ANALISA KEAMANAN JARINGAN LAN MENGGUNAKAN SNORT DENGAN METODE *PENETRATION TEST* DI LABOR TEKNIK INFORMATIKA UNIVERSITAS ISLAM RIAU

Skripsi

Diajukan Untuk Memenuhi Salah Satu Syarat Untuk Memperoleh
Gelar Sarjana Teknik Pada Fakultas Teknik
Universitas Islam Riau Pekanbaru

DISUSUN OLEH:

IRFAN SUPRATMAN
173510066

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS ISLAM RIAU
PEKANBARU
2021

LEMBAR PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

Nama : Irfan Supratman

Tempat/Tgl Lahir : Pekanbaru, 10 Juni 1999

Alamat : Komp Wadya Graha 1 Blok K No.24

Adalah mahasiswa Universitas Islam Riau yang terdaftar pada:

Fakultas : Teknik

Jurusan : Teknik Informatika

Program Studi : Teknik Informatika

Jenjang Pendidikan : Strata-1 (S1)

Dengan ini menyatakan dengan sesungguhnya bahwa skripsi yang saya tulis adalah benar dan asli hasil dari penelitian yang telah saya lakukan dengan judul **"ANALISA KEAMANAN JARINGAN LAN MENGGUNAKAN SNORT DENGAN METODE PENETRATION TEST DI LABOR TEKNIK INFORMATIKA UNIVERSITAS ISLAM RIAU"**

Apabila dikemudian hari ada yang merasa dirugikan dan atau menuntut karena penelitian ini menggunakan sebagian hasil tulisan atau karya orang lain tanpa mencantumkan nama penulis yang bersangkutan, atau terbukti karya ilmiah ini **bukan** karya saya sendiri atau **plagiat** hasil karya orang lain, maka saya bersedia menerima sanksi sesuai dengan peraturan perundangan yang berlaku.

Demikian surat pernyataan ini saya buat dengan sesungguhnya untuk dapat digunakan sebagaimana mestinya.

Pekanbaru, 15 November 2021

Yang membuat pernyataan,

Irfan Supratman

KATA PENGANTAR

Puji syukur kehadirat Allah SWT. Karena atas limpahan Karunia, Rahmat, dan Hidayah-Nya yang berupa kesehatan, sehingga Skripsi yang berjudul "Analisa Kemanan Jaringan LAN menggunakan Snort Dengan Metode *Penetration Test* Di Labor Teknik Informatika Universitas Islam Riau" dapat terselesaikan tepat pada waktunya.

Skripsi ini disusun untuk memenuhi salah satu syarat memperoleh gelar sarjana pada Fakultas Teknik Universitas Islam Riau Pekanbaru. Dalam penyusunan skripsi ini, penulis sadar bahwa tanpa bantuan dan bimbingan berbagai pihak lain maka skripsi ini sulit untuk terwujud. Untuk itu dalam kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada yang terhormat :

1. Bapak Dr. Eng. Muslim, M.T selaku Dekan Fakultas Teknik.
2. Bapak Dr. Apri Siswanto, S.Kom., M.Kom selaku ketua program studi Teknik informatika universitas islam riau dan selaku dosen pembimbing yang telah sabar dan ikhlas dalam melakukan bimbingan.
3. Bapak Yudi Arta, S.T., M.Kom selaku dosen penguji pertama yang telah memberikan ilmu dan saran yang bermanfaat dalam penelitian ini.

4. Bapak Rizdqi Akbar Ramadhan, S.Kom., M.Kom., CHFI selaku dosen penguji kedua yang telah memberikan ilmu yang sangat bermanfaat terkait dalam penelitian ini.
5. Seluruh dosen yang berada di prodi teknik informatika yang telah mendidik dan memberikan ilmu serta arahan.
6. Selanjutnya kepada kedua orang tua ayah (Alm) H. Drs. Darusman Ar, M.Pd dan ibu Hj. Arli berti, S.Pd yang telah memberikan semangat dan dukungan serta motivasi sehingga penulis dapat menyelesaikan penelitian ini tepat pada waktunya.
7. Kepada Marini Rehanisafira, S.Pd. selaku orang yang selalu memotivasi sampai pada saat sekarang ini.

Semoga skripsi ini bisa memberikan informasi mengenai perlunya pengawasan terhadap serangan jaringan dan semoga bermanfaat bagi para pembacanya. Atas perhatian dan kesempatan yang diberikan untuk membuat skripsi ini penulis ucapkan terima kasih.

12 November 2021

Penulis

Irfan Supratman

Analisa Keamanan Jaringan Lan Menggunakan Snort Dengan Metode Penetration Test Di Labor Teknik Informatika Universitas Islam Riau

Irfan Supratman
Fakultas Teknik
Program Studi Teknik Informatika
Universitas Islam Riau
Email : irfansupratman@student.uir.ac.id

ABSTRAK

Pada saat sekarang ini banyaknya kejahatan didalam dunia internet yang menyebabkan harus adanya pengawasan serta pendeteksian keamanan jaringan supaya dapat diantisipasi dengan cepat. Tujuan dari penelitian ini memberikan analisa terhadap pendeteksian adanya serangan jaringan yang berada di jaringan LAN labor Teknik informatika universitas islam riau. Sehingga diperlukannya pendeteksi seperti aplikasi snort yang dapat mendeteksi adanya sebuah serangan jaringan. Dalam penelitian ini menggunakan metode *penetration test* yang dimana metode ini merupakan metode yang bertujuan untuk melakukan pengujian terhadap sistem atau keamanan jaringan secara langsung yang berada di labor Teknik informatika universitas islam riau. Dalam penelitian ini penggunaan snort dapat berjalan dengan baik, karena snort dapat mendeteksi dan mengirimkan peringatan kepada administrator labor melalui aplikasi media sosial telegram dan setiap serangan jaringan yang terjadi didalam jaringan LAN snort berhasil mendeteksi semuanya sesuai dengan *rules* yang telah dibuat.

Kata kunci : Keamanan Jaringan, Snort, Penetration Test, Jaringan LAN

Analysis Lan Network Security Using Snort With Penetration Test Method at Labor Informatics Engineering University Islamic Riau

Irfan Supratman
Fakultas Teknik
Program Studi Teknik Informatika
Universitas Islam Riau
Email : irfansupratman@student.uir.ac.id

ABSTRACT

At this time the many crimes in the internet world that cause the supervision and detection of network security so that it can be anticipated quickly. The purpose of this study provides an analysis of the detection of network attacks located in the LAN labor network informatics engineering of riau Islamic university. So that the need for detection such as snort applications that can detect the presence of a network attack. In this study using penetration test method which is a method that aims to test the system or network security directly located in the informatics engineering labor of riau Islamic university. In this study the use of snort can run well, because snort can detect and send alerts to labor administrators through the social media application telegram and every network attack that occurs in the network LAN snort managed to detect everything in accordance with the rules that have been made.

Keywords: Network Security, Snort, Penetration Test, LAN Network

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada zaman sekarang ini internet menjadi salah satu bagian terpenting dalam kehidupan dan gaya hidup masyarakat di seluruh dunia. Karena internet telah berada kedalam segala aspek kehidupan mulai dari hiburan, lingkungan pendidikan, penunjang pekerjaan dan lain-lain. Sehingga setiap tahun nya berdasar kan data yang diperoleh dari situs APJII (Asosiasi Penyelenggara Jasa Internet Indonesia) penggunaan internet di wilayah sumatera khusus nya didaerah riau pada tahun 2018 dengan angka 3,5 juta mengalami peningkatan ke tahun 2019-2020 dengan angka sebesar 4,4 juta (APJII, 2019).

Sehingga dengan bertambah nya penggunaan internet maka bertambah pula tingkat kejahatan di internet tersebut. Berdasarkan survey yang dilakukan oleh aplikasi keamanan komputer yaitu Norton, yang di unggah pada website resminya, disebutkan bahwa dalam setahun terakhir lebih dari 978 juta orang dewasa di 20 negara cybercrime global yang berpengalaman, salah satunya Indonesia dengan total 59,45 juta orang dewasa yang menjadi pelaku *cybercrime*. Dan untuk kerugiannya sangat besar seperti yang disebutkan juga oleh Norton, total kerugian konsumen yang menjadi korban *cybercrime* secara global, Indonesia mencapai nilai yang sangat fantastis yaitu $ 3.2 miliar (*Symantec Corporation*, 2017). Sehingga kejahatan internet meliputi dari berbagai aspek mulai dari aspek Pendidikan, aspek keuangan dan lain-lainnya Dengan begitu keamanan jaringan internet sangat penting untuk dijaga validitas dan integritas data serta menjamin ketersediaan

layanan bagi penggunanya supaya data atau sistem jaringan internet tidak diganggu atau dirusak oleh penyusup.. Adapun serangan yang paling sering digunakan adalah *Port Scanning* dan DDOS (*Distributed Denial Of Service*). *Port scanning* merupakan serangan yang bekerja untuk mencari port yang terbuka pada suatu jaringan komputer sehingga hasil dari *port scanning* merupakan kelemahan dari sistem jaringan ckomputer tersebut. Sedangkan DDOS (*Distributed Denial Of Service)* merupakan serangan yang mengirim request ke server secara berulang dengan tujuan membuat server menjadi sibuk sehingga server akan mengalami kerusakan. (Kundan Kumar,2010).

IDS (Intrusion Detection Sistem) adalah sebuat aplikasi perangkat lunak yang mendeteksi aktivitas atau lalu lintas yang tidak wajar dalam sebuah sistem atau jaringan. Snort IDS merupakan IDS yang bersifat *Open Source* yang menjadi standar IDS di industri. Sehingga Snort merupakan suatu sistem yang mendeteksi secara *real time* terhadap adanya serangan jaringan dengan hasil alert dari serangan jaringan tersebut. (Kerry J & Christopher, 2004).

Perguruan tinggi terutama kampus Universitas islam riau merupakan suatu perguruan tinggi yang berdiri pada tanggal 4 September 1962 yang terletak di jalan Kaharudin Nasution No 113, Pekanbaru, Riau. Universitas islam riau memiliki banyak data-data penting sehingga diperlukan keamanan data yang sangat penting untuk dijaga. Karena di kampus universitas islam riau memiliki sangat banyak data-data penting meliputi data mahasiswa, data dosen, data keuangan dan lain-lain nya. Serta perlu nya pengawasan disetiap server yang ada disetiap fakultas di universitas

supaya tidak terjadi kebocoran data atau pun pemasukan paksa serta pengerusakan yang dilakukan oleh orang yang tidak bertanggung jawab.

Sehingga tujuan dari penelitian ini adalah untuk mengetahui kerentanan keamanan jaringan internet khususnya untuk jaringan LAN di labor Teknik informatika Universitas Islam Riau supaya bisa dengan cepat dideteksi dan diantisipasi dari bahaya nya ada nya serangan jaringan. Sesuai dengan penjelasan yang telah dijabarkan, penulis melakukan penelitian terhadap subjek yang dimana untuk mengidentifikasi dan mendeteksi keamanan jaringan dengan menggunakan SNORT dengan metode *penetration test*. Sehingga penulis melakukan penelitian yang berjudul "Analisa Keamanan Jaringan LAN Menggunakan SNORT dengan Metode *Penetration Test* Di Labor Teknik Informatika Universitas Islam Riau."

1.2 Identifikasi Masalah

Adapun identifikasi masalah yang dapat diambil dari penjelasan latar belakang tersebut "Universitas Islam Riau merupakan suatu intansi Pendidikan yang perlu nya ada nya pengawasan terhadap data-data penting dan oleh sebab itu diperlukan juga pengawasan secara berkala di labor teknik informatika universitas islam riau dari adanya bahaya serangan jaringan yang dilakukan oleh orang yang tidak bertanggung jawab".

1.3 Rumusan Masalah

Berdasarkan latar belakang masalah dan hubungan dengan pemilihan judul, penulis merumuskan pokok permasalahan yaitu

1. Mengidentifikasi adanya serangan jaringan LAN di labor Teknik informatika Universitas Islam Riau.

2. Melakukan Simulasi penyerangan untuk mengetahui kerentanan keamanan jaringan di labor Teknik informatika Universitas Islam Riau.

1.4 Batasan Masalah

Dalam pembuatan skripsi penulis membatasi masalah yang akan dilaksanakan yaitu :

1. Pengunaan aplikasi snort dalam mendeteksi adanya serangan jaringan internet
2. Penggunaan metode *penetration test* sebagai simulasi serangan terhadap jaringan.
3. *Output* dalam penelitian ini hanya berupa data serangan jaringan yang didapati dari analisis snort.
4. *Alert/*peringatan dari pendeteksian snort akan dikirimkan melalui aplikasi telegram administrator.
5. Dalam penelitian ini snort hanya berkerja sebagai pendeteksian keamanan monitoring jaringan dan berkerja secara umum.
6. Aplikasi telegram hanya sebagai pendeteksian dari serangan keamanan jaringan dan tidak sebagai remote dalam pendeteksiannya.
7. Dalam skripsi penulis tidak melakukan implementasi peningkatan keamanan jaringan yang sudah ada, tetapi hanya memberikan solusi dan mengantisipasi terhadap adanya serangan jaringan yang dilakukan oleh orang yang tidak bertanggung jawab.

8. Untuk penelitian dilaksanakan percobaan beberapa hari di labor Teknik informatika Universitas Islam Riau untuk memahami alur dan konsep yang sedang berjalan.

1.5 Tujuan Penelitian

Tujuan penelitian yang hendak dicapai meliputi :

1. Mengetahui dan mendeteksi adanya serangan jaringan LAN yang menyerang jaringan yang terhubung ke server di labor Teknik informatika Universitas Islam Riau.
2. Menganalisis serangan jaringan LAN dengan menggunakan aplikasi snort.
3. Jaringan LAN dapat diperhatikan atau lebih diawasi terhadap adanya serangan jaringan yang dilakukan oleh orang yang tidak bertanggung jawab.

1.6 Manfaat Penelitian

Manfaat penelitian yang di dapati dari hasil peneliti meliputi :

1. Memberikan solusi terbaik terhadap keamanan jaringan disekitar labor Teknik informatika di Universitas Islam Riau.
2. Membantu pihak IT untuk mengawasi keamanan jaringan dan server dari bahaya nya serangan jaringan.
3. Untuk mengetahui bahaya nya serangan jaringan tanpa adanya pengamanan serta perlu dilakukan pengawasan secara berkala terhadap keamanan jaringan itu sendiri.

BAB II
LANDASAN TEORI

2.1 Tinjauan Pustaka

Tinjauan Pustaka pertama berdasarkan penelitian yang berjudul "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan Dan Komputer (Barany Fachri, Fadli Hamdi Harahap, 2020)." menjadi dasar penelitian ini. Hasil dari penelitian yang telah dilakukan penulis menyimpulkan bahwa serangan atau penyusupan yang digunakan untuk simulasi pada penelitian ini dapat dicegah dengan menerapkan Intrusion Detection System (IDS). Serangan terdeteksi dengan cara selalu melakukan pembaharuan dari filter rules IDS.

Penelitian yang dilakukan oleh Arta, Syukur, & Kharisma, (2018) yang berjudul "Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik" yang dilakukan di Universitas Islam Riau. Penulis menyimpulkan bahwa penerapan Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) memiliki keterkaitan dalam hal mendeteksi sebuah serangan jaringan. Sehingga IPS bertindak sebagai *firewall* yang melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara mendetail.

Dalam penilitian Syaimi, Utami, Lidyawati, & Ramadhan (2013) yang berjudul "Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd" mengartikan pada dasarnya *vunaribility* yang ada pada system keamanan di dalam jaringan bisa digunakan oleh penyusup (intruder) untuk melaksanakan serangan memakai metode pencurian data secara masal dan metode perusakan jaringan yang

terhubung ke komputer. Sehingga penelitian ini memiliki arah untuk mendapatkan langkah terbaik untuk melakukan tindakan pencegahan terjadinya serangan serta untuk mengetahui adanya sebuah serangan yang dilakukan penyusup dengan memakai beberapa aplikasi atau perangkat lunak yaitu Snort IDS dan Honeyd. Dengan begitu cara kerja Snort IDS yaitu sebagai pendeteksi serangan jika adanya sebuah serangan yang akan dating ataupun yang telah dilaksanakan oleh intruder. Sehingga setelah penyerangan yang dilaksanaka berhasil dideteksi oleh Snort IDS, maka tindak pencegahan selanjutnya akan mengarahkan kesebuah membelokkannya ke server palsu (Honeyd). Akibatnya yang mungkin terjadi dari serangan tersebut adalah gangguan pada sistem server. Selain itu akan terjadi juga peningkatan kinerja server hingga 94,1%. Namun setelah dilakukan pembelokkan serangan ke server palsu, kinerja server relatif menurun menjadi 47,4%. Berikut ini merupakan tabel persamaan dan perbedaan dari penelitian sebelumnya.

