *Fedora Project* yang didukung oleh komunitas *programer* dan disponsori oleh *Red Hat*. Nama fedora sendiri berasal dari karakter fedora yang digunakan dilogo Red Hat.

f. Knoppix

Knoppix adalah distro Linux Live-cd yang dijalankan tanpa CD-ROM tanpa instalasi di Hardisk.Distro ini berbasiskan Debian Linux yang diciptakan oleh *Knopper*.

g. Gentoo Linux

Gentoo Linux adalah suatu distribusi linux yang memakai paket sistem *management Portage*.

h. Slackware

Slackware adalah sistem operasi yang dibuat oleh Patrick Volkerding dari *Slackware Linux Inc*. Slackware merupakan salah satu distro awal,dan merupakan yang tertua yang masih dikelola. Tujuan utama *Slackware* adalah stabilitas dan kemudahan desain, serta menjadi Distro Linux yang paling mirip dengan Unix.

i. Mandriva

Mandriva adalah sistem operasi yang dibuat oleh Mandriva, Mandriva Linux menggunakan RPM *Package Manager*.

j. OpenSUSE

OpenSUSE adalah salah satu Distro Linux dari perusahaan *Novell / SUSE Linux GmbH.*

k. FreeSpire

Freespire adalah Distro Linux versi gratis dari Linspire (a.k.a Lindows), dikarenakan masalah nama, dirubah menjadi *Linspire.*

l. Linux Mint

Linux Mint adalah sistem operasi berbasis Linux untuk PC. Inti dari Linux mint adalah Ubuntu, sehingga aplikasi yang berjalan di Ubuntu juga bisa berjalan pada Linux mint.

m. PC LinuxOS

PCLinuxOS adalah sistem operasi dekstop. Ini adalah sebuah sistem operasi bebas untuk komputer pribadi yang bertujuan untuk memudahkan pengguna.

n. Damn Small Linux

Damn Small Linux adalah salah satu varian linux mini, Karena ukurannya yang kecil sekiran 50MB. DSL juga memungkinkan untuk diinstal di *USB* 128MB.

o. Kuliax

Kuliax adalah sebuah distribusi Linux LiveCD.Dikembangkan oleh *Kuliax Project* untuk pendidikan di Universitas. Distribusi ini

berbasis Debian GNU/Linux dan Knoppix, dan telah dioptimasi ke arah pengguna dekstop Linux.

p. Redhat

Redhat adalah distribusi yang paling populer,minimal di indonesia,redhat merupakan distribusi pertama yang instalasi dan pengoperasiannya mudah.

q. Kali Linux

Kali linux adalah sebuah OS pembaharuan dari *BackTrack*. *BackTrack* sendiri sudah tidak dikembangkan lagi, dan versi terbaru dari *BackTrack* adalah *Kali Linux* ini. *Kali Linux* digunakan sebagai *OS* untuk penetrasi dan kemanan.

E. PENGENALAN LINUX UBUNTU

1. Pengertian Linux Ubuntu

Westriningsih (2013) Ubuntu merupakan salah satu distribusi Linux yang berbasiskan Debian dan didistribusikan sebagai software bebas. nama Ubuntu berasal dari filosofi dari Afrika Selatan yang berarti “Kemanusiaan kepada sesama”. Ubuntu didesain untuk kepentingan penggunaan personal, namun versi server Ubuntu juga tersedia, dan telah dipakai secara luas. Proyek Ubuntu resmi disponspori oleh Canonical Ltd. yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha Afrika Selatan Mark Shuttleworth. Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam Filosofi Ubuntu ke dalam dunia perangkat lunak. Ubuntu adalah sistem operasi lengkap berbasis Linux, tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional. Selain itu, Ubuntu juga bersifat Open Source. Open source adalah Kekuatan komunitas seluruh dunia yang sangat ahli terampil yang membangun, berbagi dan meningkatkan perangkat lunak yang sangat terbaru bersama kemudian membuatnya tersedia untuk semua orang.

Komunitas open-source berkembang dan saat ini menawarkan beberapa otak terbaik dalam bisnis ini. Tujuannya tidak berubah: sistem bebas dan perangkat lunak harus tersedia untuk semua orang, dimanapun mereka berada. Ada prinsip inti dari software open-source:

a. Perangkat lunak harus bebas untuk mendistribusikan.
b. Program harus menyertakan kode sumber.
c. Lisensi harus memungkinkan orang untuk bereksperimen dengan dan mendistribusikan modifikasi.
d. Pengguna memiliki hak untuk mengetahui siapa yang bertanggung jawab untuk perangkat lunak yang mereka gunakan.
e. Tidak boleh ada diskriminasi terhadap setiap orang atau kelompok.
f. Lisensi tidak boleh melarang siapapun untuk memanfaatkan program dalam bidang tertentu.
g. Tidak ada yang perlu untuk memperoleh lisensi tambahan untuk menggunakan atau mendistribusikan program tersebut.
h. Lisensi tidak boleh spesifik untuk produk.
i. Lisensi tidak boleh membatasi perangkat lunak lain.

2. Sejarah Linux Ubuntu

M Reynaldi Fauzi (2014) Ubuntu pertama kali dirilis pada 20 Oktober 2004, versi-versi ubuntu akan dirilis stiap 6 bulan sekali agar dapat memperbaharui sistem keamanan dan update program. LTS (Long Term Support) rilis, yang terjadi setiap dua tahun, didukung untuk tiga tahun pada desktop dan server untuk lima tahun. Andy Fitzsimon merupakan pencipta logo dari ubuntu yang sampai pada saat ini tidak ada perubahan dalam logo tersebut. Default User Interfaceny menggunakan GNOME .

Sejak pertama kali diluncurkan, Ubuntu mendapat perhatian yang sangat besar dari pengguna Linux yang lain. Hal ini disebabkan karena kestabilan yang dimiliki oleh Ubuntu itu sendiri. Selain itu kenyamanan dan kemudahan yang dimiliki Ubuntu menjadi daya tarik yang besar bagi pengguna Linux di seluruh belahan dunia.

Adapun versi Ubuntu yang telah dirilis dan telah beredar adalah sebagai berikut :

a. Versi 4.10 (Warty Warthdog).
b. Versi 5.04 (Hoary Hedgedog).
c. Versi 5.10 (Breezy Badger).
d. Versi 6.06 (Drapper Drake).
e. Versi 6.10 (Edgy Eft).
f. Versi 7.04 (Feisty Fawn).
g. Versi 7.10 (Gutsy Gibbson).

3. Perbedaan Linux *Ubuntu* dan *Windows*

Ada beberapa perbedaan antara Linux Ubuntu dengan *Windows*, yaitu :

a. Ubuntu dan Windows sama-sama nama untuk sistem operasi "komputer" dan sama-sama punya beberapa jenis atau pilihan, misal Linux Nusantara, BlankOn, Ubuntu, Mandriva, Fedora, openSUSE, Slackware, Debian, Gentoo, Redhat, Mint, dll. Sedanhkan di Windows ada Windows 98, Me, XP, Vista, 7, Server 2008, Mobile, dll. "komputer" itu bisa berupa pc, notebook, smartphone, dll.
b. Kita bisa mendapatkan Linux tanpa harus membayar apapun, beda dengan *Windows* yang mengharuskan kita membeli Lisensi (dan kita bisa berurusan dengan hukum bila ketahuan memakai Windows Bajakan). Di Linux tidak ada istilah "Linux Bajakan".
c. Virus-virus di *Windows* tidak akan bisa jalan di Linux. Virus untuk Linux memang ada, tapi tidak berkembang. Sehingga bisa dibilang aman untuk digunakan.
d. Hampir semua program yang ada di *Windows*, ada padanan/penggantinya di Linux. Kita tinggal memilihnya dari banyak program yang tersedia di Software Center (di Ubuntu). Aplikasi Office: OpenOffice atau LibreOffice, Pemutar Musik: Rhythmbox, Exaile, Amarok, Banshee, Pemutar Video: VLC Media Player, Totem Movie Player, Browser: hampir semua browser terkenal bisa jalan di Linux, Firefox, Google

Chrome, Opera, Email Client: Thunderbird, Empathy. IM: Pidgin (bisa buat chat facebook, YM juga bisa), Emesene, Twitter juga bisa.

e. Linux kompatibel dengan file-file *Windows*, Linux secara *default* sudah bisa mengenali file PDF, bahkan OpenOffice bisa langsung menyimpan format dokumen ke PDF. Format DOCX milik Ms Word juga bisa dikenali oleh OpenOffice.