Tabel 2.1 Persamaan dan Perbedaan Penelitian terkait

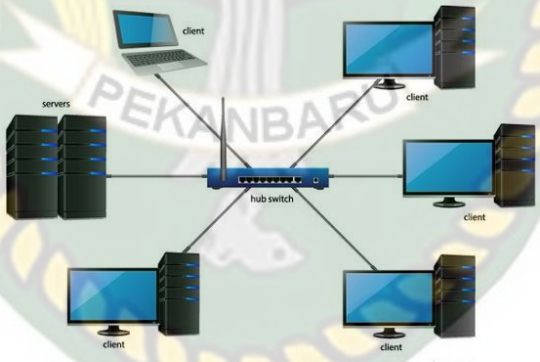
Nama penulis,tahun dan judul	**Hasil penelitian**	**Persamaan**	**Perbedaan**	
			Penelitian terdahulu	**Rencana penelitian**
Barany Fachri, Fadli Hamdi Harahap (2020), tentang Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan Dan Komputer	Penelitian tentang Intrusion Detection System (IDS) sebagai keamanan jaringan komputer sangat tepat untuk mendeteksi sebuah	Penerapan Intrusion Detection System (IDS) dalam mendeteksi serangan yang terjadi	Intrusion Detection System (IDS) menggunakan SNORT sebagai pendeteksi paket-paket dari sebuah jaringan internet selama jaringan	Analisa Keamanan Jaringan LAN Menggunakan SNORT dengan Metode *Penetration Test* Di Labor Teknik Informatika Universitas Islam Riau.

	serangan atau penyalahgunaan pada sebuah jaringan komputer		internet terhubung dengan server	
Arta.Y, syukur, charisma (2017), tentang Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik di Universitas Islam Riau	Penelitian ini membahas tentang implementasi Intrusion Prevention System (IPS) pada router yang menunjukan bahwa setiap serangan tergantung pada pola penyerangan yang ada didalam ruleIPS. Log mikrotik berkerja dengan maksimal mendeteksi serangan yang terjadi	Penerapan Intrusion Prevention System (IPS) dalam mendeteksi serangan yang terjadi	Intrusion Prevention System (IPS) menggunakan SNORT dengan melakukan penyerangan melalui *bruteforce.*	Analisa Keamanan Jaringan LAN Menggunakan SNORT dengan Metode *Penetration Test* Di Labor Teknik Informatika Universitas Islam Riau.
Aliya Hafiz, Triandi Kurniawan, Nuari Anisa sivi (2020), Tentang Analisa Celah Keamanan Jaringan Dan Server Menggunakan Snort Intrusion Detection System	Penelitian ini membahas tentang penggunaan Intrusion Detection System (IDS) Snort dapat mengurangi dampak buruk dari terjadi nya serangan jaringan.	Penerapan penggunaan IDS Snort dalam mendeteksi serangan yang terjadi	Intrusion Detection System (IDS) snort dapat langsung menemukan adanya serangan yang terjadi pada webserver. Penyerangan masuk melalui *backdoor* atau pintu belakang	Analisa Keamanan Jaringan LAN Menggunakan SNORT dengan Metode *Penetration Test* Di Labor Teknik Informatika Universitas Islam Riau.

2.2 Dasar Teori

2.2.1 Jaringan Komputer

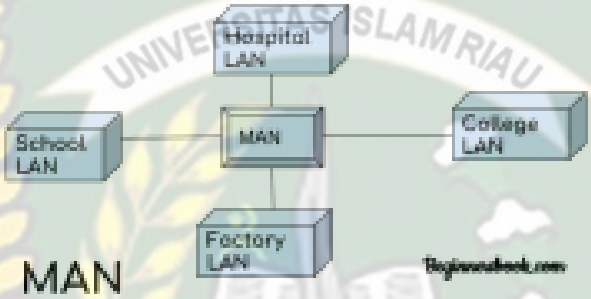
Jaringan komputer dapar diartikan sebagai perpaduan dari perangkat keras atau *hardware* dan perangkat lunak atau *software*. Perangkat tersebut mempunyai banyak manfaat, diantaranya adalah untuk menghubungkan komunikasi dari pengirim kepada penerima sesuai menggunakan metode kabel(*wired*) dan nirkabel(*wireless*) (Saputra, Irawan, & Ilhamsyah, 2014). Dalam jaringan komputer terdapat 3 jenis jaringan komputer itu, yang pertama Area jaringan Lokal atau lebih dikenal dengan Local Area Network (LAN) merupakan sebuah jaringan komputer yang memiliki cakupan area atau wilayah yang kecil seperti jaringan yang ada di dalam kampus, sebuah gedung perusahaan. (Varianto & Badrul, 2015). Gambar dari jaringan LAN dapat dilihat berikut dari



Gambar 2.1 Gambaran Bentuk Jaringan LAN

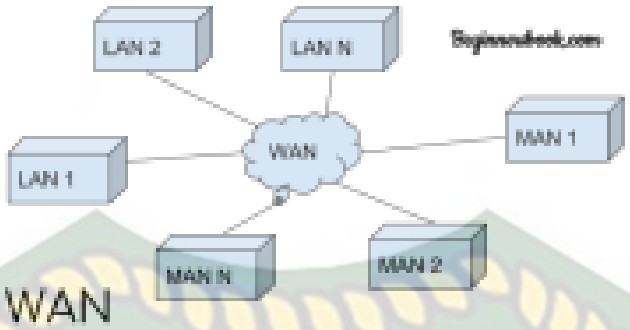
MAN merupakan singakatan dari Metropolitan Area Network dimana merupakan sebuah jaringan yang mempunyai cakupan area yang sedikit lebih luas dibandingkan jaringan LAN yang dimana jaringan MAN ini merupakan sebuah jaringan yang biasa untuk digunakan pada sebuah kantor utama, kantor cabang. Dimana MAN ini lebih dikenal dengan istilah pengabungan antara jaringan

beberapa jaringan LAN yang membentuk jaringan yang lebih besar cakupannya. Karena dengan cakupan yang besar dan luas maka akan mempercepat hubungan komunikasi, serta perpindahan data. Sehingga lebih baik daripada sebuah jaringan LAN (Lukman, 2016). Cakupan area yang dapat dicapai oleh jaringan MAN dapat dilihat pada gambar 2.2 dibawah ini.



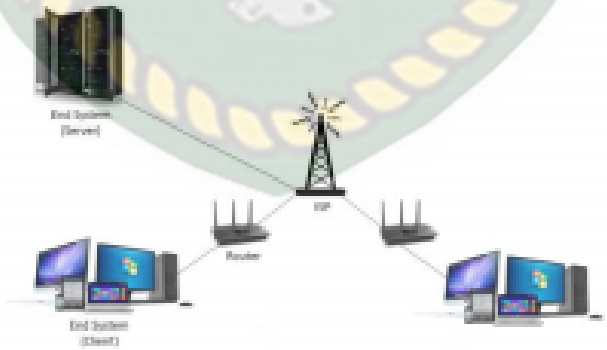
Gambar 2.2 Gambaran Bentuk Jaringan MAN

selain pada jaringan LAN dan MAN, terdapat sebuah jaringan yang memiliki area yang sangat luas, yaitu wide area network (WAN). Pada dasar nya jaringan wan merupakan jaringan yang dipakai untuk mencakup daerah yang tingkatnya lebih luas dan besar dibandingkan jaringan LAN dan MAN seperti wilayah, antar kota, antar provinsi ataupun antar negara ataupun sesama negara tetangga. Pada dasarnya metode dalam jaringan WAN yang dipakai sudah memakai bantuan satelit serta perangkat pemancarnya lebih besar seperti yang biasa digunakan perusahaan penyedia layanan internet yang dinana pemancar skala besar dan banyak ditempatkan diseluruh wilayah supaya memudahkan dalam menghubungkan komunikasi antara pengirim dan penerima dalam waktu yang cepat. (Chelara & Hermanto, 2014). Untuk dapat lebih jelas berikut ini merupakan jaringan WAN yang meliputi area yang besar dan luas seperti pada gambar 2.3 dibawah ini.



Gambar 2.3 Gambaran Bentuk Jaringan WAN

Internet merupakan sebuah konsep jaringan secara keseluruhan atau global yang mempunyai istilah jaringan dunia yang dapat menghubungkan antara sebuah jaringan dengan jaringan lainnya. seperti jaringan yang dimiliki oleh personal maupun jaringan yang dimiliki oleh sebuah instansi atau perusahaan diseluruh dunia. Melalui perangkat yang biasa disebut dengan server yang menggunakan kebijakan komunikasi yang telah disetujui bersama. Sehingga tidak akan terjadinya tabrakan atau gesekan yang menyebabkan jaringan tidak dapat digunakan antar jaringan yang ada didalam dunia internet. (Nurdin, 2015). Untuk lebih jelas dapat dilihat pada gambar 2.4 dibawah ini merupakan bentuk jaringan internet.



Gambar 2.4 Jaringan Internet

2.2.2 Topologi Jaringan

Topologi jaringan atau biasa dikenal dengan sebutan Network Topology, merupakan sebuah struktur yang menggambarkan atau pengarahan sebuah jaringan

komputer yang akan dibangun disuatu tempat tertentu. Adapun fungsinya dari topologi jaringan ini meliputi mensimulasikan sebuah jaringan yang Digambar tersebut sehingga dapat dilihat jaringan yang efektif dan efisien bagi pengguna. (Nirsal & Ali, 2017). Topologi jaringan komputer memiliki banyak jenis diantara nya:

1. Topologi Bus

Topologi bus merupakan suatu yang mempunyai titik lemah dalam proses transfer data maupun komunikasi antara pengirim dan penerima. Sehingga disebabkan oleh terjadinya tabrakan ataupun aduan dalam jaringan yang dimiliki topologi bus ini. topologi bus ini merupakan sebuah perangkat terjadi masalah atau tidak dapat terhubung ke internet maka semua perangkat dalam toplogi bus ini akan ikut mengalami masalah tersebut. Khusus topologi diwajibkan adanya konektor T-Bone Connector. Supaya tidak mudah terjadinya sebuah masalah.

2. Topologi Star

Topologi star merupakan sebuah topologi yang telah diperbarui dan lebih baik dibandingkan dengan topologi bus. Karena pada topologi star mempunyai aspek yang dapat terhubung secara tengah atau sentral, yaitu dimana pada sebuah perangkat yang diletakkan di sentral atau tengah maka diantara perangkat-perangkat yang terkoneksi, maka tabrakan data akan sangat jarang dijumpai.

3. Topologi Ring

Selanjutnya topologi ring pada dasarnya merupakan kebalikan dari topologi Star, karena topologi ring ini tidak mempunyai sebuah perangkat yang menjadi

sentral, sehingga penyusunan secara keliling pada sebuah perangkat yang terhubung, topologi ring ini pada dasarnya berbentuk seperti sebuah cincin karena topologi ini seperti lingkaran. Topologi ini kelemahannya sama seperti topologi Bus.

4. Topologi Mesh

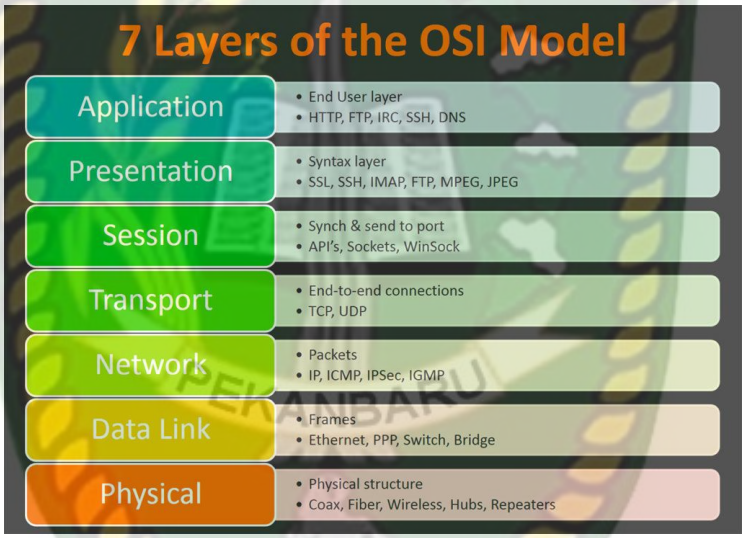
Topologi mesh merupakan topologi yang memiliki kesalahan paling minim karena topologi ini dibuat dari kesalahan-kesalahan yang telah dilakukan pada topologi sebelumnya. Sehingga di topologi ini tidak akan mungkin terjadinya sebuah tabrakan data yang menyebabkan masalah pada jaringan. Karena toplogi mesh tidak akan adanya kelumpuhan jaringan jika satu perangkat bermasalah maka perangkat lain tidak akan kenak masalah dan topologi mesh memakai konektor yang hemat daya.

5. Topologi Tree

topologi tree yang penggabungan antara topologi Bus dan topologi Star, karna bentuk dari topologi tree menggunakan metode dengan konsep sentralitas tetapi setiap perangkat dihubungkan melauin konektor T-Backbone connector. Permasalahan yang terjadi akan sama dengan masalah yang ada pada kedua topologi itu, karena jika terjadinya tabrakan data dan tidak dapat diakses nya jaringan secara keseluruhan atau semua jika terdapat sebuah perangkat yang bermasalah.

2.2.3 OSI Layer

Kepanjangan dari OSI layer adalah *Open System Interconnection* (OSI) yang dimana pada sebuah salah layer yang digunakan sebagai koordinator standar pertukaran serta sebagai pengembangan data di suatu jaringan. OSI layer ini memiliki perbedaan dengan sebuah protokol yang ada karena OSI layer selalu berdasarkan acuan dalam jaringan komputer (Supatmi, Nizar, & Fahlevi, 2014). Untuk lebih jelas dapat dilihat pada gambar 2.5 Dibawah ini.



Gambar 2.5 OSI Layer

OSI layer memiliki tujuh tingkat atau lapisan yang setiap tingkatnya memiliki fungsi yang saling berhubungan satu sama lain, ketujuh tingkat tersebut yaitu:

1. Application Layer atau tingkatan paling atas pada osi model, karena pada dasarnya layer ini bekerja sebagai *interface* sebuah aplikasi yang akan selalu membagi jalan jaringan kepada setiap aplikasi

2. Presentation Layer, pada osi model ini bekerja untuk melihat dan mengawasi data-data yang akan dikirim dari aplikasi sesuai dengan dikonversikan ke dalam format yang mudah dipahami oleh lapisan aplikasi melalui jaringannya.
3. Session Layer, pada osi model ini bekerja sebagai mengatur supaya koneksi dapat terkoneksi dengan baik sehingga osi layer ini digunaka untuk komunikasi antar aplikasi.
4. Transport Layer, osi model ini memiliki kerja sebagai pengiriman paket data dari pengirim hingga sampai kepada penerima dan osi layer ini juga dapat melihat dan mengawasi paket data yang telah sampai ke penerima dengan baik atau tidak
5. Network Layer, pada osi model ini memiliki tugas sebagai pendefinisikan antara alamat IP sehingga selanjutnya akan berfungsi sebagai yang melaksanakan routing dalam jaringan menggunakan perangkat seperti *Router dan Switch.*
6. DataLink Layer, pada osi model ini memiliki spesifikasi IEEE 802 yang dimana itu berfungsi sebagai pembagi antara layer ini menjadi dua layer lagi. Sehingga keduanya memiliki lapisan Logical Link Control (LLC) dan lapisan Media Access Control (MAC).
7. Physical Layer, pada model osi ini memiliki tugas sebagai pemproses dan menentukan media yang dipakai sebagai sebuah transmisi jaringan, sehingga banyak terdapat juga aktifitas untuk menentukan sebuah sinyal yang digunakan dan bagaimana untuk sinkronisasi bite, penggambaran

arsitektur pada sebuah jaringan, dan juga pada topologi jaringan dan tipe dan jenis kabel yang digunakan.

2.2.4 Internet *Protocol* (IP)

Internet protocol atau *ip Address* mempunyai pengertian sebagai pengalamatan sebuah alamat jaringan dengan cara yang itu melakukan penyebaran baris numeric atau angka untuk semua perangkat jaringan sehingga dapat digunakan di interface dari sebuah perangkat tersebut. Pada dasarnya sebuah IP Address memiliki manfaat sebagai mendeteksi masalah yang ada pada saat pengiriman dan penerimaan paket data. Sehingga saat sedang berlangsungnya komunikasi antar data-data, *IP Address* memberlakukan dua aturan yang dimana aturan itu yaitu, addressing dan fragmentation (Wardoyo, Ryadi, & Fahrizal, 2014). Pada dasarnya sebuah alamat IP atau disebut juga dengan *IP address* yang memiliki pengertian sebagai identitas dari sebuah perangkat yang ada dimana perangkat itu seperti *personal computer* (PC), serta laptop dan perangkat keras jaringan lainnya, sekalipun *handphone* atau *smartphone*. Identititas itu memiliki cara penulisannya seperti kumpulan-kumpulan numerik angka yang unik yang sudah diacak secara random. Karena susunan angkanya acak dan unik, maka setiap perangkat dipastikan tidak akan memiliki identitas yang sama dengan perangkat lainnya. (Tambunan, Raharjo, & Purwadi, 2013). *IP address* berdasarkan sifat dan karakternya tyang dapat dilihat atas 4 macam, yang pertama *Static IP Address*, yaitu sebuah alamat IP yang penggunaannya hanya dipakai sebagai pemasukan yang dilakukan oleh user itu sendiri dan tidak auto atau otomatis. Selanjutnya yang kedua yaitu *Dynamic IP Address*, yaitu dimana kebalikan dari *Static IP Address* karena pada *Dynamic Ip*

Address setiap perangkat dapat mempunyai alamat IP secara otomatis yang dibagi melalui server yang biasa dikenal dengan DHCP Server. Selanjutnya yang ketiga, *Public IP Address,* alamat IP ini dibuat masih secara massif, dengan aturan yang pada dasarnya semua perangkat terhubung ke jaringan yang sama, maka jaringan itu akan terhubung kejaringan internet.

2.2.5 Server

Pada dasarnya sebuah server memiliki bentuk yang sama dengan komputer client. Yang membedakannya yaitu jika server lebih memiliki spesifikasi yang lebih baik daripada sebuah *personal computer client*, karena server akan banyak memproses data dalam skala besar sehingga pasti membutuhkan performa yang baik dan tinggi atau bisa juga karena server juga memiliki tugas sebagai penyedia layanan (sesuai dengan namanya) yang dimana layanan yang ditawarkan dari server beragam jenisnya seperti web server, dns server dan masih banyak lagi sesuai dengan yang dibutuhkan dan sesuai dengan konfigurasi yang dibutuhkan oleh administrator server (Bawafie & Muslihudin, 2013).

2.2.6 Linux

Linux adalah sebuah sistem opeasi yang menggunakan kernel sebagai sistem operasi yang berisikan sebuah *script* yang ada. Selanjutnya linux memiliki terdapat juga banyak user yang mempunyai pengaruh besar dalam perkembangan sistem operasi linux ini. Pada dasarnya linux banyak digunakan untuk pentest dalam sebuah pengujian sistem keamanan jaringan karena linux mempunyai banyak tools yang memudahkan dalam melakukan pengujian sistem keamanan itu. Untuk keseluruhan dari sistem operasi ini adalah sistem operasi ini pada yang berbasis

General Public License (GPL) yang ditetapkan pada tahun 1983 oleh Richard Stallman. Pengaruh GNU yang sangat besar karena sebagai pelopor munculnya nama alternatif GNU/Linux (Harjono, 2016).