4. Kelebihan Linux Ubuntu

Linux Ubuntu juga memiliki kelebihan, yaitu :

a. Freeware, yaitu software yang bersifat free tanpa ada tuntutan dari hak cipta.
b. Kita bisa mencoba menggunakan ubuntu tanpa perlu menginstalnya kedalam hard disk computer, dengan menggunakan fitur Live CD pada Ubuntu melalui proses boot pada CD atau flash disk saja.
c. Start / shutdown cepat.
d. Tahan virus.
e. Hasil update game online tersimpan dalam server (patch game online) termasuk flash player.
f. Performansi bagus (speedy 1 Mbps terasa seperti speedy 2 Mbps)
g. Dengan sedikit oprek pada squid bisa cache dinamic content seperti video youtube.
h. Banyak yang mengatakan kalau kepingin bisa cache youtube harus pake LUSCA.
i. Tersedia banyak aplikasi mulai dari aplikasi Office (libreOffice, openOffice), browsing (Firefox, chromunium), multimedia (Rhythmbox, VLC player), grafik (GIMP, shotwell), game (linecity, hedgewar), edukasi/pendidikan (educational suite gcomprize,quran) dan berbagi aplikasi lainnya yang sebagian besar diantaranya adalah gratis (*free*).
j. Terdapat lebih dari 55 bahasa, termasuk bahasa Indonesia. Sehingga memudahkan anda dalam menggunakan Ubuntu, jika anda tak mengerti bahasa Inggris.

k. Tidak begitu membutuhkan hardware yang terlalu besar kapasitasnya maupun biayanya.
l. Akses data full proteksi dari pengguna

5. Kelemahan Linux Ubuntu

Linux Ubuntu juga memiliki kelemahan seperti :

a. Struktur direktori dan hak akses yang sudah terbiasa dengan Windows dan belum mengenal UNIX/Linux sama sekali.
b. Proses instalasi agak lama karena paket yang di install harus update secara online.
c. Belum user friendly, dikarenakan sebagian besar pengguna Ubuntu berasal dari migrasi Windows dan lainnya.
d. Tak semua aplikasi windows anda kompatibel dengan wine sehingga aplikasi kegemaran kita mungkin tidak bisa digunakan di Ubuntu.

6. Fitur – fitur Linux Ubuntu.

Di linux ubuntu ini terdapat fitur-fitur yang dapat kita gunakan berikut fitur fitur nya di bawah ini :

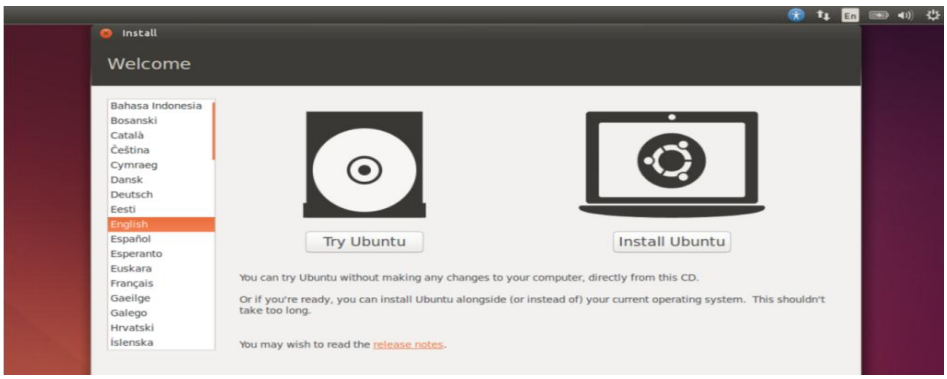
a. Web browsing Ubuntu memiliki segala yang dibutuhkan untuk menelusuri web dengan cepat dan aman. Mozilla Firefox datang sebagai standar dan Anda dapat memilih browser alternatif seperti Google Chrome dari Pusat Ubuntu Software.
b. Aplikasi Office Ubuntu sangat kompatibel dengan Microsoft Office. Itu berarti kita dapat membuka dan mengedit file seperti dokumen Word, Excel spreadsheet dan presentasi PowerPoint, dan membaginya dengan pengguna lainnya dengan cepat dan mudah.
c. Sosial dan email Ubuntu dikemas dengan aplikasi untuk komunikasi cepat dan mudah. Dan dengan Thunderbird, kita dapat mengakses email, buku alamat dan kalender.

d. Musik dan mobile Bermain, membuat dan mengedit MP3, streaming musik ke PC atau ponsel. Ubuntu punya semua yang kita butuhkan untuk mendengarkan musik.
e. Foto dan video Ubuntu adalah penuh dengan aplikasi gratis untuk membantu kita mengelola, mengedit dan berbagi foto dan video kita dengan dunia, apa pun gadget yang kita gunakan, dengan dukungan fantastis untuk kamera dan telepon, kita tidak perlu driver tambahan.
f. Ubuntu Software Centre Ubuntu Software Centre memberikan Anda akses cepat ke ribuan aplikasi gratis dan open source. Dan sekarang kita dapat membeli aplikasi dari beberapa penyedia terkemuka juga. Semua perangkat lunak kami adalah mudah untuk menemukan dan menginstal sehingga kita dapat memiliki desktop sesuai dengan yang kita inginkan dalam waktu singkat.

7. Penginstalan Linux Ubuntu

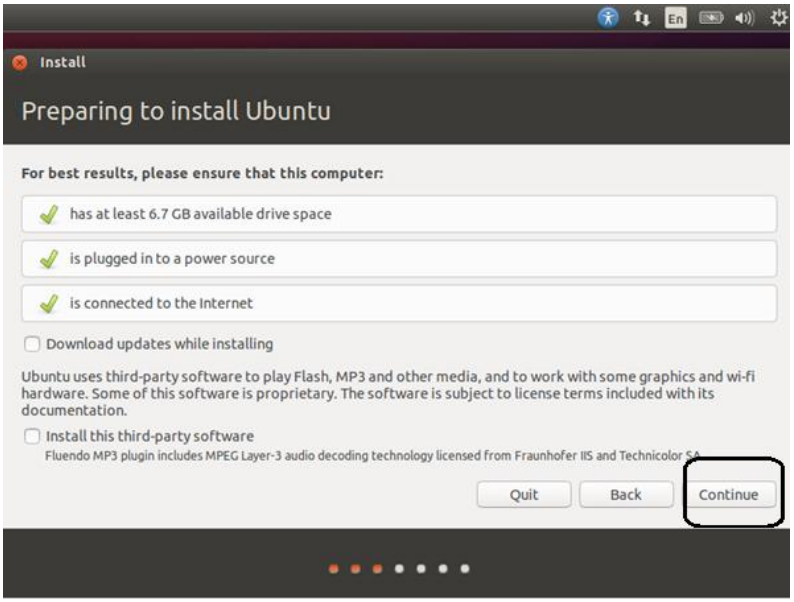
Pada tahap ini akan membahas proses penginstallan sistem operasi *Linux Ubuntu* sebagai server yang akan diinstallkan *suricata* sebagai IDPS.

a. Langkah pertama dalam penginstallan *linux ubuntu* ialah memilih bahasa lalu, pilih *button install linux ubuntu* untuk menginstall *ubuntu* secara langsung tanpa mencoba terlebih dahulu.



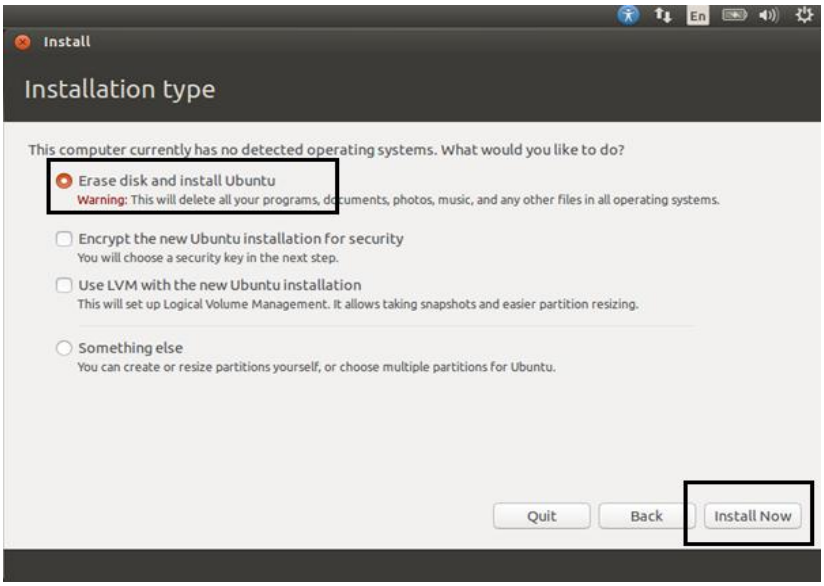
Gambar 2. 4 *Pemilihan Bahasa*

b. Selanjutnya tunggu paket-paket ubuntu terinstall semua. Setelah semua tersinstall, dapat dilihat dengan ketika paket sudah tercentang hijau maka dapat dilanjutkan dengan mengklik *button continue*.