2.2.7 Snort

Snort merupakan sebuah aplikasi atau tool keamanan yang berfungsi untuk mendeteksi intrusi-intrusi jaringan (penyusupan, penyerangan, pemindaian, dan beragam bentuk ancaman lainnya), sekaligus juga melakukan pencegahan. Dalam praktiknya, snort sangat andal untuk membentuk logging paket-paket dan analisis trafik-trafik secara real-time dalam jaringan berbasis TCP/IP. Sehingga Snort merupakan suatu sistem yang mendeteksi secara *real time* terhadap adanya serangan jaringan dengan hasil alert dari serangan jaringan tersebut. (Kerry J & Christopher, 2004). Snort dapat dioperasikan dalam 4 mode, yaitu:

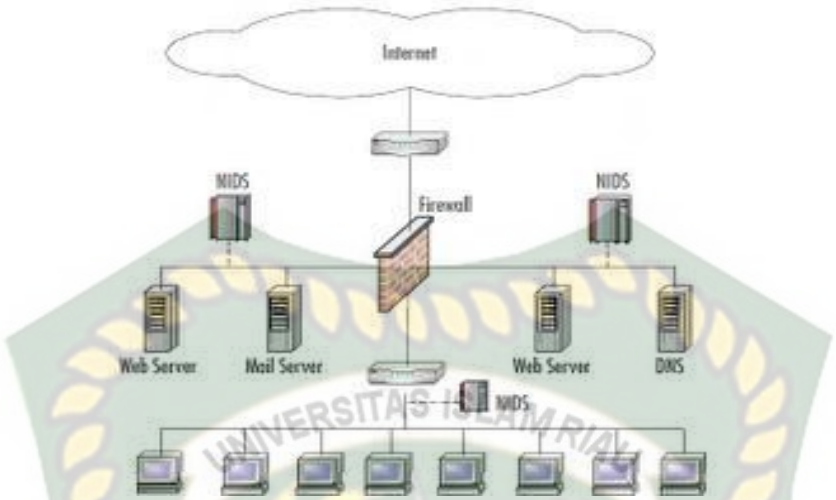
1. ***Sniffer mode***. Pada mode ini snort melakukan tugasnya untuk menangkap seluruh data yang lewat dan serta snort dapat melihat seluruh paket data pada sebuah jaringan.
2. ***Logger mode.*** Pada mode ini snort bertugas mencatat semua paket data yang lewat dalam sebuah jaringan sehigga dapat dilihat dan dianalisis dikemudian hari.
3. ***Intrusion Detection Mode***. Pada mode ini Snort akan akan bertugas sebagai pendeteksi sebuah tindakan serangan jaringan komputer. Karena untuk memerlukan beberapa file atau *rules* yang akan membedakan sebuah paket normal dengan sebuah paket yang membawa serangan serangan jaringan.

4. ***Inline mode***. Pada mode ini snort bertugas membandingkan sebuah paket data dengan aturan iptables dan libpcap dan kemudian dapat menentukan iptables untuk melakukan penjatuhkan paket yang berisi serangan atau paket normal atau bisa juga menerima paket berdasarkan aturan snort yang lebih baik lagi.

Penempatan Snort sebagai IDS dalam jaringan dapat dilakukan dengan 3 konsep *Snort* IDS Placement, tergantung kebutuhan dan ketersediaan perangkat yang ada. Konsep penempatan Snort IDS dalam jaringan adalah sebagai berikut:

1. Network Intrusion Detection System

Pada dasarnya Snort NIDS ini melakukan monitoring paket data pada sebuah perangkat jaringan yang telah dipasang Snort, namun juga terhadap semua bentuk lalu lintas sebuah jaringan yang berada didalam segmen jaringan dirnana Snort itu berada. Adapun kelebihan dari sistem NIDS ini meliputi cakupan jaringan yang diawasi cukup luas, sehingga dalam melakukan pengamanan pada sebuah jaringan yang memiliki sistem IDS maka mempunyai jangkauan yang lebih luas. Sedangkan kelemahannya dalam NIDS ini meliputi jaringan komputer yang menggunakan IDS akan melakukan mempunyai lalu lintas data yang sangat banyak, Untuk dapat lebih jelas pada gambar 2.6 dibawah ini :

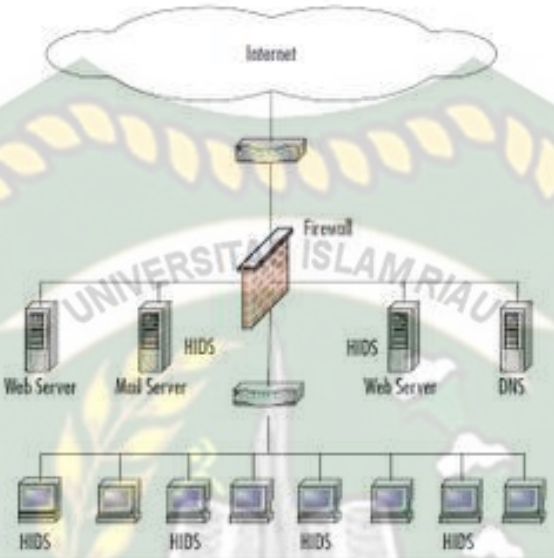


Gambar 2.6 Skema Jaringan Snort NIDS (Mohammad Affandi, Sigit Setyowibowo, 2013)

2. Host Intrusion Detection System

Host Based Intrusion Detection System atau HIDS ini kebalikan dari NIDS. Karena pada Sistem HIDS ini hanya melakukan pengamatan lalu lintas pada sebuah data yang berada perangkat jaringan, yang di mana snort diletakkan atau snort berada. Berada kegunaannya konsep sistem ini. Dimana snort dapat dijalankan pada server seperti web server, jaringan server maupun database server. Adapun keuntungan dari sistem HIDS meliputi penggunaan rule yang lebih simpel. Karena HIDS hanya bekerja untuk sebuah server saja berada dengan NIDS yang bekerja untuk jaringan yang luas. maka rule yang diperlukan adalah rule unluk mendeteksi adanya eksploitasi terhadap web server tanpa perlu menggunakan rule untuk deteksi serangan terhadap aplikasi layanan yang tidak dijalankan oleh mesin tersebut. Konsekuensinya, maka rule yang digunakan lebih sedikit, sehingga dapat meningkatkan performa mesin komputer dan mengurungi beban pada processor

karena data yang harus diperiksa oleh sensor IDS lebih sedikit. Skema jaringan sistem Snort HIDS digambarkan pada Gambar 2.7 dibawah ini :



Gambar 2.7 Skema Jaringan Snort HIDS (Mohammad Affandi, Sigit Setyowibowo, 2013)

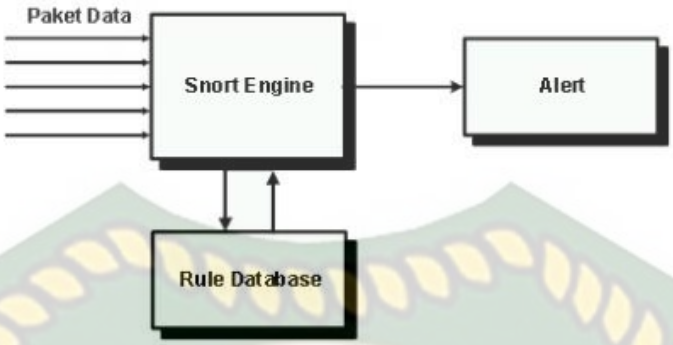
Dalam pendeteksian ada nya serangan jaringan ini bertujuan untuk pengamanan server dan jaringan dari bahaya nya serangan jaringan. Snort merupakan suatu aplikasi yang dapat mendeteksi semua jenis serangan. Berikut daftar serangan jaringan yang bisa dideteksi oleh snort.

Tabel 2.2 Serangan Jaringan Yang Dapat Dideteksi Oleh Snort

NO	Serangan Jaringan
1.	*Brute Force*
2.	*Dictionary*
3.	*Buffer Overflow.*
4.	*DDOS dan DOS*

5.	*Floading attack*
6.	*Port Scanning*
7.	*Ping Of Death*
8.	*Smurf attack*
9.	*Stream attack*
10.	*spoofing*
11.	Serangan *main-in-the-middle*
12.	*Teardrop*
13.	*sniffer*
14.	*DNS Poisoning*
15.	*SQL Injection*
16.	*Remote controlled attack*
17.	*phising*
18.	*Script Kiddies*
19.	*Cross Scripting*
20.	*Land Attack*

Sebagai kelengkapan dari sebuah sistem perangkat lunak. Snort IDS mempunyai 3 komponen utama yang saling berhubungan satu sama lain. Komponen utama dari Snort tersebut adalah snort engine, rule snort dan alert. Snort engine merupakan pemroses yang akan melakukan pembandingan paket data dengan rule Snort untuk dapat menghasilkan output berupa alert. Ketiga komponen tersebut bekerja dalam satu siklus yang saling berpengaruh, seperti ditunjukkan pada Gambar 2.8 tentang komponen Snort tersebut adalah sebagai berikut:



Gambar 2.8 Komponen Snort

2.2.8 Keamanan Jaringan

Pada dunia komputer hal yang paling penting dalam proses berjalannya sistem komputer salah satunya adalah keamanan dari jaringan komputer itu sendiri, baik itu jaringan yang terhubung secara lokal ataupun jaringan yang terhubung ke dunia luar atau disebut juga internet. Keamanan jaringan komputer diperhatikan dan dianggap penting sejak adanya kasus kriminalitas lewat internet, contohnya kasur pencurian data, pencurian uang online, peretasan situs ataupun komputer server, penyerangan komputer dengan cara menyebarkan virus dan banyak contoh lainnya. Keamanan jaringan komputer pada umumnya sudah banyak dilakukan pencegahan serta penanggulangannya jika sudah diretas hinggake server. Salah satu contohnya seperti sistem keamanan komputer SNORT IDS dan SNORT IPS serta adanya Security Onion. (Muhartin, 2017).

BAB III
METODOLOGI PENELITIAN

3.1 Metode Penelitian

Penelitian ini menggunakan metode *penetration test* yang merupakan bentuk penelitian pengujian serangan langsung menggunakan simulasi serangan jaringan untuk mengetahui kerentanan jaringan pada instansi terkait. Dalam menggunakan metode *penetration test* sama dengan sebuah penyerangan secara langsung. Pada penelitian ini, mengambarkan sebuah IP address client/korban dilakukan penyerangan dengan menggunakan kali linux, sehingga untuk mengetahui atau mendeteki adanya serangan tersebut dapat dideteksi oleh snort. Dalam penelitian ini menggunakan jenis IDS berdasarkan penempatannya yaitu NIDS (*network intrusion detection system*), yang dimana pengujian ini bertujuan untuk mengetahui keamanan jaringan yang berada di instansi. Karena setiap akses yang menuju ke server harus melewati sistem IDS ini.

Snort merupakan tool keamanan untuk mengetahui adanya penyusupan jaringan dan penyegahan. Dalam penelitian ini *penetration test* menggunakan metode *grey box* yang dimana dalam pengujian ini penguji menjadi sebagai pengguna sehingga penguji memiliki akses dan informasi sebatas sebagai pengguna.

3.2 Alat Dan Bahan Penelitian Yang Dibutuhkan

3.2.1. Spesifikasi Perangkat Lunak

Spesifikasi perangkat lunak adalah software yang digunakan sebagai penghubung dalam melakukan penelitian ini. Berikut adalah *software* yang digunakan:

Tabel 3.1 Spesifikasi perangkat lunak

Perangkat Lunak	Spesifikasi
Sistem Operasi (*Client*/Target)	Linux Ubuntu
Virtual Machine	Virtual Box
Sistem Operasi (penyerang/*Attacker*)	Kali Linux,
Intrusion Detection System (IDS)	Snort

3.2.2. Spesifikasi Perangkat Keras

Spesifikasi perangkat keras adalah peralatan yang digunakan sebagai pendukung dalam melakukan penelitian ini. Berikut dibawah ini adalah merupakan perangkat keras yang digunakan dalam melakukan penelitian ini:

Tabel 3.2 Spesifikasi perangkat keras

Perangkat Keras	Spesifikasi
Laptop	Asus 456UR
Harddisk	1 TB
SSD	1 TB
Processor	Intel core I5-7200U
Ram	12 GB

3.3 Jenis Data

Jenis data yang digunakan dalam penelitian adalah :

1. Data primer yaitu data yang di peroleh dan didapati langsung dari labor teknik informatika universitas islam riau
2. Data sekunder yaitu data yang di peroleh dari buku, jurnal ilmiah dan internet.

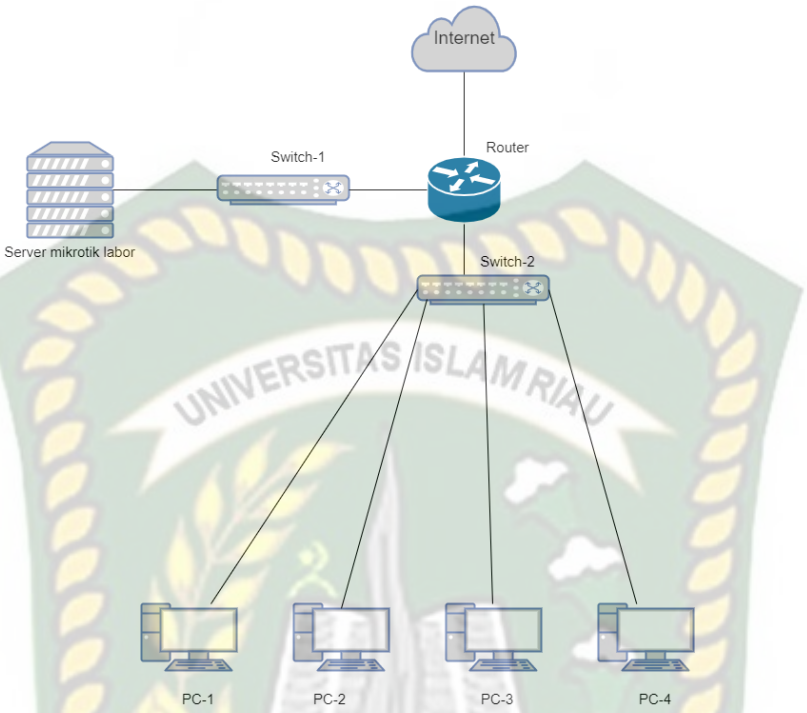
3.4 Metode Pengumpulan Data

1. Observasi : Melakukan pengamatan terhadap jaringan lokal dilabor Teknik informatika Universitas Islam Riau
2. Wawancara : Pengumpulan informasi dari tanya jawab terhadap salah satu pegawai dan dosen di labor Teknik informatika Universitas Islam Riau.

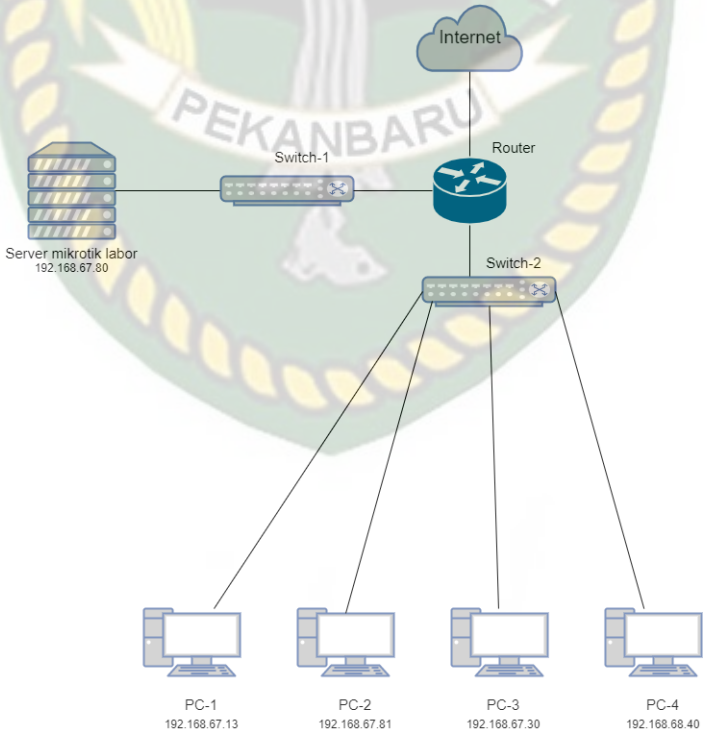
3.5 Analisa Sistem Yang Sedang Berjalan

3.5.1 Topologi Jaringan Labor Teknik Informatika Universitas Islam Riau

Topologi merupakan hal paling mendasar dalam membentuk sebuah jaringan, untuk topologi jaringan yang digunakan dilabor Teknik informatika universitas islam riau menggunakan Topologi *Star*, karena setiap komputer menggunakan satu kabel jaringan, apabila satu komputer ada yang rusak maka jaringan komputer yang lain tidak terganggu. Topologi *star* mengutamakan komputer *server* sebagai pusat kontrol. Hal ini menyangkut fungsi dan efisiensi instansi dalam pengawasan keamanan jaringan. Untuk itu berikut ini merupakan topologi fisik dan topologi *logic* di labor teknik informatika universitas islam riau.



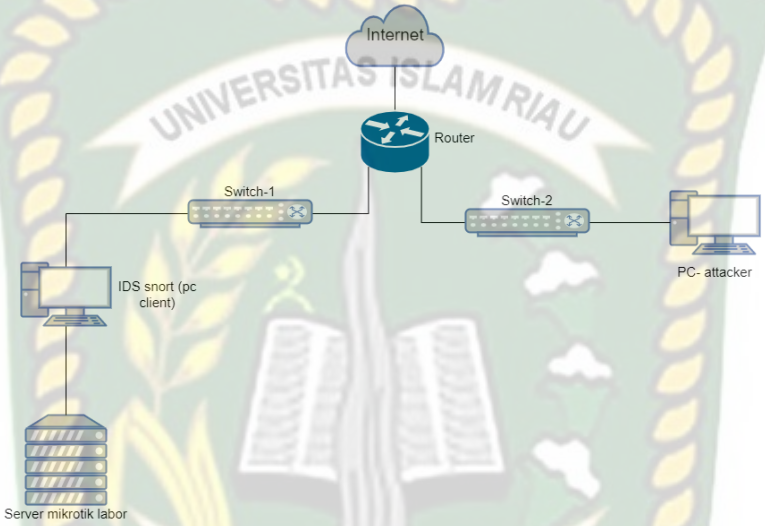
Gambar 3.1 Topologi Logic Labor Teknik Informatika Universitas Islam Riau



Gambar 3.2 Topologi Fisik Labor Teknik Informatika Universitas Islam Riau

3.6 Gambaran umum sistem

Sistem IDS dalam penelitian ini memiliki arsitektur jaringan yang memberikan gambaran secara jelas mengenai interkoneksi antar perangkat satu dengan perangkat lainnya. Berikut gambar 3.3 dibawah ini merupakan sistem IDS snort.



Gambar 3.3 Implementasi sistem IDS snort

3.7 Permasalahan Yang Dihadapi

Permasalahan yang dihadapi dalam melakukan objek penelitian meliputi keamanan data yang bisa dibilang data penting yang tidak bisa diketahui oleh orang umum. Serta minimnya pengawasan terhadap keamanan jaringan labor Teknik informatika universitas islam riau. Sehingga dengan ada nya penelitian ini memudahkan pegawai IT/administrator dalam melakukan pendeteksi terhadap adanya serangan jaringan.

3.8 Usulan Perancangan Sistem

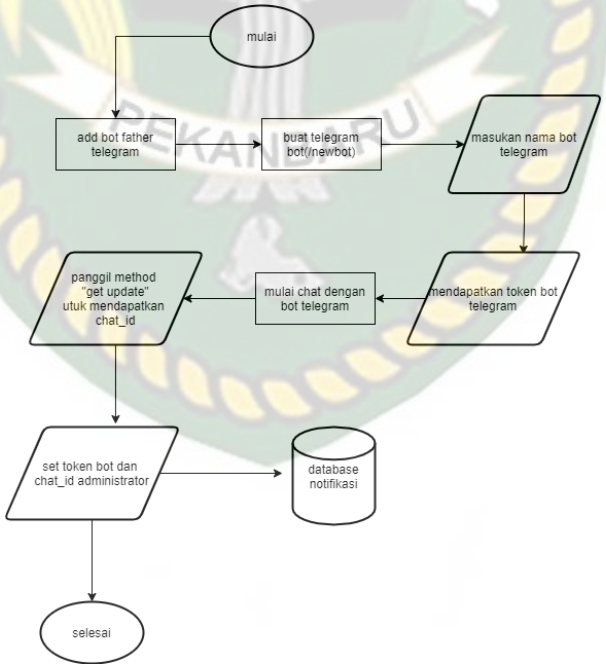
Perancangan sistem untuk mengatasi permasalahan yang ada diinstansi terkait meliputi pengawasan terhadap keamanan jaringan melalui *tool/software* yang berguna untuk pencegahan terhadap serangan jaringan yang mungkin saja bisa

dilakukan saat tidak terduga. *Software* bisa meliputi snort yang bertujuan untuk mendeteksi adanya serangan jaringan dan menangkap paket-paket data. *Penetration test* adalah metode yang sudah digunakan khalayak umum, terutama dalam kalangan *network tester* dimana tujuan dari metode ini adalah menguji atau mengetest keamanan dari sistem yang telah ada atau yang baru dirancang yang meliputi pada jaringan lokal. Berikut ini merupakan proses alur dalam *penetration test*.

Gambar 3.4 Flowchart Penetration test

3.8.1 Diagram pembuatan bot telegram

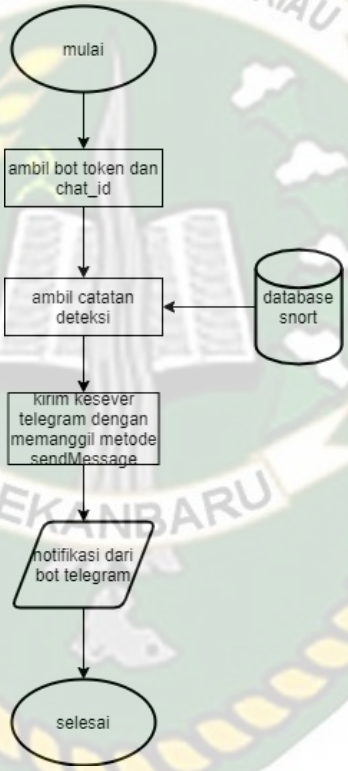
Pada proses selanjutnya yaitu pembuatan bot telegram. proses pembuatan dimulai dengan meminta akun bot resmi pada @botfather. Dengan memasukan perintah bot baru hingga mendapatkan token dari bot yang akan digunakan sebagai media peringatan pendeteksian pada snort agar diketahui oleh administrator. Pada dasarnya notifikasi yang dikirimkan oleh bot telegram sepenuhnya berasal dari 1 database yang sama dengan yang digunakan untuk menampung alert snort. Untuk mengetahui id pengguna, administrator harus memulai chat terhadap bot. kemudian mengunjungi situs telegram dengan alamat http://api.telegram.org/bot <token> /getupdates. Dimana <token> diisi dengan token bot telegram yang didapati dari botfather. Untuk lebih jelas bisa melihat gambar 3.4 diagram dibawah ini.



Gambar 3.5 flowchat pembuatan bot telegram

3.8.2 Diagram pengiriman notifikasi

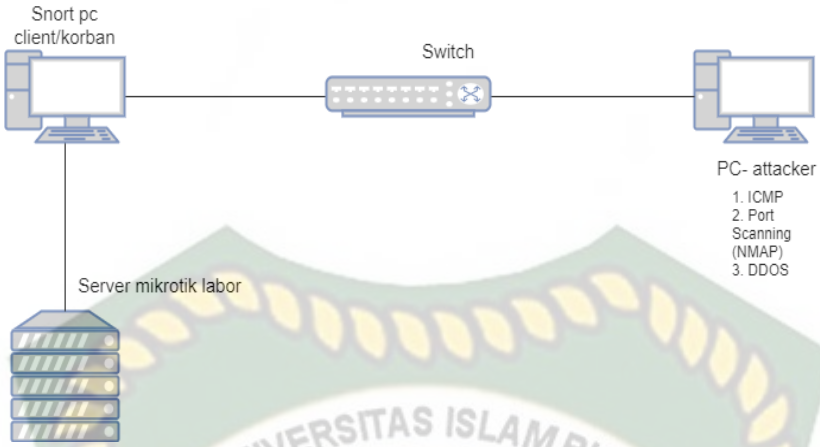
Pengiriman notfikasi yang dikirim berasal dari satu database yang sama dengan yang digunakan snort untuk menyimpan hasil deteksi nya. Token dari bot telegram berfungsi untuk mengakses API telegram, sehingga tidak sembarang orang bisa untuk dapat mengakses bot yang dijadikan sebagai media pengiriman peringatan dari snort. Untuk lebih jelas dapat melihat gambar 3.5 dibawah ini.



Gambar 3.6 flowchart pengiriman notfikasi telegram

3.9 Pengujian sistem

Pengujian sistem merupakan tahapan untuk melakukan evaluasi atau uji coba dari penelitian ini. Evaluasi ini bertujuan untuk menentukan efektif dari snort sebagai sistem pendeteksian dari adanya ancaman-ancaman jaringan. Untuk skema pengujian dapat dilihat pada gambar 3.7 dibawah ini.



Gambar 3.7 Tahapan pengujian sistem

Pada gambar 3.7 diatas ini merupakan tahapan pengujian yang dimana penyerang akan melakukan pengujian ke komputer client/korban yang terhubung ke server jaringan dilabor Teknik informatika universitas islam riau. Sehingga saat penyerang melakukan pengujian maka snort akan mendeteksi adanya ancaman atau serangan.

BAB IV

HASIL DAN PEMBAHASAN

Analisis ini digunakan supaya dapat mengetahui keamanan yang ada dalam sebuah jaringan LAN di labor Teknik informatika universitas islam riau. Keamanan jaringan komputer yang berada di labor Teknik informatika universitas islam riau masih diperlukan untuk peningkatan keamanan, karena dilabor Teknik informatika memiliki jaringan yang terhubung keserver yang dimana pada server tersebut memiliki data-data penting terkait informasi dan pembagian jaringan dilabor Teknik informatika. Sehingga skenario dalam melakukan pengujian keamanan jaringan di labor Teknik informatika meliputi pengujian keamanan terhadap adanya serangan-serangan jaringan yang dilakukan oleh orang yang tidak bertanggung jawab. Dimana dalam melakukan pengujian ini memiliki adanya ip address penyerang dan ip address client/korban.

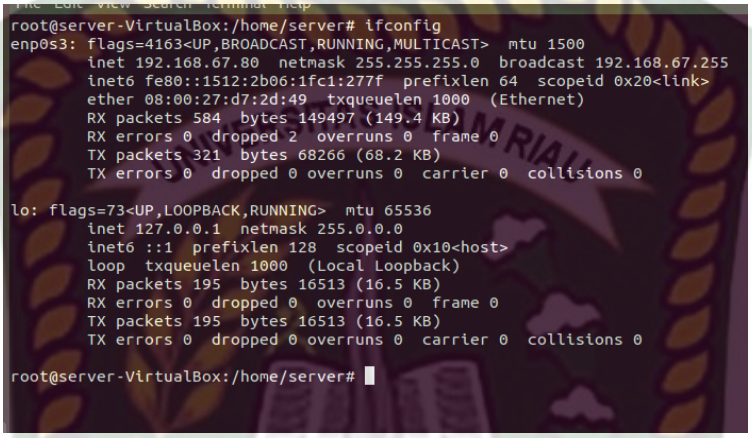
Tabel 4.1 IP address

NO	IP address penyerang	Ip address client/korban
1	192.168.67.81 dan 103.100.120.10	192.168.67.80

4.1 Analisa hasil penelitian

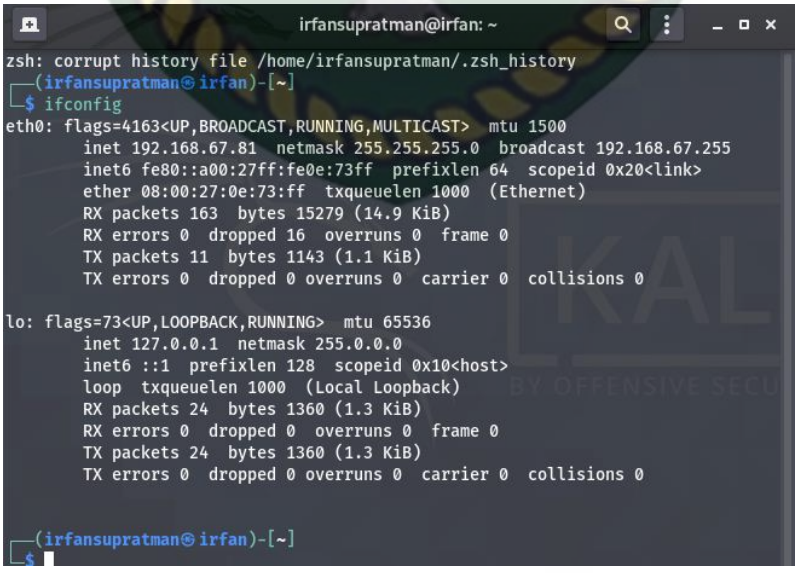
Skenario dalam pengujian ini sebelum melakukan pemasangan snort pada sebuah komputer yang terhubung kedalam jaringan LAN labor Teknik informatika, ada beberapa hal yang diperlukan yang pertama terkait untuk melihat ip address dari server, dari client dan jika sudah terhubung dalam satu jaringan LAN maka baru dilakukan pemasangan snort pada komputer tersebut. Snort merupakan sistem

yang dapat untuk mendeteksi adanya serangan jaringan atau penyalahgunaan jaringan sehingga diperlukannya percobaan dengan melakukan penyerangan terhadap jaringan yang sudah dipasang snort. Berikut ini ip server pada gambar 4.1 dibawah ini :



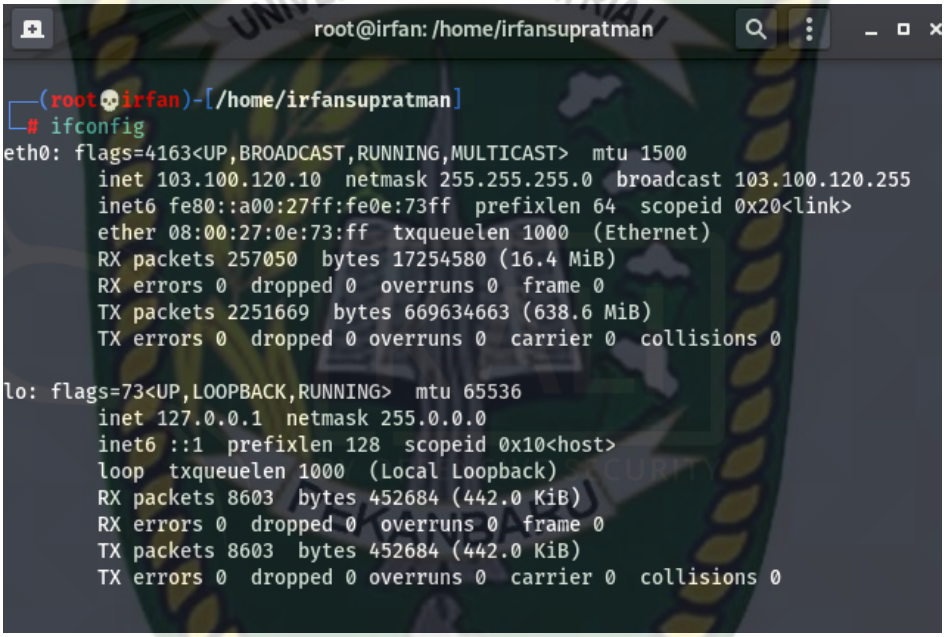
Gambar 4.1 IP address client/korban

Pada gambar 4.1 ketika menuliskan ifconfig pada terminal linux ubuntu maka akan menampilkan IP 192.168.67.80 (sebagai *client*/korban) yang dimana ip address ini akan diserang oleh penyerang. Berikut ini gambar 4.2 merupakan IP address jaringan komputer sebagai penyerang:



Gambar 4.2 IP address penyerang

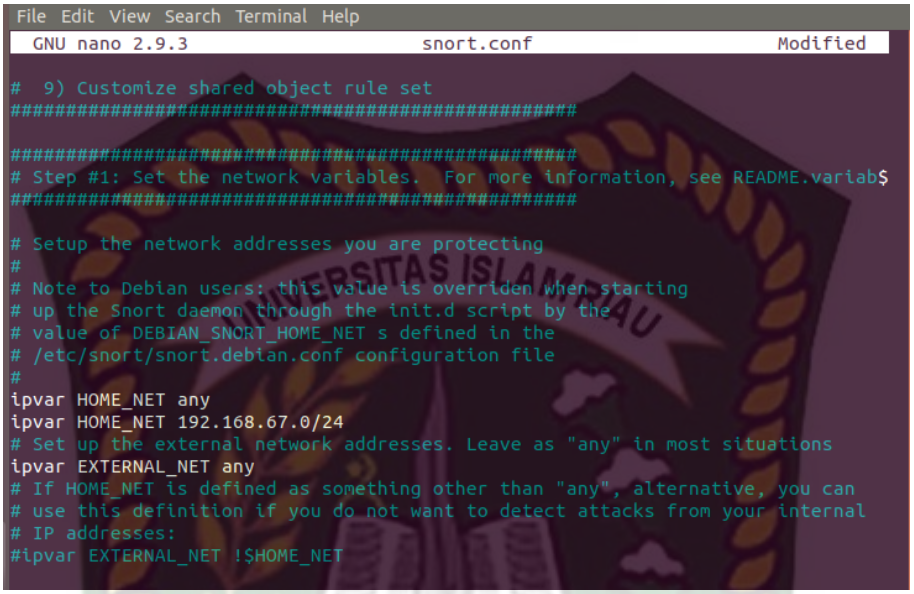
Untuk menampilkan ip address penyerang pada komputer penyerangan dengan menggunakan sistem operasi kali linux dapat menulis kan ifconfig pada terminal sehingga akan memunculkan ip address penyerang 192.168.67.80 (penyerang). Selanjut nya pada jaringan yang berbeda dapat mengetikan ifconfig dan akan muncul ip 103.100.120.10. untuk lebih jelas dapat dilihat pada gambar 4.3 dibawah ini.



Gambar 4.3 Ip address penyerang berbeda

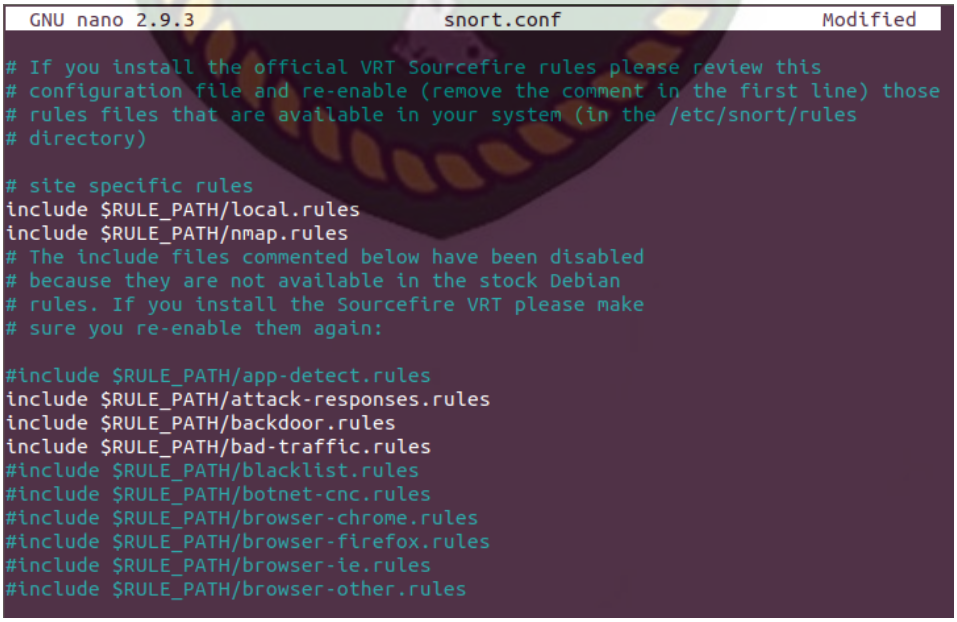
Sebelum tahapan pengujian ada beberapa hal yang perlu dilakukan dalam pendeteksian snort apakah berjalan sesuai dengan diharapkan diantara nya dengan melakukan pembuatan rule snort terkait adanya ancaman supaya dapat terdekteksi oleh snort. Selanjutnya konfigurasi snort supaya snort dapat bekerja sebagai IDS untuk mendeteksi serangan. Dalam konfigurasi snort ada hal yang penting perlu untuk dilaksanakan seperti untuk memasukan ip address client yang ingin dilindungin pada folder snort.conf dan snort.debian.conf, sehingga snort dapat

berjalan mendeteksi jika adanya percobaan penyerangan terhadap ip client tersebut. Untuk lebih jelas dapat dilihat pada gambar 4.4 dibawah ini.