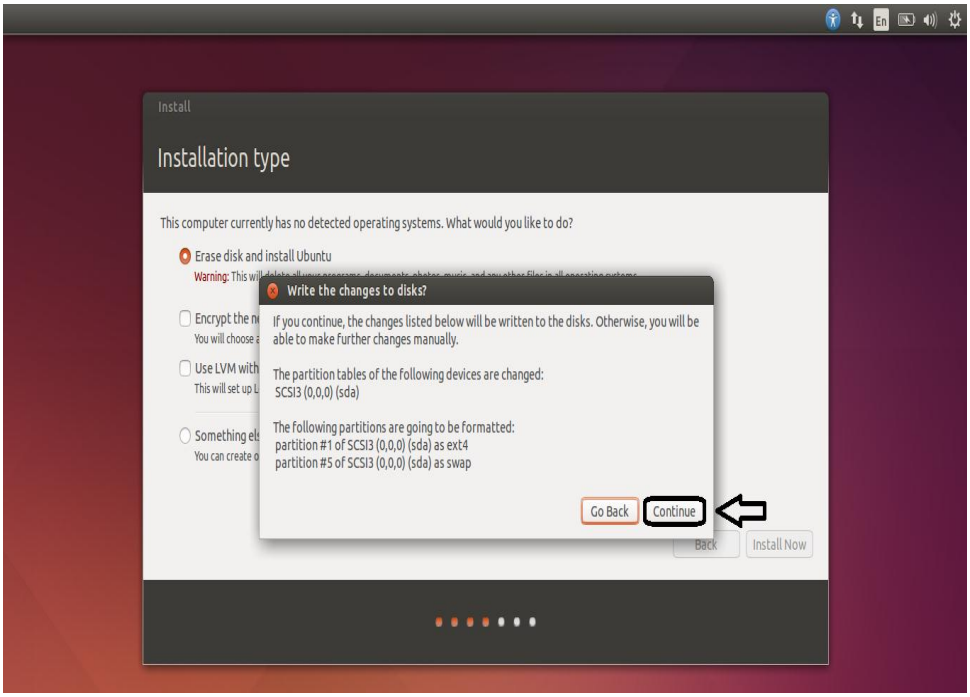
Gambar 2. 5 *Penginstalan Paket Ubuntu*

c. Tahap selanjutnya pilih *erase disk and install ubuntu* untuk menghapus data pada partisi server dan untuk menginstalkan ubuntu. Klik *install now* untuk memulai instalan.



Gambar 2. 6 *Menghapus Disk dan Install Ubuntu*

d. Klik continue. Untuk mengkonfirmasi installan sudah siap untuk dijalankan.

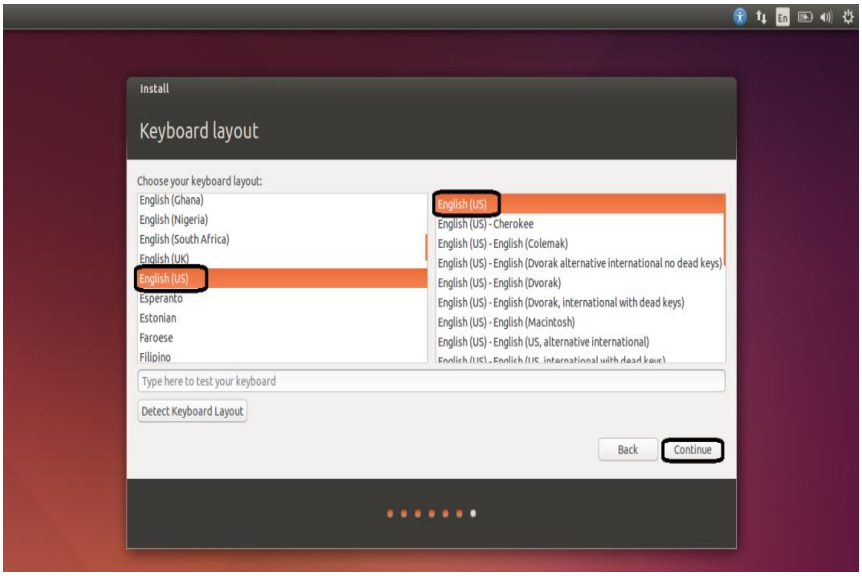


Gambar 2. 7 *Konfirmasi Instalan*

e. Pilih lokasi default untuk menentukan waktu setempat. Disini pilih Jakarta *time*, karena posisi penulis mengikuti Waktu Indonesia bagian Barat.

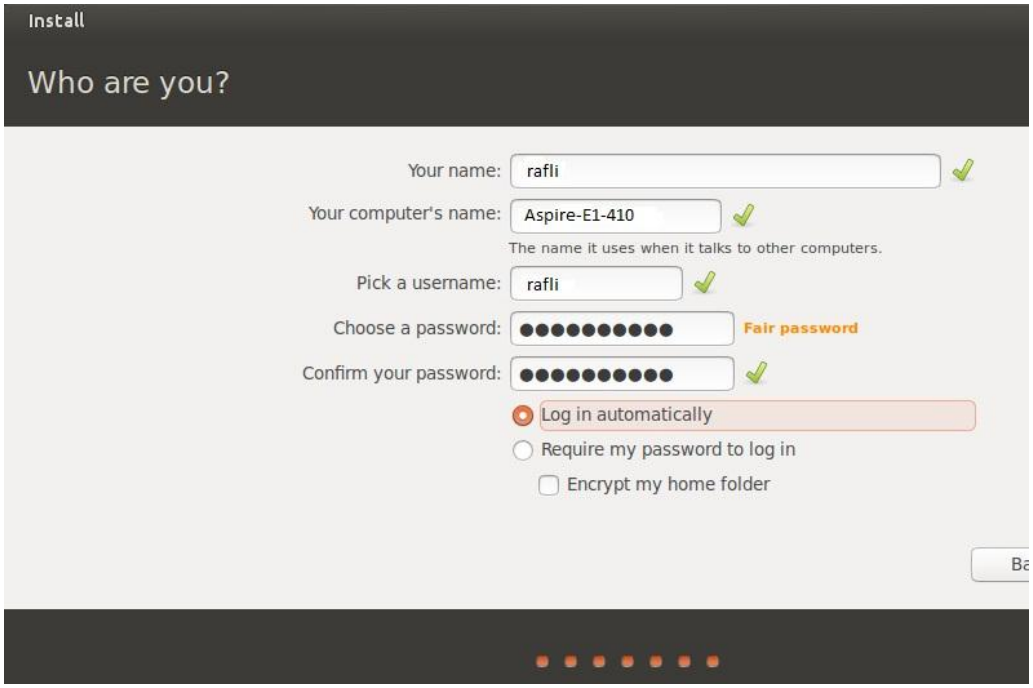
Gambar 2. 8 *Pemilihan Lokasi Waktu*

f. Pilih mode *keyboard* yang dibutuhkan. Untuk menyesuaikan dengan server, penulis memilih mode *keyboard English(US)*.



Gambar 2. 9 *Pemilihan mode keyboard*

g. Isi nama *user* server dan *password* untuk *login linux ubuntu.*



Gambar 2. 10 *User*

h. Selanjutnya tunggu proses penginstalan selesai lalu *restart* ubuntu. Setelah ubuntu hidup kembali, *linux ubuntu* siap untuk digunakan dan diinstalkan *Snort*.