Gambar 4.4 tampilan konfigurasi ip address snort

Pada gambar 4.4 diatas dapat dilihat ip address yang ingin dilindungi oleh snort yang dimana ip nya 192.168.67.0/24. Selanjutnya memilih rules-rules snort yang dingin diaktifkan seperti pada gambar 4.5 dibawah ini.

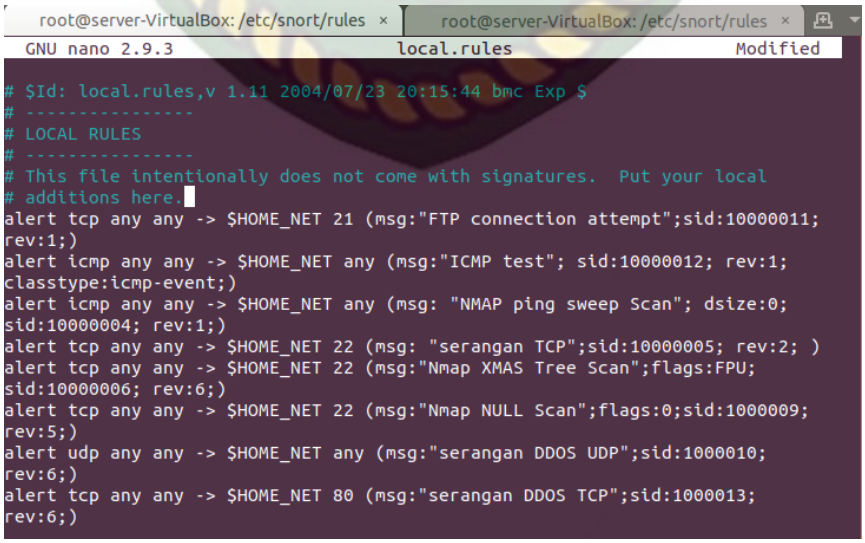


Gambar 4.5 konfigurasi memilih pengaktifkan rule snort

Selanjutnya konfigurasi pada folder snort.debian.conf dalam konfigurasi difolder ini sama dengan folder snort.conf yang dimana memasukan ip address yang ingin dilindungi untuk lebih jelas nya dapat dilihat pada gambar 4.6 dibawah ini.

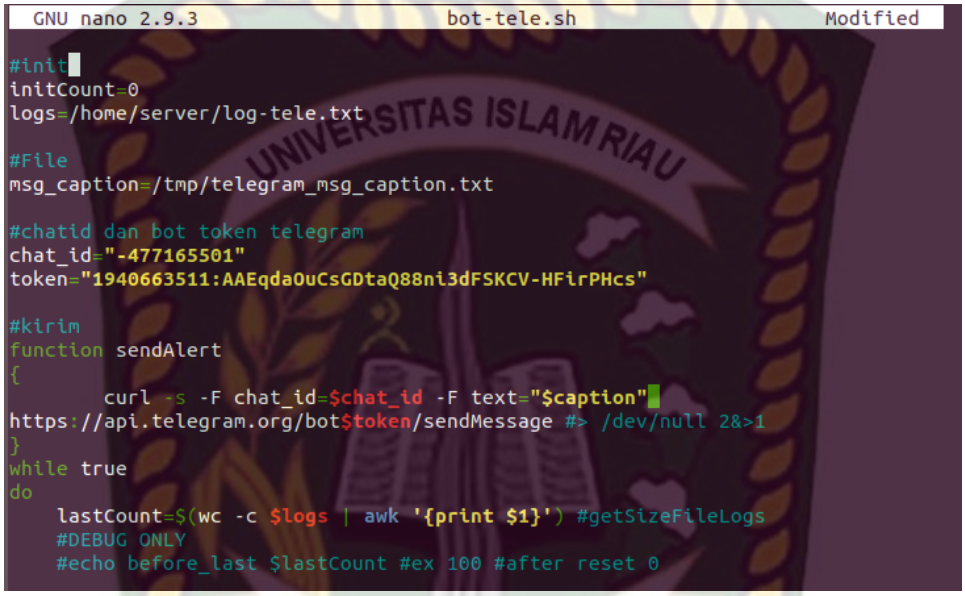
Gambar 4.6 konfigurasi pada folder snort.debian.conf

Setelah melakukan konfigurasi pada folder snort.conf dan snort.debian.conf maka Langkah selanjutnya membuat rule snort supaya snort dapat mendeteksi serangan sesuai dengan serangan. Untuk lebih jelas dapat dilihat pada gambar 4.7 dibawah ini.



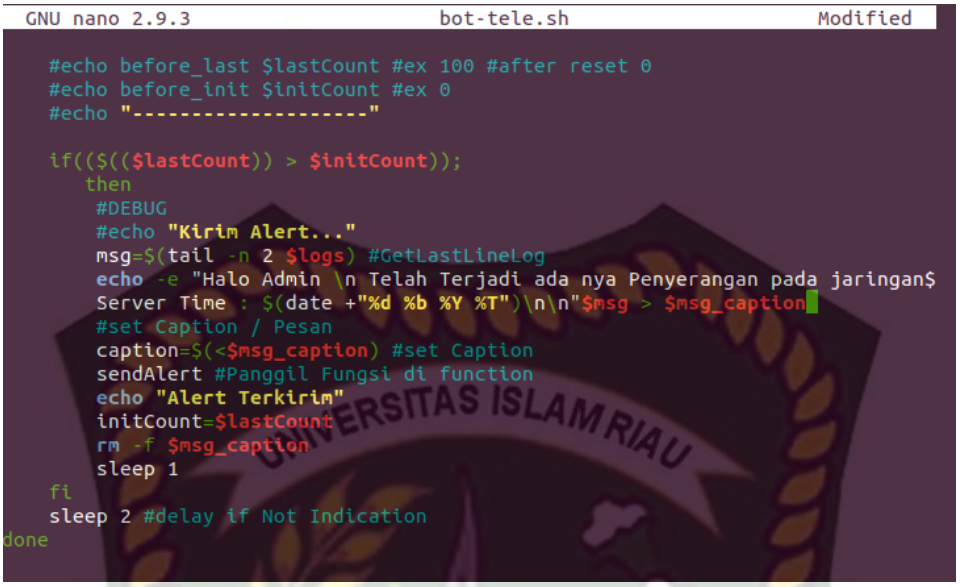
Gambar 4.7 rules snort

Selanjutnya konfigurasi snort dan telegram supaya jika terjadi penyerangan snort dapat mendeteksi adanya serangan dan melakukan pengiriman peringatan kepada administrator/pegawai IT melalui telegram. Pada gambar 4.8 dibawah ini merupakan konfigurasi untuk membuat snort terhubung ke API telegram.



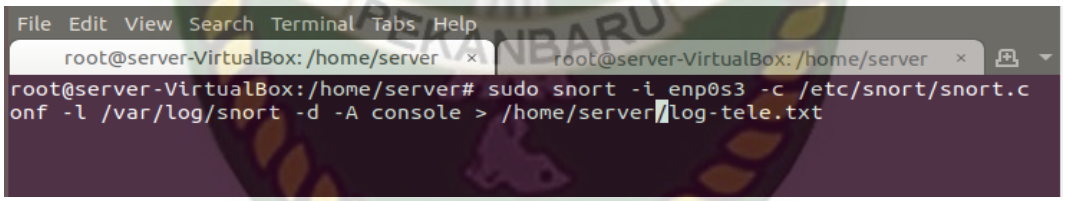
Gambar 4.8 Konfigurasi snort ke telegram

Pada gambar 4.8 diatas dapat dilihat dimana pada konfigurasi ini memasukan chat_id dan token yang didapati dari telegram, supaya snort dapat terhubung ke telegram. Pada gambar 4.9 ini merupakan tampilan kata-kata yang akan ditampilkan pada interface telegram administrator.



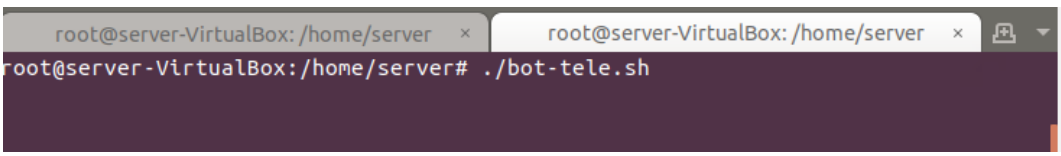
Gambar 4.9 konfigurasi kalimat yang tampil ditelegram

Untuk menjalakan snort dapat menuliskan perintah seperti gambar 4.9 dibawah ini. Yang dimana perintahnya **sudo snort -i enp0s3 -c /etc/snort/snort.conf -l /var/log/snort -d -A console > /home/server/log-tele.txt**



Gambar 4.10 perintah untuk mengaktifkan snort

Untuk menjalankan peringatan snort yang terhubung ketelegram dalam dilihat pada gambar 4.10 dibawah ini.

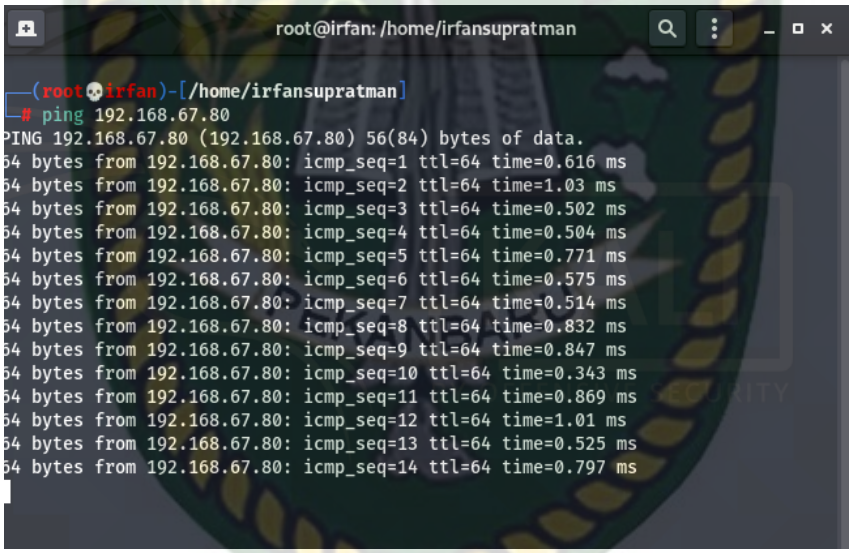


Gambar 4.11 perintah menghubungkan snort ke telegram

4.2 Tahapan pengujian

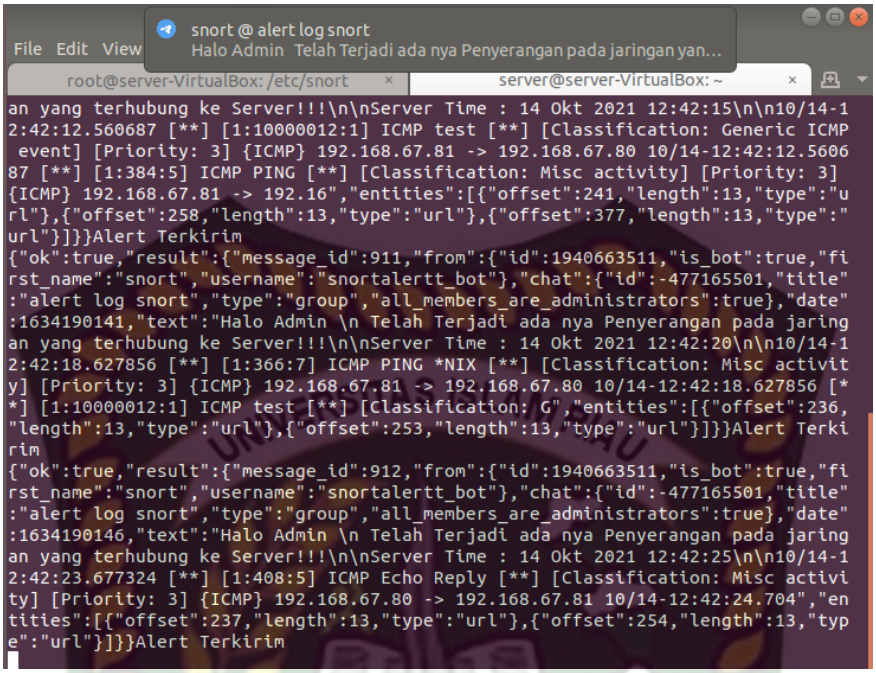
4.2.1 ICMP (Internet Control Message Protocol)

Komputer yang sudah terpasang snort akan mencoba mendeteksi adanya serangan atau aktivitas yang tidak wajar didalam jaringan yang terhubung ke server. ICMP merupakan suatu protokol yang bertugas untuk mengirimkan pesan kesalahan dan kondisi lain yang memerlukan perhatian khusus. Berikut gambar 4.12 dibawah ini merupakan tampilan ping dari jaringan penyerang ke jaringan *client/*korban. Maka jika jaringan *client/*korban yang sudah terpasang snort maka akan tampil snort sebagai pendeteksi(adanya aktivitas ping).



Gambar 4.12 ping *ip address* korban dari penyerang

Pada gambar 4.13 dibawah ini merupakan tampilan di *client/*korban yang sudah terpasang snort maka akan menampilkan *alert* (peringatan) ada aktivitas ping, yang dimana itu dibuat berdasarkan rules snort yang telah dibuat. sehingga akan menampilkan perintah deteksi snort seperti berikut ini pada gambar 4.13:

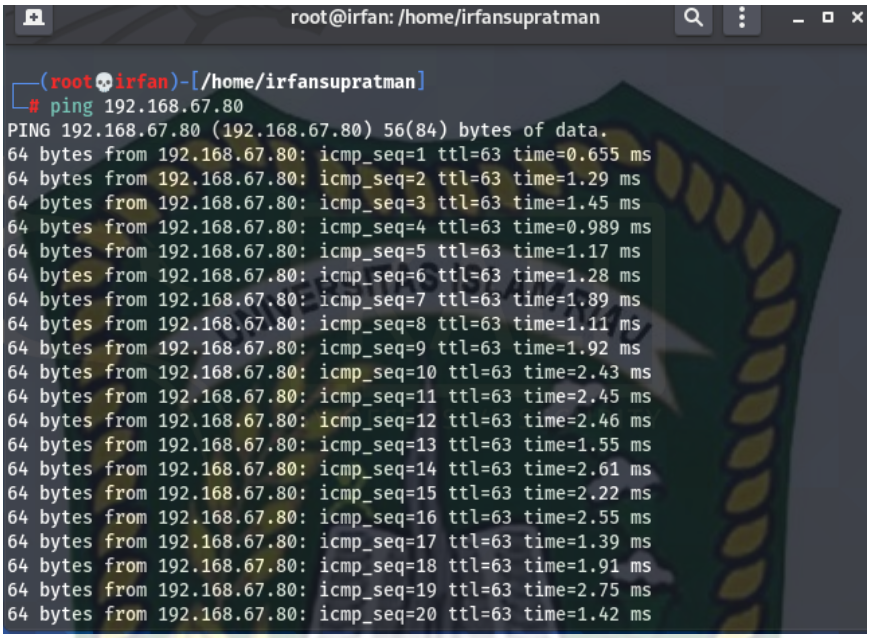


Gambar 4.13 ICMP snort

client yang sudah terpasang snort dapat mendeteksi adanya ping untuk mengetahui apakah sudah terkoneksi atau tidak dengan hasil reply dari 192.168.67.81. setelah snort mendeteksi adanya serangan jaringan, maka snort akan mengirim peringatan kepada administrator melalui aplikasi telegram. Seperti pada gambar 4.14 dibawah ini.

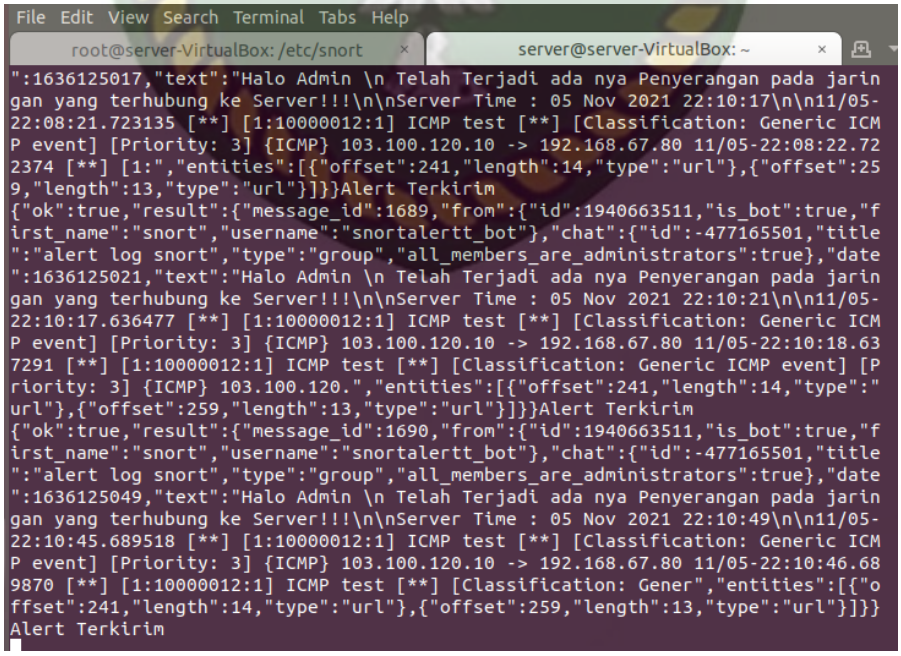
Gambar 4.14 tampilan telegram saat mendapatkan notifikasi serangan ping

Pada gambar 4.15 dibawah ini merupakan percobaan ICMP dari ip yang berbeda. Untuk lebih jelas dapat dilihat pada gambar 4.15 dibawah ini.