F. *SNORT Intrusion Detection System* (IDS)

Denny Wijanarko (2015) Snort Intrusion Detection System (IDS) merupakan IDS open source yang secara defacto menjadi standar IDS di industri. Snort dapat diimplementasikan dalam jaringan yang multiplatform, salah satu kelebihannya adalah mampu mengirimkan alert dari mesin Unix atupun Linux ke platform Microsoft Windows dengan melalui Server Message Block (SMB).Snort dapat bekerja dalam 3 modus:sniffer mode (penyadap), packet logger dan network intrusion detection mode. Modus kerja yang akan digunakan dalam membangun sistem pencegahan penyusupan adalah modus kerja network intrusion detection. Snort memiliki kemampuan untuk mengumpulkan data log seperti alert dan yg lainnya ke dalam database. Snort diciptakan untuk menjadi IDS berbasiskan open source yang berkualitas tinggi. Snort di desain untuk dapat digabung dengan tools yang sudah ada dan kemampuan ekspansi yang tinggi.

1. Komponen Snort

Snort dibagi kedalam beberapa komponen. Komponen ini bekerjasama untuk mendeteksi serangan yang berbeda dan untuk menghasilkan keluaran pada format yang diinginkan pada sistem deteksi. IDS berbasiskan Snort umumnya terdiri dari komponen :

a. Dekoder Paket

Dekoder paket mengambil paket dari beberapa jenis jaringan yang berbeda dari antarmuka jaringan dan mempersiapkan paket untuk di proses atau di kirim menuju detection engine. Antarmukanya dapat berupa Ethernet, SLIP, PPP dan yang lain.

b. Preprocessor

Preprocessor merupakan komponen atau plug-ins yang dapat digunakan pada snort untuk menyusun atau mengubah paket data sebelum detection engine melakukan beberapa operasi untuk mencari tahu jika paket digunakan oleh penyusup. *Preprocessor* pada snort dapat mendekode-kan URL HTTP, *men-defragmentasi* paket,

menggabungkan kembali aliran TCP dan yang lain.Fungsi ini merupakan bagian yang sangat penting pada sistem deteksi intrusi.

c. Detection Engine

Detection engine adalah bagian terpenting dari Snort. Tugasnya adalah untuk mendeteksi jika terjadi aktifitas penyusup pada paket. *Detection engine* mempekerjakan rules Snort untuk tujuan ini. Rules dibaca ke dalam struktur atau rantai data internal kemudian dicocokkan dengan paket yang ada. Jika paket sesuai dengan rules yang ada, tindakan akan diambil,jika tidak paket akan dibuang. Tindakan yang diambil dapat berupa logging paket atau mengaktifkan alert.

Detection engine merupakan bagian dari snort yang sangat bergantung pada waktu tanggap. Waktu tanggap merupakan waktu yang dibutuhkan untuk merespon paket, hal ini bergantung pada seberapa bagus server yang ada dan seberapa banyak rules yang telah didefinisikan.Berikut hal-hal yang mempengaruhi waktu tanggap pada detection engine :

1) Jumlah rules
2) Kekuatan mesin pada sistem
3) Kecepatan bus internal server snort
4) Beban pada jaringan Ketika mendesain sistem keamanan komputer berbasiskan NIDS (*Network Intrusion Detection System*), faktor ini harus dipertimbangkan. Catatan bahwa sistem deteksi dapat membelah paket dan menerapkan rules pada bagian paket yang berbeda. Bagian tersebut diantaranya :
   a) IP header paket
   b) *Header layer transp*ort. *Header* ini dapat berupa TCP, UDP atau *header layer transport* lainnya. Hal ini juga dapat bekerja pada header ICMP.
   c) *Header level layer* aplikasi. Header layer aplikasi termasuk header DNS, FTP, SNMP dan SMTP, namun tidak dibatasi hanya header ini saja.

d) *Packet payload*. Hal ini berarti dapat diciptakan rules yang digunakan oleh detection engine untuk mencari string di dalam data yang ada pada paket.

d. *Sistem Log* dan *Alert*

Berdasarkan apa yang ditemukan detection engine pada paket, paket dapat digunakan untuk me-log kegiatan atau mengaktifkan alert, bergantung pada apa yang ditemukan detection engine pada paket. Log di simpan pada format file teks sederhana, file berjenis tcpdump atau bentuk yang lain. File log disimpan di direktori /var/log/snort secara default.Perintah snort -l pada command line dapat digunakan untuk memodifikasi lokasi dari log dan alert yang dihasilkan.

e. Model Output

Modul Outputdapat melakukan beberapa operasi berbeda tergantung bagaimana cara penyimpanan keluaran yang dihasilkan sistem log dan alert dari Snort. Pada dasarnya modul ini mengatur jenis keluaran yang dihasilkan oleh sistem log dan alert. Berdasarkan konfigurasi, keluaran modul dapat melakukan hal-hal berikut:

1) Logging ke dalam file /var/log/snort/alerts atau file lainnya.
2) Mengirimkan traps SNMP
3) Mengirimkan pesan ke syslog
4) Logging ke dalam database seperti MySQL atau Oracle.
5) Menghasilkan output eXtensible Markup Language (XML)
6) Mengubah konfigurasi pada router atau firewall
7) Mengirimkan pesan Server Messager Block (SMB) kepada mesin berbasiskan Linux atau Windows

2. Supported Platforms

Snort didukung pada sejumlah *platform* perangkat keras dan system operasi. Saat ini Snort tersedia untuk system operasi berikut :

a. Linux
b. OpenBSD

c. FreeBSD
d. NetBSD
e. Solaris(both Sparc and i386)
f. HP-UX
g. AIX
h. IRIX
i. MacOS
j. Windows

3. Mode Kerja

Secara umum snort dapat dioperasikan dalam tiga buah modus, yaitu:

a. Sniffer mode

Modus ini digunakan untuk mengamati paket yang masuk ke dalam jaringan yang sedang diamati. Untuk menjalankan snort pada sniffer mode contoh perintahnya terdapat di bawah ini :

1) snort –v
2) snort –vd
3) snort –vde
4) snort -v -d -e Dengan menambahkan beberapa switch -v, -d, -e akan menghasilkan beberapa keluaran yang berbeda, yaitu :
   a) -v, untuk melihat header TCP/IP paket yang lewat.
   b) -d, untuk melihat isi paket.
   c) -e, untuk melihat header link layer paket seperti ethernet header

b. Packet logger mode

Packet logger mode berfungsi untuk mencatat semua paket yang lewat dijaringan yang kemudian akan dianalisa. Bahkan dapat menyimpan paket dalam disk. Sehingga perlu diinisialisasikan terlebih dahulu logging direktorinya pada file configurasi snort. Cara kerja :

1) Collecting

Cara kerja yang pertama dari packet sniffing adalah merubah interface yang digunakan menjadi"promicius mode", dan mulai

mengumpulkan atau mengelompokkan semua paket data yang lewat melalui jaringan dalam bentuk raw binary.

2) Conversion

Cara kedua adalah mengkonversi atau merubah data yang berbentuk binary kedalam data yang mudah dibaca atau mudah dipahami.

3) Analysis

Cara kerja ketiga adalah dimana betuk data tersebut diklasifikasikan kedalam blok-blok protocol berdasarkan sumber dari transmisi data tersebut baik berupa tcp,udp dan lain-lain.

4) Pengambilan Atau Pencurian Data

Cara kerja yang terakhir adalah setelah melakukan klasifikasi terhadap data-data yang telah dikirim maka hacker atau penyusup melakukan pencurian data.

c. Intrusion Detection Mode

Modus operasi snort yang paling rumit adalah sebagai pendeteksi penyusup (intrusion detection). Ciri khas modus kerja untuk pendeteksi penyusup adalah dengan menambahkan perintah ke snort untuk membaca file konfigurasi -c nama-file-konfigurasi. conf. Isi file konfigurasi, sebagian besar telah di atur secara baik dalam contoh snort. conf yang dibawa oleh source snort.

Beberapa perintah untuk mengaktifkan snort untuk melakukan pendeteksian penyusup di Linux dapat di atur dengan perintah -A sebagai berikut :

1) -A fast, mode alert yang cepat berisi waktu, berita, IP & port tujuan.
2) -A full, mode alert dengan informasi lengkap.
3) -A unsock, mode alert ke unix socket.
4) -A none, mematikan mode alert.

BAB III
ANALISA DAN PERANCANGAN SISTEM

A. Analisa dan Kebutuhan Sistem

Sebelum memasuki tahap perancangan program, tahap analisa dilakukan agar nantinya dalam merancang program tidak terjadi kesalahan. Tahap analisa ini berperan penting dalam sebuah sistem karena apabila pada tahap ini terjadi kesalahan maka tahap selanjutnya sudah dipastikan akan terjadi kesalahan.