Gambar 4.15 ping dari ip address yang berbeda

Pada gambar 4.16 dibawah ini merupakan tampilan saat snort berhasil mendeteksi adanya serangan jaringan dari sistem operasi windows.



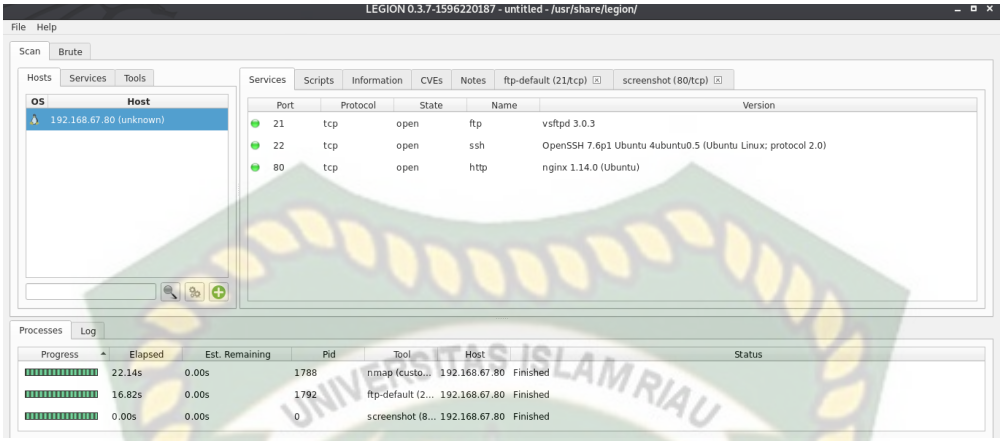
Gambar 4.16 hasil snort mendeteksi adanya serangan

Pada gambar 4.16 diatas dapat dilihat snort berhasil mendeteksi adanya ICMP ke jaringan komputer yang telah terpasang snort. Pada gambar 4.17 dibawah ini merupakan tampilan aplikasi telegram saat mendeteksi adanya serangan dari ip yang berbeda dapat dilihat pada ip yang menyerang 103.100.120.10 melakukan icmp kepada ip 192.168.67.80.

Gambar 4.17 Tampilan telegram saat mendeteksi adanya ICMP dari ip berbeda

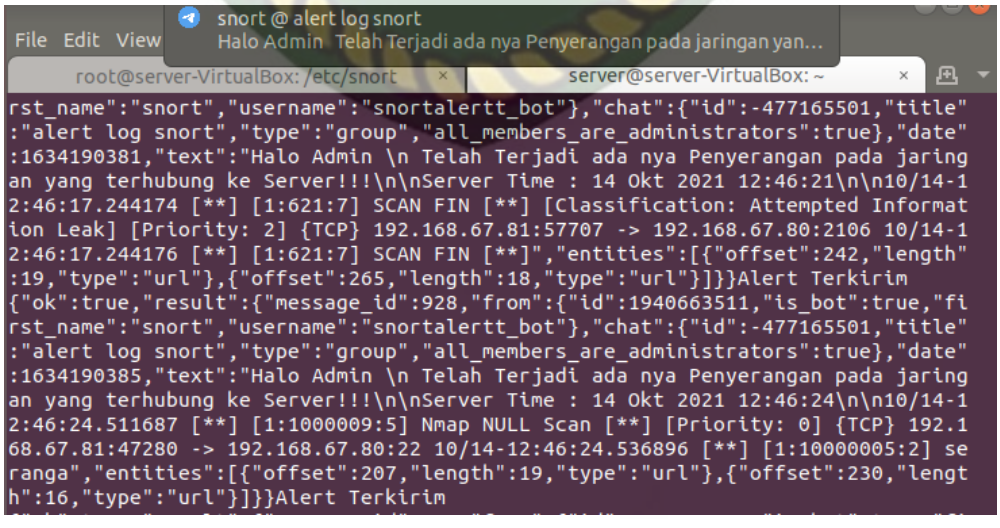
4.2.2 Nmap (*port scanning*)

komputer yang sudah terpasang snort akan dicoba untuk melakukan metode penyerangan nmap yaitu serangan dengan *port scanning* dari komputer penyerang. legion merupakan sebuah aplikasi atau tools yang berguna untuk audit dan eksplorasi suatu keamanan jaringan. Berikut gambar 4.18 dibawah ini aplikasi nmap pada kali linux (legion) untuk melakukan pengujian ke snort apakah snort dapat membaca serangan nmap:



Gambar 4.18 *port scanning* ke ip *client* dengan menggunakan legion

Pada gambar 4.18 diatas dapat dilihat setelah melakukan port scanning ke jaringan *client* maka jaringan *client* memiliki 3 port yang terbuka yang dimana port 21 ftp, 22 ssh dan port 80 http. Sehingga ini merupakan sebuah celah dimana penyerang dapat memasuki atau pun lebih mendalami untuk melakukan penyerangan kedalam jaringan.Pada gambar 4.19 dibawah ini merupakan tampilan linux ubuntu yang telah dipasang snort maka snort akan mendeteksi adanya serangan atau aktivitas yang tidak wajar didalam jaringan. sehingga snort akan menampilkan peringatan pendeteksi snort seperti berikut ini pada gambar 4.19:

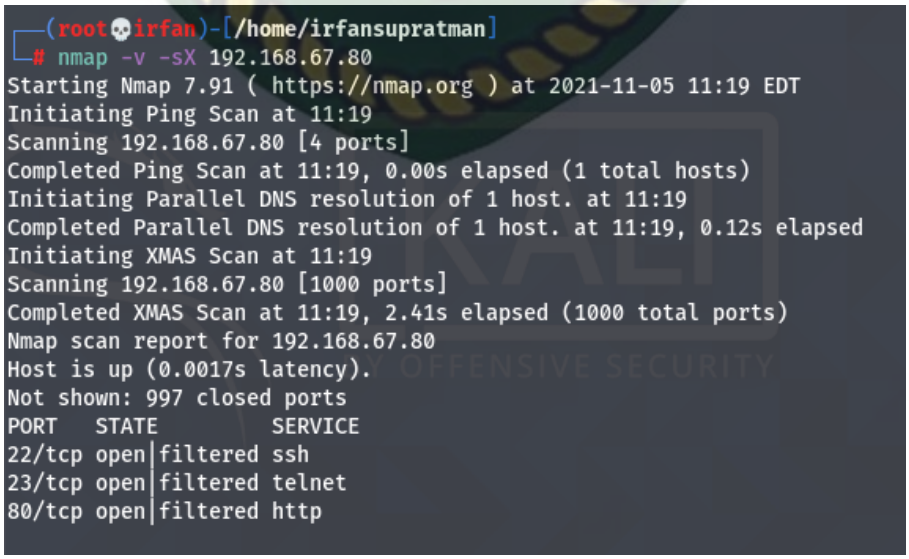


Gambar 4.19 hasil client yang terpasang snort mendeteksi adanya *port scanning*

Setelah snort mendeteksi adanya serangan atau ancaman snort akan mengirimkan peringatan ada nya *port scanning* ke telegram administrator. Seperti pada gambar 4.20 dibawah ini.

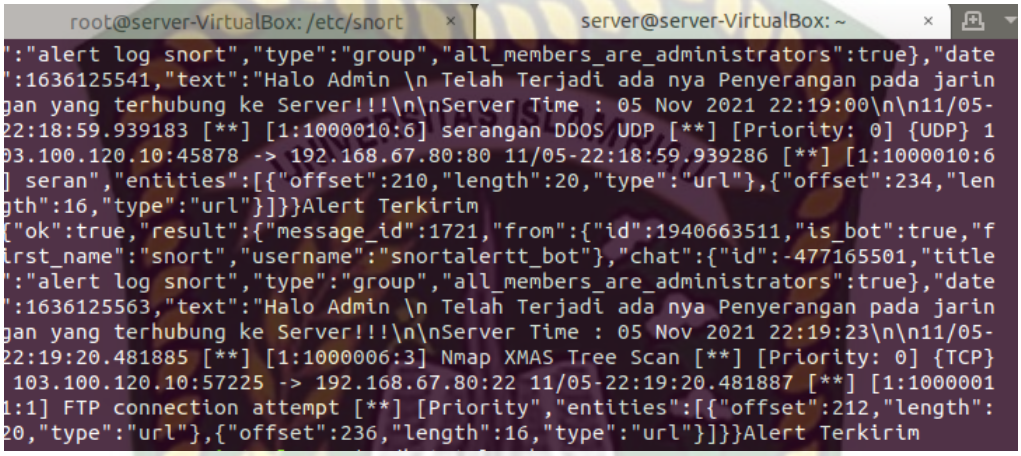
Gambar 4.20 tampilan telegram saat mendapatkan notifikasi serangan port scanning

Pada gambar 4.21 dibawah ini melakukan port scanning dengan nmap menggunakan ip address yang berbeda. Untuk lebih jelas dapat dilihat pada gambar 4.21 dibawah ini.



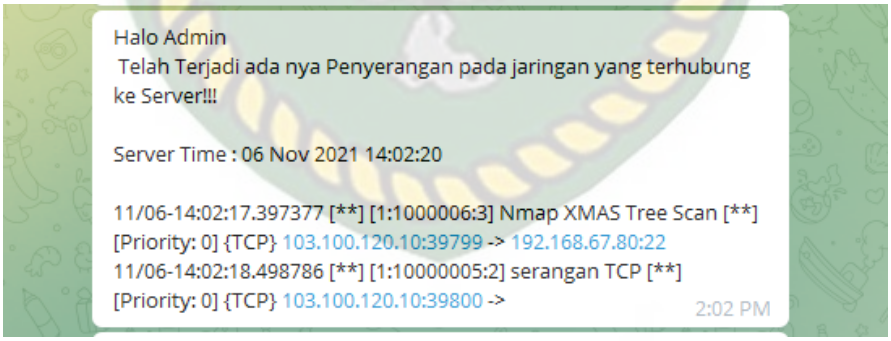
Gambar 4.21 Nmap dari ip address berbeda

Pada gambar 4.21 diatas penyerang berhasil port scanning ke ip address 192.168.67.80. selanjutnya pada gambar 4.22 dibawah ini merupakan tampilan log snort saat mendeteksi adanya sebuah serangan port scanning. Untuk lebih jelas dapat dilihat pada gambar 4.22 dibawah ini.



Gambar 4.22 Nmap dari ip address berbeda

Pada gambar 4.23 dibawah ini merupakan tampilan telegram pada saat pendeteksian snort. Telegram berhasil mendeteksi dan menangkap paket yang dideteksi oleh snort kemudian mengirimkan kepada administrator.



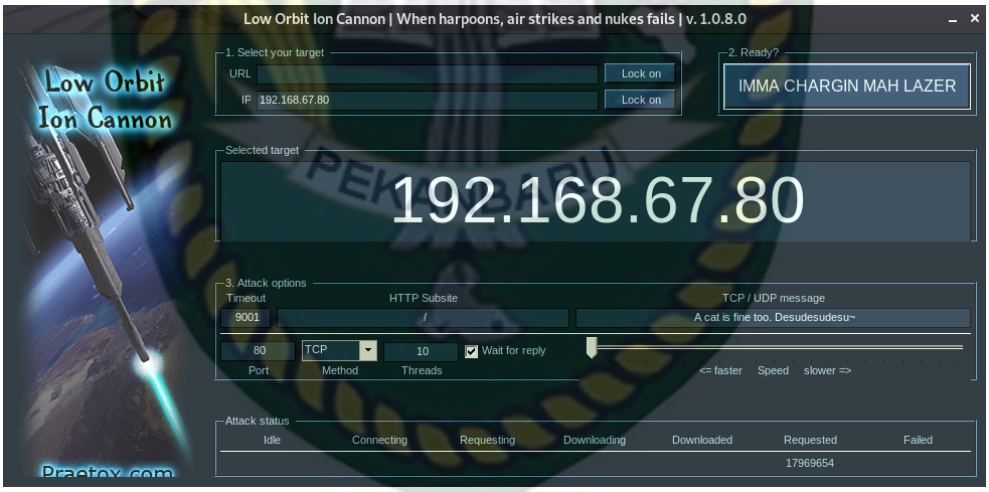
Gambar 4.23 Tampilan telegram dari ip address berbeda

4.2.3 DDOS (Distributed denial of service)

komputer yang sudah terpasang snort akan dicoba untuk melakukan metode penyerangan DDOS yaitu jenis serangan yang dilakukan dengan cara membanjiri lalu lintas jaringan internet yang terhubung server, sistem, atau jaringan.

Berdasarkan dari pengujian sebelumnya menggunakan port scanning, maka akan dilakukan penyerangan dengan pembanjiran lalu lintas jaringan berdasarkan celah atau port yang terbuka tadi. Sehingga dalam penelitian ini dilakukan pengujian sistem keamanan snort yang telah terhubung kedalam jaringan yang meliputi pengujian serangan DDOS dengan metode TCP dan melakukan pengujian serangan DDOS dengan metode UDP.

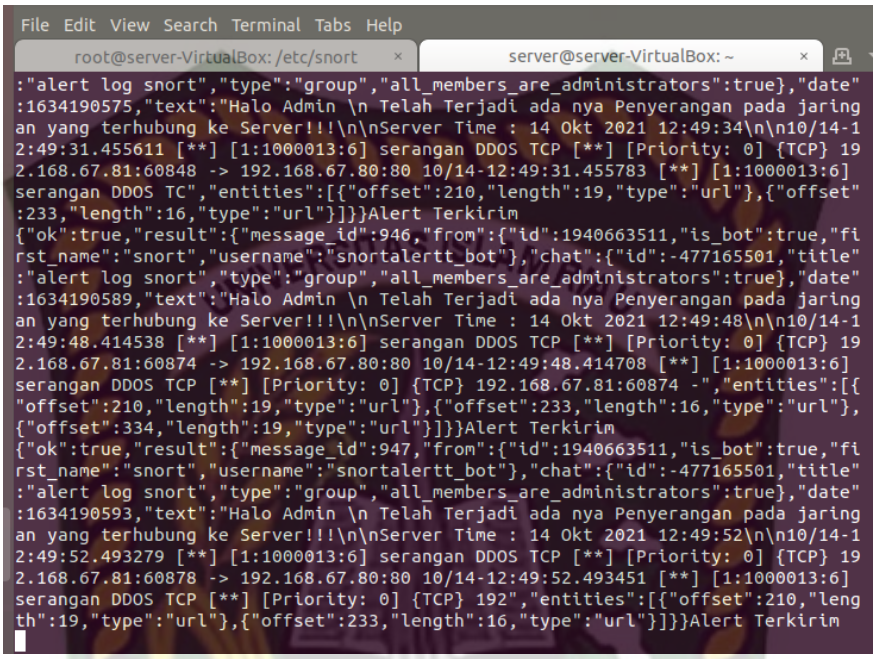
Berikut gambar 4.24 dibawah ini merupakan penyerangan DDOS yang dilakukan dengan menggunakan aplikasi LOIC.EXE dan snort dapat mendeteksi adanya serangan DDOS dan memberikan *alert* (peringat) kepada administrator melalui aplikasi telegram.



Gambar 4.24 aplikasi LOIC melakukan serangan DDOS dengan metode TCP

Pada gambar 4.24 diatas dapat dilihat penyerangan melakukan penyerangan dengan ip *client* dimana dapat dilihat dilakukan penyerangan pada port 80 dengan metode TCP. Pada gambar 4.25 dibawah ini merupakan tampilan snort yang mendeteksi adanya serangan jaringan yang dimana jenis serangan ini merupakan

serangan TCP. Sehingga dapat dilihat snort mendeteksi adanya serangan TCP dan mengirimkan peringatan langsung ketelegram administrator.

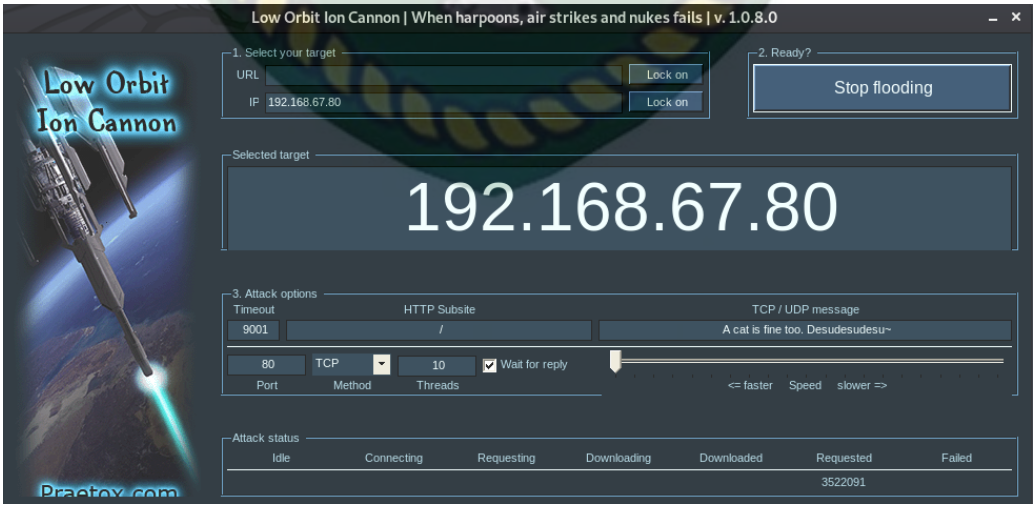


Gambar 4.25 hasil serangan DDOS menggunakan metode TCP

Pada gambar 4.25 diatas setelah snort mendeteksi adanya serangan snort langsung mengirim peringatan kepada administrator melalui aplikasi telegram. Untuk hasil dari serangan TCP snort mengirim peringatan ke administrator telegram dapat dilihat pada gambar 4.26 dibawah ini.