Adapun kelemahan jaringan jika tidak menggunakan firewall diantaranya. Firewall tidak dapat membantu mencegah pencurian data ataupun peretasan yang dilakukan dari dalam. Pencurian data atau peretasan yang berlaku secara internal, atau dari dalam tidak dapat dicegah oleh firewall. Kebanyakan, tindakan kejahatan peretasan ini dilakukan karena komputer yang dituju memiliki pengamanan firewall yang lemah.

Hal ini terjadi apabila peretasan dan pencurian data dilakukan oleh mereka yang mengetahui password dan security key dari komputer tersebut. Perlu diingat, firewall hanya akan beraksi ketika mendeteksi adanya konten mencurigakan yang berusaha menyusup ke dalam komputer melalui jaringan internet.

Maka dari itu penulis mencoba membuat system keamanan jaringan dengan menggunakan snort yang diterapkan sebagai pengganti firewall yang dapat mendeteksi dan mencegah tindakan mencurigakan yang dapat merugikan para user yang terhubung kedalam jaringan internet.

Dalam hal ini sistem yang dibuat membutuhkan *hardware* (perangkat keras) sebagai *input* dan penghasil suatu tindakan, serta *software* (perangkat lunak) sebagai pengolah data dari masukan sehingga mampu menghasilkan suatu informasi yang bisa digunakan untuk memberikan suatu perintah eksekusi (tindakan). Kedua perangkat ini mempunyai peran yang sangat penting dalam menjalankan dan mengoperasikan suatu peralatan.

B. Perancangan Sistem Keamanan Jaringan

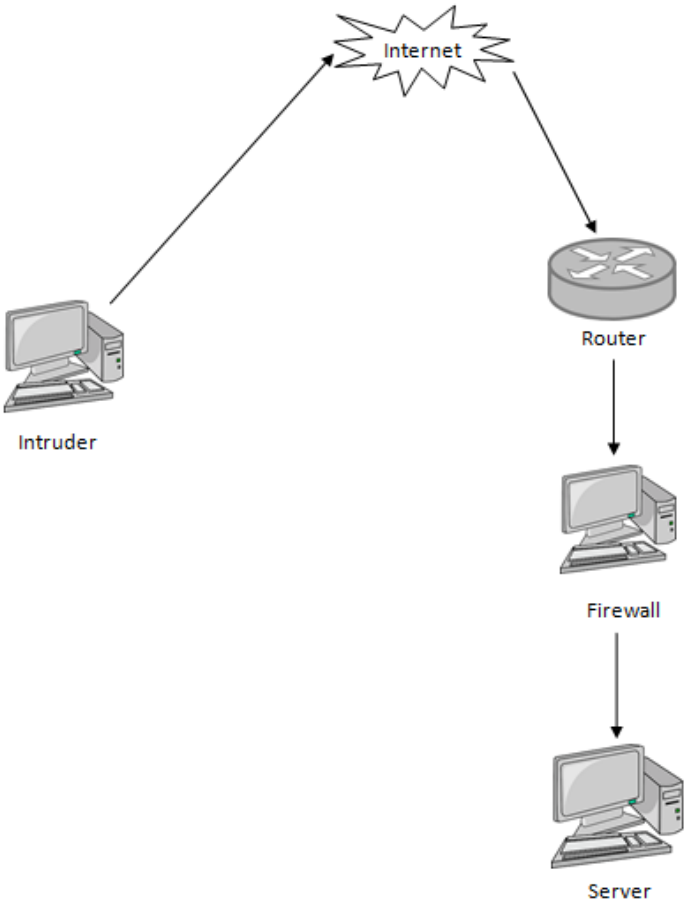
Perancangan sistem merupakan proses yang dilakukan terhadap keamanan jaringan, mulai dari perancangan system keamanan jaringan dan hardware maupun perangkat lunak hingga hasil jadi yang akan difungsikan. Pada prinsip perancangan dan sistematika yang baik akan memberikan kemudahan-kemudahan dalam proses pembuatan system keamanan. Dalam hal ini sistem yang akan di rancang adalah sebuah monitoring keamanan jaringan agar tindak kejahatan terhadap jaringan bisa diatasi sehingga tidak mengganggu pengguna jaringan lainnya.Agar tindak kejahatan terhadap jaringan bisa diketahui, maka monitoring kemanan ini di pasang sebagai firewall. Kejahatan terhadap jaringan yang di maksud adalah kejahatan yang bisa merugikan orang lain,seperti pencurian data,melakukan serangan terhadap jaringan yang memiliki dampak buruk terhadap rusaknya suatu system komputer atau rusaknya data pada database.

Prinsip kerja system keamanan ini adalah medeteksi serangan pada jaringan menggunakan snort berfungsi untuk mendeteksi adanya tindakkan yang mencurigakan menggunakan rules yang ada pada snort. Disini kita mengunakan snort sebagai pendeteksi serangan dan pencegahan terhadap serangan pada jaringan. Apabila ada yang mencoba melakukan tindak kejahatan terhadap jaringan maka snort akan mengetahui dengan sistem alert yang ada pada rule snort yang telah kita buat. Selanjutnya snort akan melakukan tindakan pemblokiran terhadap user yang mencoba melakukan tindakan kejahatan terhadap jaringan.

Tujuan dari perancangan sistem adalah untuk memenuhi kebutuhan pengguna (*user*) mengenai gambaran yang jelas tentang sistem yang akan dibuat. Selain itu perancangan sistem juga bermanfaat agar tidak terjadi kebingungan kepada pengguna yang ingin mengimplementasikan sistem yang akan dibuat sehingga bisa menghemat banyak sumber daya, baik sumber daya manusia, waktu, tenaga, pikiran, dan biaya.

1. Persiapan awal yang perlu dilakukan adalah sebagai berikut:
   a) 1 unit laptop yang akan dijadikan target
   b) 1 unit laptop untuk penyerang atau intruder
   c) 1 unit laptop untuk firewall
   d) 1 unit USB LAN CARD
   e) Aplikasi *Snort* yang dijadikan sebagai pendeteksi dan pencegahan serangan pada jaringan.
2. Skema simulasi jaringan

   Untuk lebih jelas mengenai skema simulasi sistem keamanan jaringan ini dapat dilihat pada gambar 3.1 yaitu skema keseluruhan yang meliputi laptop penyerang atau intruder,internet,router,firewall,server.



Gambar 3. 1 *Skema Simulasi Jaringan*

Untuk mendapatkan IP address dan subnetting yang akan digunakan,kita perlu mencarinya dengan cara menghitung jumlah subnet terdekat.

Angka terdekat 2^4 = 8, Jumlah maximum ip 256-8 = 248, Maka dapat lah subnetnya menjadi 255.255.255.248, Range ip yang dapat kita gunakan adalah 192.168.1.0 – 192.168.168.1.7, Dan jumlah host yang dapat kita gunakan adalah 6 host 192.168.1.1 – 192.168.1.6. Ip addres yang dapat digunakan sekarang dapat dilihat dalam tabel 3.1.

Tabel 3. 1 *IP Address*

Perangkat	*IP Address*	Length	Subnet Mask
PC Intruder	192.168.1.3	/29	255.255.255.248
PC Firewall	192.168.0.2	/29	255.255.255.248
USB Lan Card	192.168.1.1	/29	255.255.255.248
PC Target	192.168.0.4	/29	255.255.255.248

C. Penginstallan Aplikasi

Snort ialah sebuah sistem intrusi jaringan yang gratis dan *open source*, dapat digunakan untuk memeriksa lalulintas jaringan dengan menggunakan aturan dan tata bahasa. *Snort* dikelola oleh *Open Information Security Foundation* yang digunakan sebagai *intrusion detection system, intrusion prevention system* dan *network monitoring*. Berikut langkah penginstalan *snort*:

1. Update dan upgrade *Linux Ubuntu*

   Sebelum memulai *suricata* ada baiknya sistem dan perangkat lunak anda sudah dalam versi terbaru. Pertama, *login* ke *root* dan jalankan perintah berikut:

   #apt-get update –y

Perintah apt-get update –y digunakan untuk mengupdate repository pada linux ubuntu.

#apt-get upgrade –y

Perintah apt-get upgrade –y digunakan untuk mengupgrade paket pada linux ubuntu.

2. Installasi paket pendukung *snort*

Sebelum menginstall *snort* pastikan paket pendukung telah terinstall dengan memasukan perintah yang dapat menjalankan fungsi pendukung snort secara otomatis. Perintahnya sebagai berikut :

#sudo apt-get install build-essential –y

Secara *default*, *snort* bekerja sebagai *intrusion detection system*. Sehingga, harus ditambahkan beberapa installan paket agar dapat berfungsi sebagai *intrusion detection and prevention system.* Untuk menjalanan *snort* dalam mode *intrusion prevention system* maka perlu ditambahkan perintah berikut :

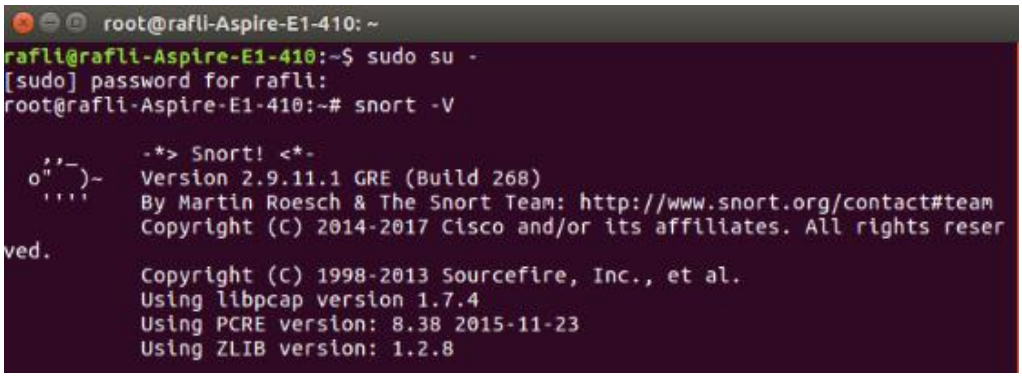
#bison flex

libpcap-dev libpcre3-dev libdumbnet-dev bison flex -y

3. Download Snort

Pada tugas akhir ini penulis menggunakan *snort* versi 2.0.6 maka penulis memasukan *coding* VER=<versi> untuk menentukan versi yang dipilih. Berikut langkah penginstallan *snort* versi 2.0.6 :

a. Download *snort* pada *website* resminya dengan perintah wget.
   #wget https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
b. Ekstrak file yang telah di *download* dengan dengan perintah tar.
   #tar -zxvf snort-2.9.8.2.tar.gz
c. Buka file *snort* yang telah diekstrak dengan perintah cd.
   #cd snort-2.9.8.2
d. Setelah berhasil diinstal maka untuk melihat versi snort yang sudah terinstal bisa kita lihat dengan perintah snort –V



Gambar 3. 2 *Versi snort*

4. *Configure enable source*

   Untuk mengatur agar penginstalasi snort dilakukan dengan membaca kode sumber pada pemasangan *snort* dengan perintah:

   #./configure --enable-sourcefire

   Setelah selesai melakukan *compile snort* dengan perintah di atas penulis menginstall *snort* dengan perintah :

   $make

   Perintah make digunakan untuk membangun sebuah program

   $sudo make install

   Perintah sudo make instal digunakan untuk menginstal program yang ada pada respository kita.

5. Configurasi Snort

   a. Configuring snort

      Pada tahap configurasi snort ini kita menggunakan perintah pada terminal linux dengan perintah sudo /etc/snort.conf masukkan ip yang akan kita lindungi

      #Ipvar HOME_NET 192.168.1.0/29

   b. Pembuatan Rules Ping

      Setelah melakukan configurasi Ip yang akan dilindungi,langkah selanjutnya melakukan pembuatan rules sebagai bentuk pendeteksi adanya percobaan ping dengan melakukan perintah pada terminal linux

      #sudo gedit /etc/snort/sid-msg.map

1 || 10000001 || 001 || icmp-event || 0 || Ada percobaan Ping || url,tools.ietf.org/html/rfc792

c. Pembuatan Rules DdoS

Selanjutnya membuat rules DDoS sebagai bentuk pendeteksi adanya serangan berupa DDoS yang mencoba menyerang server,kita dapat melakukan pembuatan rules dengan perintah pada terminal linux

gedit /etc/snort/rules/local.rules

alert icmp any any -> $HOME_NET any (msg:"ada yang mencoba melakukan DDoS"; GID:1; sid:10000001; rev:001; classtype:icmp-event;)

6. Penginstalan Bernyard2 dan Mysql Database

Setelah melakukan penginstalan snort dan melakukan configurasi pada snort,selanjutnya kita melakukan penginstalan aplikasi yang dapat membantu snort dalam melakukan kinerjanya sebagai pelaporan detection. Adapun langkah yang kita jalankan untuk melakukan penginstalan Bernyard2 ini adalah melakukan penginstalan pendukung bernyard2 terlebih dahulu agar bernyard2 dapat berfungsi dengan baik.

Berikut aplikasi pendukung bernyard2 yang perlu kita instalkan terlebih dahulu :

sudo apt-get install mysql-server libmysqlclient-dev mysql-client autoconf libtool –y

Setelah melakukan penginstalan paket pendukung bernyard2, selanjutnya kita mengubah file ouput pada bernyard2 dengan perintah :

sudo gedit /etc/snort/snort.conf

Selanjutnya kita melakukan pengubahan outputnya

output unified2: filename merged.log, limit 128, nostamp, mpls_event_types, vlan_event_types

Menjadi

output unified2: filename snort.u2, limit 128

a. Penginstalan Bernyard

Setelah melewati beberapa tahap diatas,maka selanjutnya kita melakukan penginstalan bernyard2 dengan perintah :

cd ~/snort_src/

git clone git://github.com/firnsy/barnyard2.git

Setelah melakukan pengunduhan bernyard2 dari situs resminya,selanjutnya kita membuka file bernyard yang kita download tadi dengan perintah :

cd barnyard2/

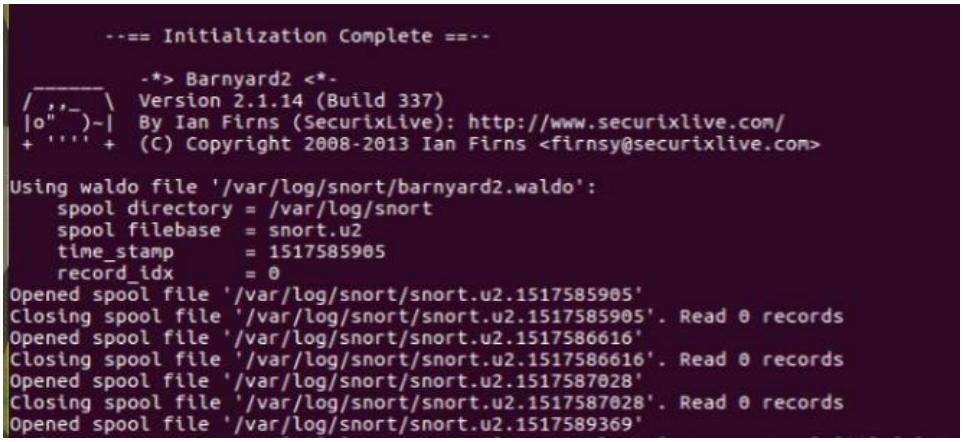
Untuk memperbarui file konfigurasi pada file bernyard2 dapat dijalankan dengan perintah :

autoreconf -fvi -I ./m4

Selanjutnya kita akan melakukan penginstalan bernyard2 dengan perintah

make instal

Setelah berhasil melakukan penginstalan bernyard dapat dilihat pada gambar 3.3 dibawah ini.



Gambar 3. 3 ***Penginstalan Bernyard***

b. Pembuatan Mysql Database

Setelah melakukan penginstalan bernyard2 maka selanjutnya kita melakukan pembuatan mysql yang dapat membantu dalam kinerja pendeteksian snort dan bernyard. Kita dapat melakukan pembuatan mysql database dengan cara melakukan perintah pada terminal linux, dengan perintah :

mysql -u root –p

Selanjutnya membuat database pada snort dengan perintah:

mysql> create database snort;

Selanjutnya kita menggunakan mysqlnya terhadap snort sekaligus memasangnya pada bernyard2 yang berfunsi untuk membaca skema tabel barnyard dan membuatnya di mysql dengan menggunakan perintah :

mysql> use snort

mysql> source ~/snort_src/barnyard2/schemas/create_mysql

Selanjunya melakukan pembuatan User sekaligus melakukan konfigurasi pada mysql databasenya dengan perintah :

mysql> CREATE USER 'snort'@'localhost'IDENTIFIED BY '**********';

mysql> grant create, insert, select, delete, update on snort.* to 'snort'@'localhost';

c. Configurasi Barnyard2 Terhadap Mysql Database

Tahapan selanjutnya melakukan configurasi Barnyard2 untuk memakai mysql database sehingga dapat membantu barnyard2 dalam melakukan proses kinerjanya dalam pendeteksian terhadap adanya serangan pada jaringan, adapun perintah untuk configurasi barnyard2 terhadap mysql database dapat dilakukan dengan perintah :

sudo gedit /etc/snort/barnyard2.conf

Selanjutnya membuat password pada mysqlnya, password disini yang kita buat adalah “root” sekaligus melakukan akses terhadap mysql database.

output database: log, mysql, user=snort password=**** dbname=snort host=localhost

sudo chmod o-r /etc/snort/barnyard2.conf

Setelah selesai melakukan configurasi barnyard2 terhadap mysql database, tahap selanjutnya yaitu melakukan pengujian simulasi.