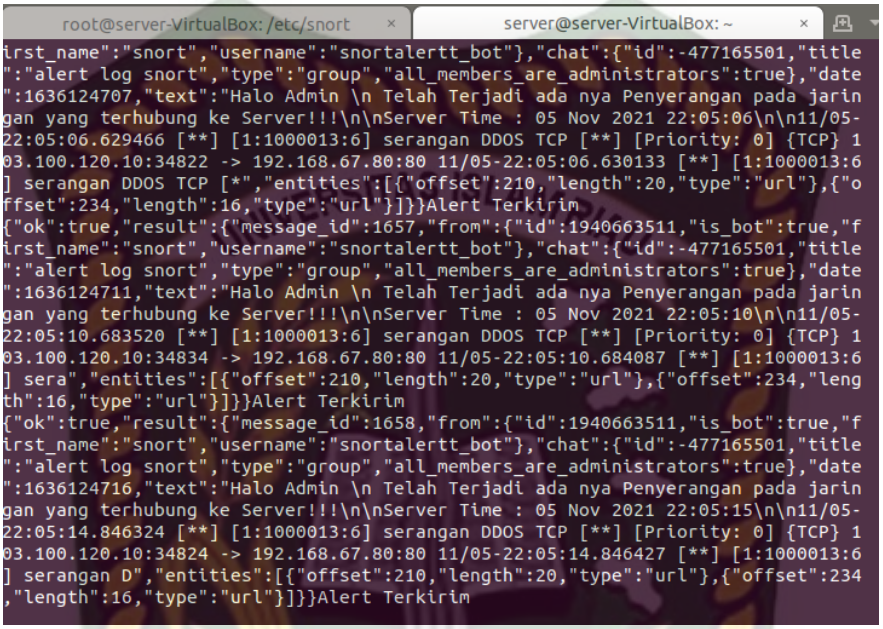
Gambar 4.26 tampilan telegram saat mendapatkan notifikasi serangan metode TCP

Selanjutnya dilakukan percobaan dari ip address berbeda melakukan serangan DDOS tcp dimana jaringan tersebut berhasil membanjiri jaringan server 192.168.67.80. untuk lebih jelasnya dapat dilihat pada gambar 4.27 dibawah ini.



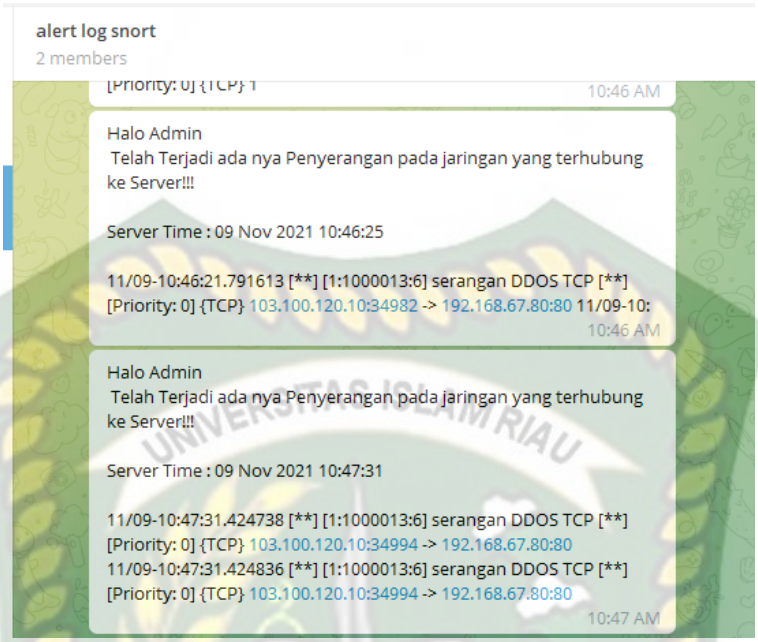
Gambar 4.27 serangan ddos tcp dari ip address berbeda

Pada gambar 4.27 diatas merupakan gambar pada saat attacker melakukan serangan dengan ip address yang berbeda. Pada gambar 4.28 dibawah ini merupakan tampilan snort mendeteksi adanya serangan ddos dengan metode tcp.



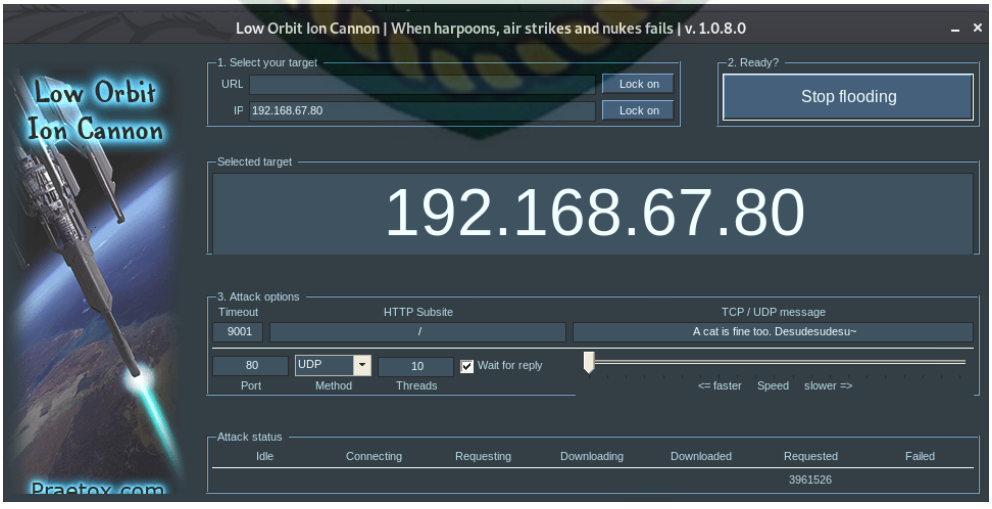
Gambar 4.28 tampilan snort mendeteksi serangan dari ip address berbeda

Setelah snort mendeteksi adanya serangan, snort akan mengirimkan peringat ketelegram administrator. Dimana pada gambar 4.29 dibawah ini merupakan snort berhasil mengirimkan peringatan pendeteksian ke telegram administrator. Untuk lebih jelasnya dapat dilihat pada gambar 4.29 dibawah ini.



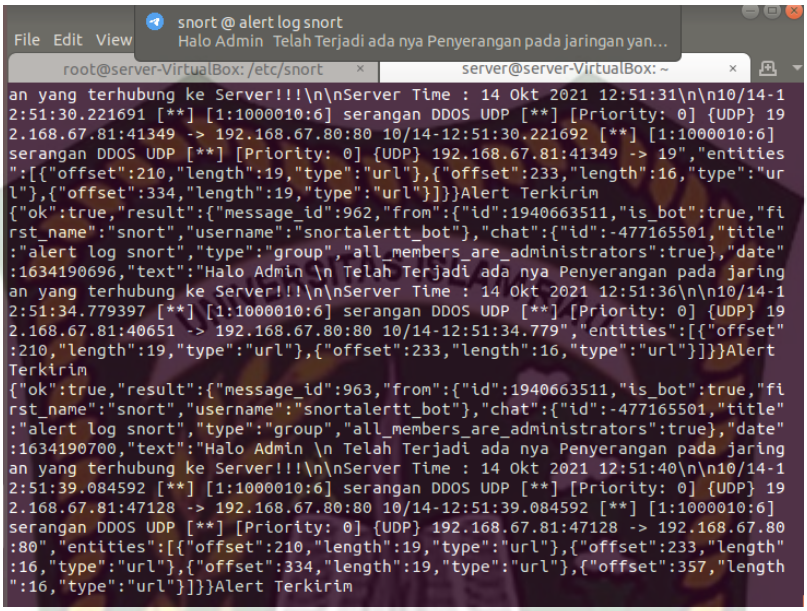
Gambar 4.29 Tampilan telegram mendeteksi adanya serangan dari ip address berbeda

Selanjutnya dilakukan penyerangan DDOS dengan metode UDP ke jaringan yang terhubung ke server. Pada gambar 4.30 dibawah ini merupakan tampilan aplikasi LOIC dalam melakukan penyerangan dengan menyerang menggunakan port 80 dengan metode UDP.



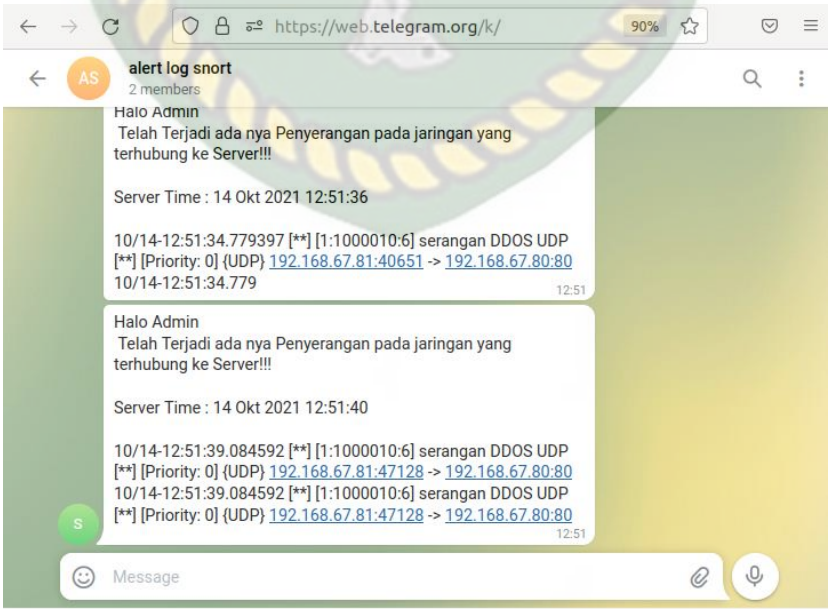
Gambar 4.30 aplikasi LOIC melakukan serangan DDOS dengan metode UDP

Pada gambar 4.31 dibawah ini merupakan tampilan snort yang mendeteksi adanya serangan UDP.



Gambar 4.31 hasil serangan DDOS menggunakan metode UDP

Pada gambar 4.31 diatas snort dapat mendeteksi adanya serangan dengan metode UDP. Pada gambar 4.32 dibawah ini merupakan tampilan telegram saat mendapat peringat dari adanya serangan yang dapat dideteksi oleh snort.

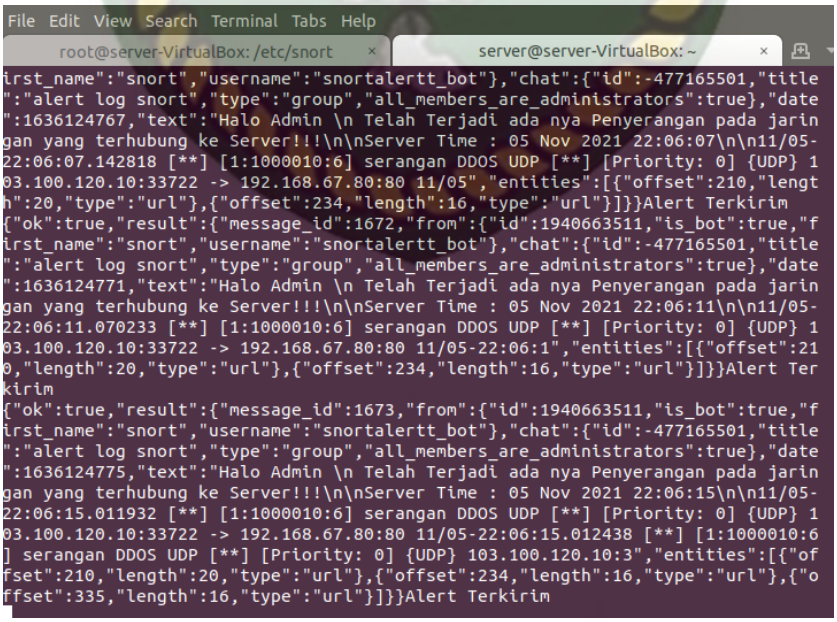


Gambar 4.32 tampilan telegram saat mendapatkan notifikasi serangan metode UDP

Selanjutnya dilakukan penguji serangan ddos dengan metode UDP dari ip address yang berbeda. Untuk lebih jelas dapat dilihat pada gambar 4.33 dibawah ini.

Gambar 4.33 Serangan ddos udp dari ip address berbeda

Setelah melakukan mengirimkan serangan ddos UDP, snort berhasil mendeteksi adanya serangan ddos UDP dari ip address yang berbeda. Untuk lebih jelas dapat dilhat pada gambar 4.34 dibawah ini.

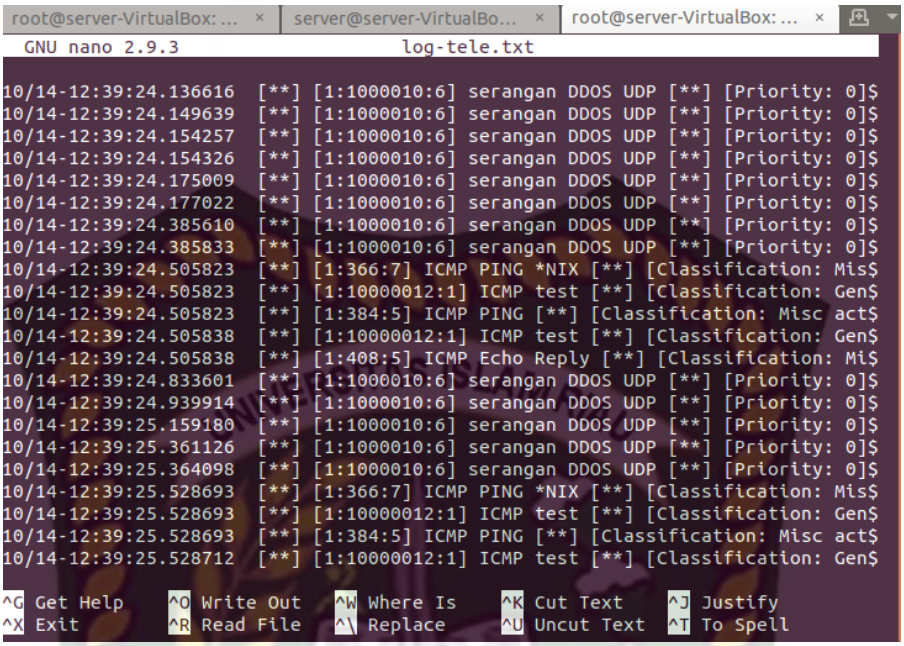


Gambar 4.34 snort mendeteksi UDP dari ip address berbeda

Pada gambar 4.34 diatas snort berhasil mendeteksi adanya serangan ddos UDP snort lanjutnya mengirimkan peringatan ke pada administrator melalui aplikasi telegram. Untuk lebih jelasnya dapat dilihat pada gambar 4.35 dibawah ini.

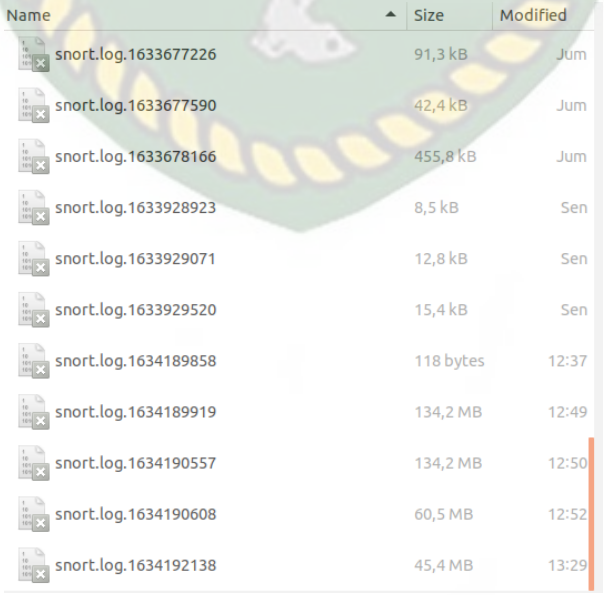
Gambar 4.35 tampilan telegram mendeteksi serangan UDP dari ip address berbeda

Pada gambar 4.36 dibawah ini merupakan tampilan log snort yang disimpan kedalam file log-tele.txt, yang berguna untuk dianalisis dikemudian hari oleh administrator.



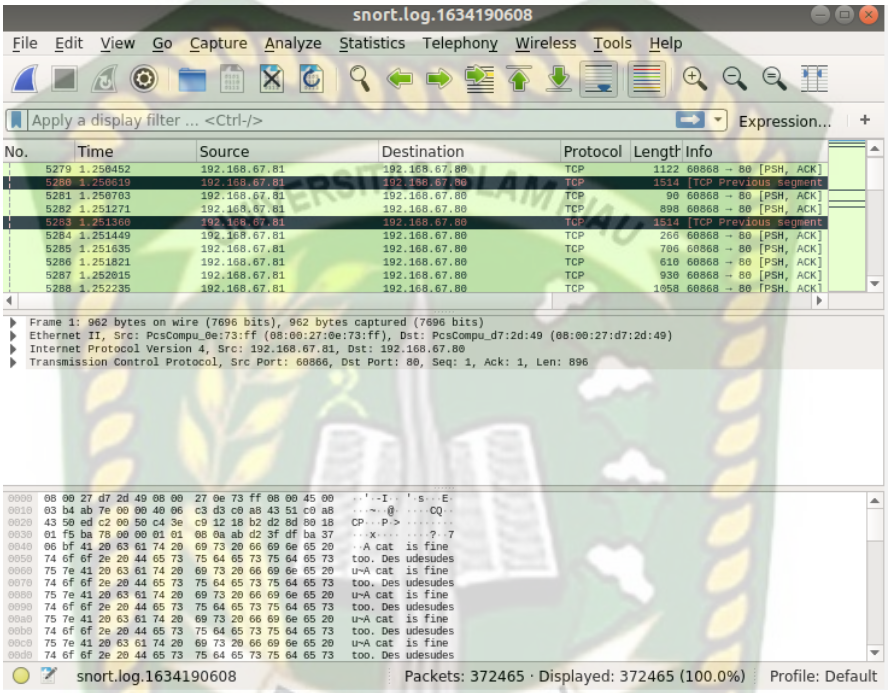
Gambar 4.36 tampilan log-tele.txt

Pada gambar 4.36 diatas merupakan tampilan dari serangan yang tersimpan di log snort kemudian dapat dibaca file log-tele.txt untuk dapat dibuka pada setiap 1 hari penyerangan. Pada gambar 4.37 dibawah ini merupakan tampilan file log snort secara keseluruhan yang tersimpan kedalam komputer administrator.