D. Pengujian Dan Hasil

1. Pengujian

   Dari hasil perancangan ini setelah melakukan penginstalan dan konfigurasi server, maka langkah selanjutnya menampilkan hasil dan cara pengujian dari aplikasi *snort*. Dengan menggunakan sistem operasi *Linux Ubuntu* sebagai server, laptop sebagai target dan 1 laptop sebagai penyusup, serta kabel *cross* sebagai media penghubung antara laptop target ke laptop firewall dan 1 kabel *cross* lagi sebagai penghubung antara laptop penyusup ke laptop firewall dengan melalui perantara *USB LAN Card*.

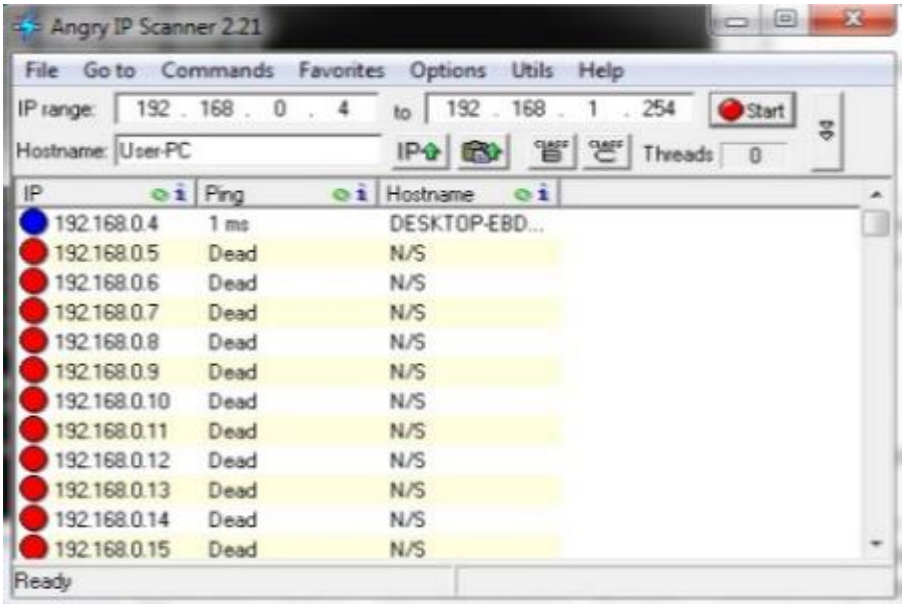
   Adapun langkah-langkah yang dilakukan antara lain:

   a. Penyusup atau intruder menghubungkan komputer atau laptopnya ke jaringan internet.
   b. Setelah penyusup atau intruder berhasil menghubungkan komputer atau laptopnya ke internet, selanjutnya penyusup atau intruder melakukan port scanning pada jaringan yang telah dimasuki untuk mendapatkan ip address server.
   c. Setelah ip address server didapatkan. Maka penyusup atau intruder bisa melakukan penyerangan terhadap server.
   d. Selanjutnya firewall akan mendeteksi adanya kegiatan yang mencurigakan seperti port scanning dan membuat pelaporan adanya penyusup yang mencoba melakukan serangan pada jaringan.
   e. Setelah itu firewall akan melakukan pencegahan terhadap serangan pada jaringan.

2. Hasil

   a. Scanner IP address

      Sebelum melakukan percobaan simulasi penyerangan terhadap jaringan,awalnya kita melakukan scanning terhadap jaringan untuk mendapat ip target yang akan kita jadikan untuk pengujian simulasi serangan terhadap jaringan.

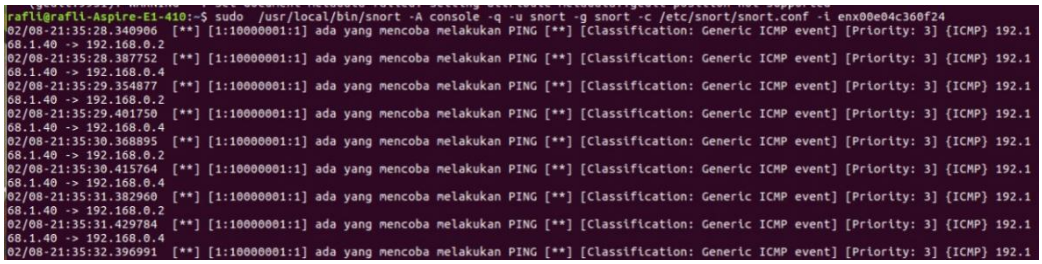


Gambar 3. 4 *IP Scan*

Setelah melakukan scanning dengan angry IP scanner,kita berhasil mendapat satu IP yang lagi terkoneksi kejaringan internet dengan ip 192.168.0.4. Langkah selanjutnya adalah melakukan penyerangan terhadap ip target yang kita dapatkan tadi dengan melalui Ip Scan.

b. Percobaan dengan *ping*

Dalam percobaan ini penyerang dengan ip address 192.168.1.3 mencoba menyusup dan melakukan pingflood terhadap server dengan ip 192.168.0.2 melalui sebuah jalur dengan menggunakan *USB LAN Card* dengan ip 192.168.1.1 dan berhasil dideteksi oleh snort.



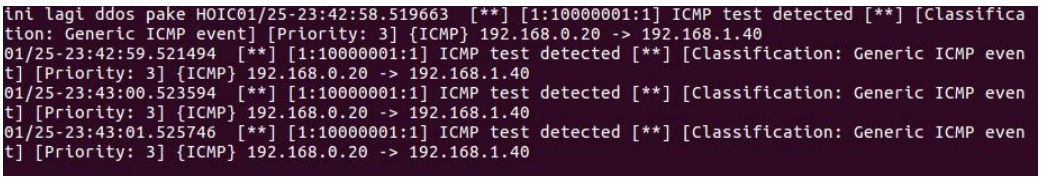
Gambar 3. 5 *perbobaan Ping*

c. Percobaan Dengan menggunakan DdoS Attack

Untuk melakukan serangan ini, penyerang menggunakan comand prom, kemudian melakukan ping ke IP server dengan mengirim paket yang ukurannya besar. Serangan *DDoS attacks* ini dilakukan dengan cara

mengirim paket ICMP yang berlebih secara berturut-turut terhadap server. Tujuan penyerangan ini membuat sistem menjadi *crash* dan *hang*. Teknis penyerangan ini adalah ketikkan pada terminal: ping -f -s <size> <host>. Proses penyerangan tersebut penulis uraikan sebagai berikut :

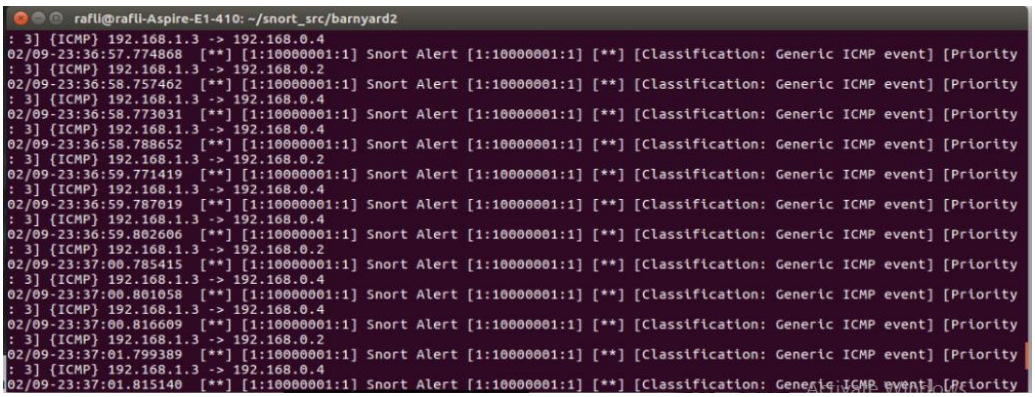
1) Penyerang dengan IP 192.168.1.3 melakukan serangan terhadap laptop target dengan IP 192.168.0.4 berhasil dideteksi oleh snort.