Gambar 4.37 tampilan file log snort keselurahan dikomputer admin

Pada gambar 4.38 dibawah ini untuk melihat serangan yang tersimpan log snort untuk dianalisis secara detail dikemudian hari dapat membuka file log snort di wireshark. Untuk lebih jelas dapat dilihat pada gambar 4.38 dibawah ini.



Gambar 4.38 tampilan log snort di wireshark

4.3 Hasil pengujian

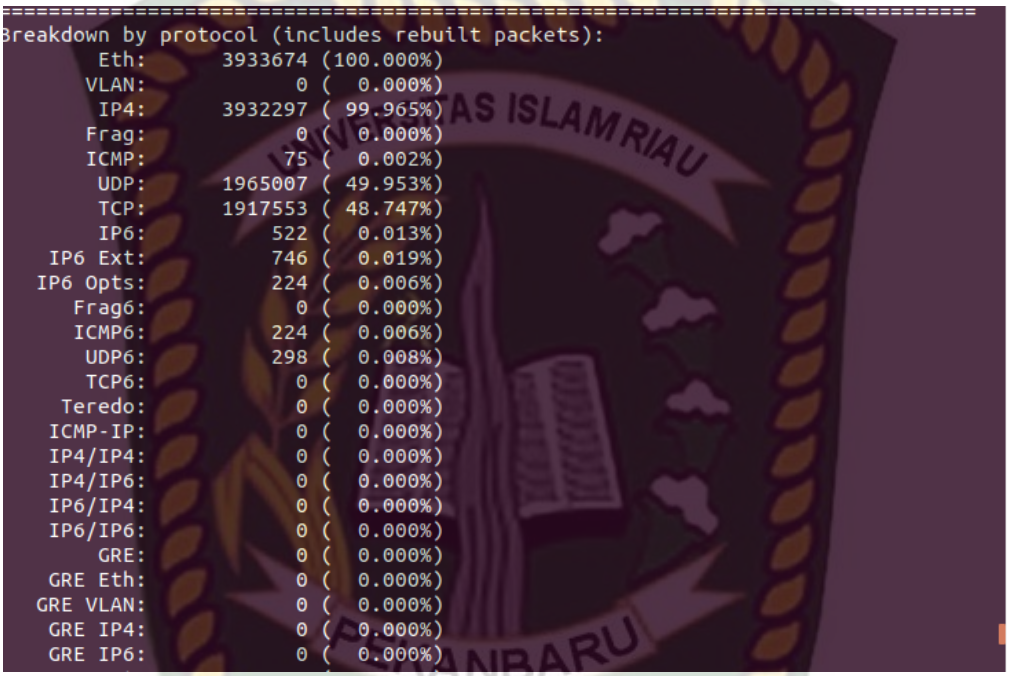
4.3.1 Analisis Snort

Pada hasil pengujian menggunakan snort terbukti bahwa snort dapat melakukan pendeteksian adanya aktivitas jaringan yang tidak wajar. Dimana pada gambar 4.39 dibawah ini merupakan analisis dari snort itu sendiri terhadap adanya serangan-serangan.

```
Packet I/O Totals:
   Received:      9102200
   Analyzed:      3933531 ( 43.215%)
    Dropped:      5168668 ( 36.218%)
   Filtered:            0 (  0.000%)
Outstanding:      5168669 ( 56.785%)
   Injected:            0
```

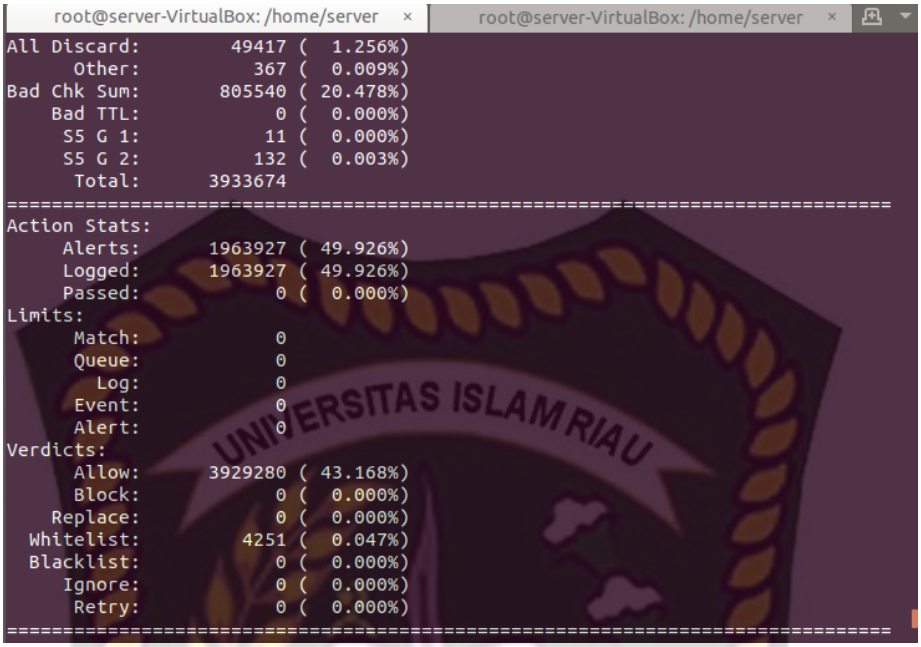
Gambar 4.39 Analisis snort

Dapat dilihat pada gambar 4.39 diatas ini snort yang menangkap sejumlah serangan dari peyerang ke *client* selama 30 menit. Dimana snort menerima paket 9102200 dan snort menganalisis paket serangan sehingga menghasilkan (43,215%) dan paket yang jatuh sebesar (36,218%).



Gambar 4.40 analisis detail packet snort

Pada gambar 4.40 diatas dapat dilihat merupakan analisis dari paket detail snort yang dimana snort merekam untuk penyerangan atau ancaman yang berada dijaringan. Untuk serangan atau ancaman ICMP snort dapat sebanyak 75 dengan presentasi (0,002%). Dan untuk penyerangan dengan metode TCP sebanyak 1965007 dengan presentase (49,953%). Dan untuk penyerangan dengan metode UDP sebanyak 1917553 dengan presentase (48,747%).



Gambar 4.41 analisis total snort

Pada gambar 4.41 diatas dapat dilihat total snort mereka sebanyak 3933674. Dengan aksi status snort mengirim peringatan sebanyak 1963927 dengan presentase (49,926%).

4.3.2 Hasil Monitoring CPU client

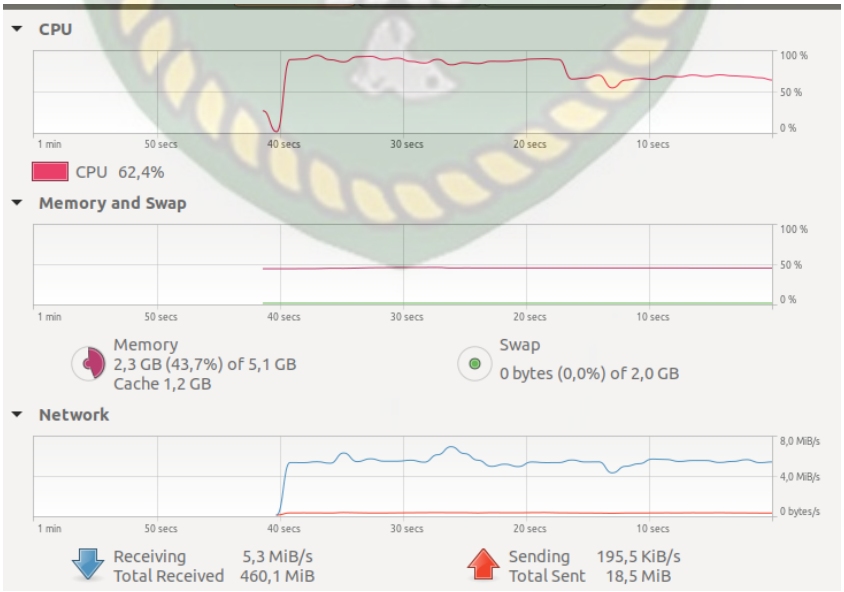
1. Saat belum terjadi penyerangan

Pada gambar 4.42 dibawah ini merupakan tampilan CPU *client* saat sebelum terjadi penyerangan. Dapat dilihat pada CPU *history dan network history* CPU masih berjalan seperti biasa.

Gambar 4. 42 CPU Server Saat tidak terjadi penyerangan

2. Saat terjadinya penyerangan metode TCP

Pada gambar 4.43 dibawah ini merupakan tampilan CPU saat terjadi pada penyerangan DDOS dengan metode TCP.

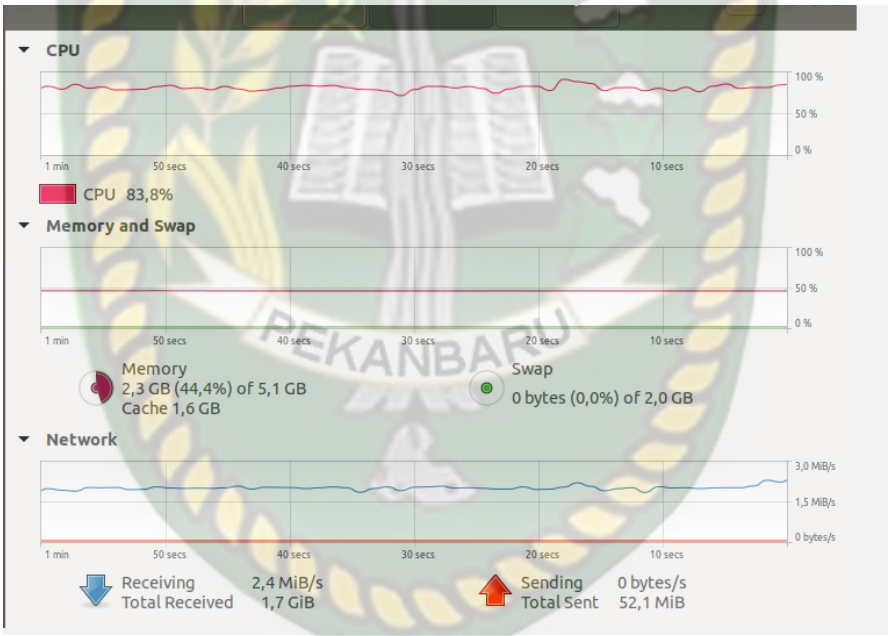


Gambar 4. 43 Tampilan CPU pada saat penyerangan dengan metode TCP

Pada gambar 4.43 diatas dapat dilihat pada CPU *History* mengalami kenaikan pada saat tidak adanya penyerangan CPU berjalan diangka 22% dan pada saat terjadinya penyerangan metode TCP CPU *History* meningkat mencapai angka tertinggi 50% - 75%. Dan untuk network *history* data yang diterima 5,3 Mib/s dengan total 460,1 MiB.

3. Saat terjadi penyerangan metode UDP

Pada gambar 4.44 dibawah ini merupakan tampilan CPU *history client* saat terjadi penyerangan dengan menggunakan metode UDP.



Gambar 4.44 Tampilan CPU pada saat penyerangan dengan metode UDP

pada gambar 4.44 diatas CPU *History* mengalami kenaikan saat terjadinya penyerangan, CPU *History* meningkat mencapai angka tertinggi 70% - 90%. Dan untuk network *history* data yang diterima 2.4 Mib/s dengan total 1,7 GiB dan data yang terkirim 0 byte/s dengan total 52,1 Mib.

4.3.3 Hasil Penetration test

Hasil dari metode *penetration test* secara keseluruhan dari waktu pengujian keamanan jaringan LAN (local area network) di labor Teknik informatika universitas islam riau pada tanggal 14 Oktober 2021 – 9 November 2021. dapat dilihat pada tabel dibawah ini.

Tabel 4.2 waktu pengujian

NO	Jenis serangan	Waktu		
		Awal serangan	Waktu terdeteksi	Terkirim
1.	ICMP	12:42:50	12:42:51	12:42:52
2.	Port scanning	12:46:14	12:46:17	12:46:21
3.	Ddos attack aplikasi LOIC	12:50:10	12:50:12	12:50:17

Pada saat penyerangan dengan ip address berbeda membutuhkan waktu yang sedikit agak lama dalam pendeteksian nya. Untuk lebih jelas dapat dilihat pada tabel 4.3 dibawah ini.

Tabel 4.3 waktu pengujian dengan ip address berbeda

NO	Jenis serangan	Waktu		
		Awal serangan	Waktu terdeteksi	Terkirim
1.	ICMP	10:36:05	10:37:11	10:37:14

2.	Port scanning	14:01:48	14:02:17	14:02:20
3.	Ddos attack aplikasi LOIC	10:46:49	10:47:21	10:47:25

Sehingga hasil penetration test dalam pengujian dapat dilihat pada tabel dibawah ini.

Tabel 4.4 hasil pengujian

NO	Jenis serangan	Hasil pengujian sistem	Kesimpulan
1.	ICMP (linux)	Terdeteksi	Berhasil
2.	Port Scanning (NMAP)	Terdeteksi	Berhasil
3.	Ddos menggunakan aplikasi LOIC(kali linux)	terdeteksi	Berhasil

Dapat dilihat pada tabel diatas seluruh pengujian mendapatkan hasil yang sesuai dengan yang diharapkan. Sistem dapat mendeteksi adanya serangan yang dilakukan attacker, pendeteksian serangan sesuai dengan yang dibuat mulai dari ICMP, *port scanning, Ddos attack.*

BAB V

SIMPULAN DAN SARAN

5.1 Simpulan

Berdasarkan hasil pengujian dari bab IV penulis menarik simpulan sebagai berikut ini.

1. Snort dapat mendeteksi serangan-serangan jaringan mulai dari ICMP, NMAP, Serta serangan DDOS yang dimana serangan DDOS dengan metode TCP dan UDP sehingga menghasilkan dampak pada CPU Komputer secara berlebihan.
2. Metode *Intrusion Detection System* merupakan metode yang dapat mengoptimalkan tingkat keamanan jaringan komputer melalui pendeteksian serangan sehingga administrator dapat melakukan Tindakan penyegahan.
3. Snort terbukti dapat melakukan analisis terhadap serangan-serangan jaringan.
4. Pada komputer yang tidak terpasang snort, maka komputer itu tidak dapat untuk mengetahui apa-apa saja yang terjadi pada komputer yang sedang diserangan.

5.2 Saran

Dalam penelitian ini penulis berharap penelitian ini dapat ditingkatkan lagi bukan hanya dalam skala jaringan LAN tetapi dapat pada skala jaringan MAN dan

WAN. Serta penulis berharap penelitian ini dapat terus dikembangkan mulai dari rules snort itu sendiri serta dapat untuk memperbarui rules secara otomatis dan Sistem IDS ini dapat untuk memblokir serangan secara otomatis. Dan *Intrusion Detection System* merupakan metode yang tepat dalam melakukan pendeteksian serangan jaringan. Dan penulis berhadap penelitian ini dapat dikembangkan lagi terutama untuk peringatan peringatan ke aplikasi telegram supaya dapat secara otomatis memberi peringatan tanpa pengaktifkan snort dilinux ubuntu terlebih dahulu.

DAFTAR PUSTAKA

AGITA SYAIMI PUTRI UTAMI, L. L. (2013). Perancangan Dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort Ids Dan Honeyd. *Jurnal Reka Elkomika*, 317-327.

Akbar, M. (2018). Perancangan Software Ids Snort Untuk Pendeteksian (Netcut) Serangan Interruption Pada Jaringan Wireless. *Jurnal Instek (Informatika Sains Dan Teknologi)*, 121–129.

Aliy Hafiz, T. K. (n.d.). Analisis Celah Keamanan Jaringan Dan Server Menggunakan . *Stmik Dian Cipta Cendikia Kota Bumi* , 59-66.

Arta, Y. (2017). Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal. *IT Journal Research and Development*, 43-50.

Arta, Y. S. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *It Journal Research and Development*, 94–104.

Barany Fachri, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan Dan Komputer. *Jurnal Media Informatika Budidarma*, 413-420.

Corporation, S. (2017). *Norton Cyber Security Insights Report Global Results.*

eddypn, e. (2019). Sistem reporting keamanan pada jaringan cloud computing melalui bot telegram dengan menggunakan teknik intrusion detection system and prevention system. *Jurnal teknologi terpadu*, vol.5,no 2.

Fathoni, W. F. (2016). Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort. *E-Proceeding of Engineering*, 1169–1172.

Febrison, Y. (Nov 2020). Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan Security . *Journal of Information System and Technology*, Vol.01 No.02,37-61.

Harahap, M. H. (2018). Implementasi Snort Intrusion Detection System (IDS) Pada Sistem Jaringan Komputer. *Informatika : Fakultas Sains dan Teknologi*, vol 6. No.3.

Indonesia, A. -A. (2020). *Statistik Pengguna internet di Indonesia*. Retrieved from https://www.apjii.or.id/survei/download/survei-APJII-2019-2020 (Q2)

Manuaba, I. B. (2012). Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas). *Jnteti*, 5.

Rahim, A. (2016). Rancang Model Sistem Keamanan Menggunakan Intrusion Prevention System Dengan Prevention System Dengan Kasus KPDE Provinsi Jambi . *Jurnal Ilmiah Media SISFO*, 190–205.