Gambar 3. 6 *serangan DDoS*

2) Melihat Alert Dengan Barnyard2

Setelah melakukan penyerangan dan dideteksi oleh snort maka selanjutnya barnyard2 sebagai pendukung snort juga berhasil melakukan pendeteksian dengan system alertnya.

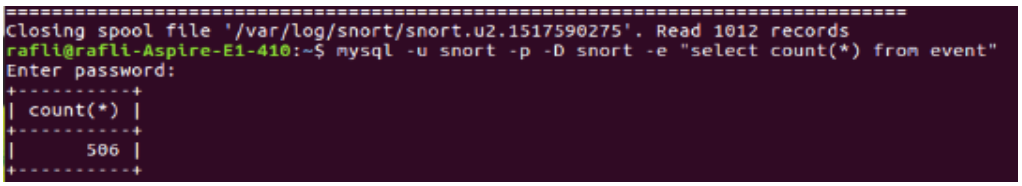


Gambar 3. 7 *Snort Alert*

3) Perhitungan serangan dengan mysql

Selanjutnya dengan untuk melihat berapa jumlah percobaan ping pada server kita melihatnya pada perhitungan di mysql pada snort dengan perintah :

#mysql –u snort –p –D snort –e “select from (*) from event”

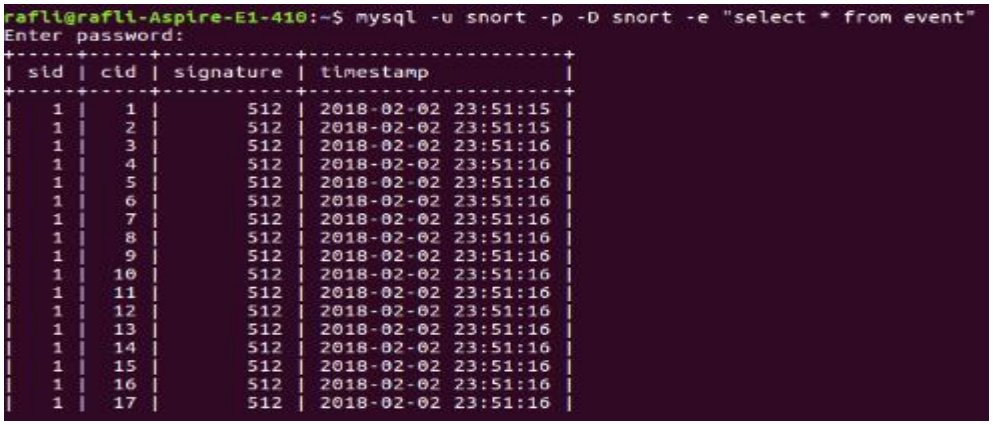


Gambar 3. 8 ***Jumlah Baris ditable serangan***

4) Statistik

Untuk melihat paket data yang masuk dari hasil percobaan penyerang melakukan serangannya terhadap server dapat kita lihat dengan menggunakan perintah pada terminal linux ubuntu

mysql –u snort –p –D snort –e "select from * from event"



Gambar 3. 9 ***Table statistic penyerang***

Setelah berhasil mendeteksi adanya serangan terhadap jaringan,maka langkah selanjutnya adalah memblokir ip penyerang yang ipnya 192.168.1.3 agar tidak bisa lagi melakukan tindak kejahatan yang dapat merugikan orang lain,adapun perintah yang dapat kita gunakan untuk memblokir ip penyerang itu adalah :

#iptables –A INPUT –s 192.168.1.3 –j DROP

BAB IV
PENUTUP

A. Kesimpulan

Bab ini merupakan bab yang terakhir daripenulisan Tugas Akhir ini, yang mana pada bab ini berisikan kesimpulan dan saran-saran untuk dilakukan perbaikan-perbaikan yang dianggap perlu pada sistem yang ada pada saat ini. Penulis menyadari bahwa sistem yang diusulkan ini masih ada kelemahan-kelemahan dan kekurangan.

Dari uraian masalah yang telah dikemukakan diatas, serta berdasarkan analisa dari data yang ada maka dapat ditarik kesimpulan sebagai berikut:

1. Snort sebagai IDS dapat berfungsi dengan baik dalam melakukan pendeteksiandan memonitor adanya perilaku atau tindakan kejahatan dalam jaringan yang dapat merugikan banyak orang.
2. Snort sangat baik dalam membuat adanya pelaporan terhadap para user lain yang mencoba untuk menyusup dalam komputer kita sehingga kita dapat mengetahui dan membuat tindakan selanjutnya seperti memblock user yang mencoba menyusup pada laptop atau komputer kita

B. Saran

Dari hasil penelitian dan analisa yang ada,saya menginginkan untuk kedepannya system keamanan jaringan yang sudah ada dapat ditingkatkan lagi demi keselamatan dan menjaga kerahasiaan data yang ada pada komputer kita.

DAFTAR PUSTAKA

Akbar Ali. (2006). Panduan Mudah Linux. Semarang : Informatika Bandung.

Gondohanindijo, Jutono. 2012. *Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System),* Fakultas Ilmu Komputer Universitas AKI.

Harjono Edy Budy. 2016. *Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Dengan Metode LSF Dan REMASTER*. Jurnal & Penelitian Teknik Informatika, 1 (1) : 30 – 35.

http://www.junalkomputer.com/pengenalan-jaringan-komputer.pdf (12 juli 2003)

Iswahyudi, Catur dkk. 2014. *Implementasi IDS Menggunakan Jejaring Sosial sebagai Media Notifikasi, Makalah, Jurusan Teknik Informatika, FTI, IST AKPRIND.*

Nur, Muhammad. 2011. *Snort Intrusion Detection System (IDS) Untuk Keamanan Jaringan, Skripsi, Fakultas Pendidikan dan Ilmu Pengetahuan Alam (FPMIPA) Universitas Pendidikan Indonesia*.

Rafiudin Rahmat. 2010. *Mengganyang Hacker dengan SNORT*. Yogyakarta: Andi.

Wahana Komputer. 2013. *Ubuntu 12 untuk Small Office Home Office*. Semarang: Andi.

Wijanarko, D. 2015. *SISTEM KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SNORT*. Jurnal Teknologi Informasi dan Terapan, 2 (1) : 171 – 176.

KEMENTERIAN AGAMA
INSTITUT AGAMA ISLAM NEGERI BATUSANGKAR
PROGRAM DIII MANAJEMEN INFORMATIKA

Jl. Sudirman No. 137 Kubu Rajo Lima Kaum Batusangkar 27213 Telp. (0752) 71150, 574221, Fax. (0752) 71879
http://www.stainbatusangkar.ac.id e-mail: mi@stainbatusangkar.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

KARTU BIMBINGAN PENULISAN TUGAS AKHIR

NIM : 14 205 087
Nama : Rafli Razak
Jurusan : D.III Manajemen Informatika
Dosen Pembimbing : Zikrawahyu, M.Kom
Judul Tugas Akhir : Pendeteksian Dan Pencegahan Serangan Pada Jaringan Menggunakan Snort Pada Linux Ubuntu

NO	Hari/Tanggal	Materi Bimbingan	Paraf
	Kamis 4-12-2017	perbaiki BAB I, II, tambahkan sequence;	
		perbaiki struktur penulisan.	
	Jumat 7/12-2017	tambahkan teori/literatur Hy	
		linux/ubuntu pada BAB II, snort	
	Rabu 10-01-2018	perbaiki skema penyerangan,	
		IP address dan subnetting yg	
	Selasa 30-01-2018	belum di gunakan.	
	11/1-2018	perbaiki perbaiki lagi. Analisa	
	Senin 5-02-2018	kebutuhan, gambarkan skema penyerangan	
		kompleksnya jangan.	
	2/2-2018	test simulasi	

Catatan : Setiap konsultasi dengan dosen pembimbing kartu ini harap dibawa, diisi, dan diparaf oleh dosen pembimbing

Batusangkar, _____
Mahasiswa

Rafli Razak
NIM. 14 205 087

Dosen Pembimbing Tugas Akhir

Zikrawahyu, M.Kom
NIP.19740507 200501 1 006

Mengetahui,
Dosen Penasehat Akademik

Gampito, S.E., M.Si
NIP.19670219 200501 1 005