Journal of Information System and Technology, Vol.01 No.02, Nov 2020, pp.37-61
ISSN: -

Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan *Security Onion* Dan *Mikrotik*

Febrison Yohaness[1], Haeruddin[2]
Sistem Informasi, Fakultas Ilmu Komputer, Universitas Internasional Batam, Sei Ladi, Jl. Gajah Mada, Baloi Permai, Kec. Sekupang, Kota Batam, Kepulauan Riau 29442
Email : febrison@uib.ac.id, haeruddin@uib.ac.id

Abstrak

Dengan kemajuan teknologi pada era digitalisasi ini, hampir semua aspek dan bidang telah menerapkan teknologi informatika dalam sistem kerja perusahaan, akan tetapi masih terdapat celah keamanan yang dapat menyebabkan terjadinya *cyber crime*. Tujuan dari penelitian proyek ini adalah untuk memberikan menganalisa serta merancang sebuah sistem yang dapat mencegah ataupun menanggulangi masalah *cyber crime*. Metode pengujian yang digunakan dalam proyek ini adalah *Penetration Test* pada jaringan virtualisasi dan terhubung ke jaringan lokal. Hasil akhir dari proyek ini adalah sebuah sistem yang dikombinasikan dengan perangkat *MikroTik* untuk mengawasi serangan yang masuk ke dalam jaringan lokal. Sistem keamanan yang digunakan adalah *Security Onion*.

Kata Kunci: Jaringan Lokal, *MikroTik*, *Security Onion*, *cyber crime*, Keamanan Jaringan Lokal

Abstract

With the advancement of technology on this digitalized era, almost every aspect and field has implemented information technology in the work system of companies, yet there are still security gaps that can lead to cybercrime. The purpose of this research is to both provide an analysis and design a system that can prevent and tackle cybercrime issues. The testing method used in this project is Penetration Test on network virtualization and is connected to local network. The end result of this project is a system that is fused with MikroTik software to monitor attacks to the local network. The security system used is Security Onion.

***Keywords**: Local Network, MikroTik, Security Onion, cybercrime, Local Network Security*

I. PENDAHULUAN

Jaringan *internet* mempunyai manfaat yang sangat banyak dan mencakup banyak aspek baik itu dalam aspek kehidupan ataupun aspek dari suatu bidang. Jaringan *internet* ini dapat memasimalkan komunikasi dari segi kecepatan dan keefektifan untuk melakukan komunikasi tersebut, baik itu antara perorangan, perusahaan ataupun antar negara. Jaringan *internet* berperan besar dalam peningkatan kualitas dan kuantitas serta perkembangan yang pesat dari semua bidang yang ada didunia ini. (Riadi, 2014)

Pada tahun modern era digital ini, jaringan *internet* telah banyak dipakai secara masal di dalam banyak organisasi dan juga pada beberapa perusahaan. Kemudahan dan keefektifan akses serta juga kecepatan transfer data menjadi faktor yang menarik khalayak ramai untuk menggunakan jaringan *internet*. Namun,

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

kemunculan masalah keamanan pada jaringan-jaringan *internet* yang ada di dunia menjadi suatu ancaman terhadap proses berkembangnya jaringan *internet*. (Heru, Benny, Defendy, & Hento, 2014)

Untuk mengamankan jaringan internet ada banyak caranya. Salah satu cara yang dapat digunakan adalah dengan menerapkan system pendeteksian penyusupan Jaringan atau *Instrusion Detection System* (IDS). IDS adalah sebuah operasi untuk mendeteksi adanya ancaman yang terjadi pada jaringan komputer seperti pencurian data, informasi dan pengerusakan system oleh *hacker*. Salah satu aplikasi berbasis IDS yang dapat digunakan dalam pengamanan jaringan adalah SNORT. SNORT adalah perangkat lunas atau *software open-souce* yang bebas digunakan dan dimodifikasi sesuai dengan kebutuhan. (Fathoni, Fitriyani, & Nurkahfi, 2016).

Oleh karena itu sesuai dengan penjelasan yang telah dijabarkan diatas penulis melakukan penelitian yang mengambil subjek bagaimana cara meningkatkan keamanan jaringan dengan menggunakan *Security Onion* yaitu SNORT dan menggunakan MikroTik Router sebagai *gateway* jaringan internet yang diteliti tersebut. Penelitian ini berjudul "**Analisa dan Perancangan Keamanan Jaringan Lokal Menggunakan *Security Onion* dan *MikroTik***".

Tujuan Proyek ini dilaksanakan berdasarkan atas beberapa pertimbangan yang sudah dipikirkan dengan matang oleh penulis, tujuannya antara lain:

1. Meningkatkan sistem keamanan jaringan lokal dari adanya serangan menggunakan *Security Onion* dan MikroTik Router.
2. Memperluas wawasan ilmu serta pengetahuan dengan cara proses merancang sebuah sistem pendeteksi serangan yang akan datang dari luar jaringan.
3. Membantu penulis untuk mempratekkan ilmu pengetahuan yang penulis dapatkan dari perancangan keamanan jaringan lokal dari serangan DDOS menggunakan *Security Onion* dan MikroTik Router.

Selain mempunyai tujuan, proyek ini juga memiliki manfaat yang ditujukan kepada setiap aspek dan bidang, yaitu:

1. Mengedukasi masyakarat terutama kalangan petinggi perusahaan, instansi, institusi pendidikan tinggi dan instansi lainnya dalam memakai jaringan lokal tentang pentingnya sistem keamanan yang tedapat di jaringan lokal yang digunakan.
2. Memberi himbauan atau informasi terhadap khalayak umum atau kaum awam salah satunya pada karyawan perusahaan manufaktur, instansi pemerintahan, institusi pendidikan tinggi dan bagian lainnya tentang sistem keamanan pada jaringan lokal dan serangan jaringan lokal serta solusi yang dapat dilakukan.
3. Meningkatkan pengetahuan terkait keamanan jaringan lokal dan seragan DDOS menggunakan *Security Onion* dan *MikroTik Router*.

II. TINJAUAN PUSTAKA

Penelitian yang berjudul "Simulasi Implementasi *Intrusion Prevention System* (IPS) Pada Router Mikrotik" yang dilakukan di Universitas Islam Riau (Arta, Syukur, & Kharisma, 2018) menjadi dasar penelitian ini. Hasil dari penelitian yang dilakukan mereka menyimpulkan bahwa serangan atau penyusupan yang digunakan untuk simulasi pada penelitian ini dapat

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

dicegah dengan menerapkan *Intrusion Prevention System* (IPS). Serangan terdetesi dengan cara selalu melakukan pembaharuan dari *filter rules* pada IPS. *Log* dari router MikroTik yang dikombinaasikan dengan IPS terbukti bekerja secara maksimal untuk mendeteksi serangan yang terjadi pada penelitian ini.

Penelitian yang dilakukan oleh (Muhartin, 2017) yang berjudul "Implementasi Sistem Monitorin Jaringan Wireless Dengan Metode Network Security Monitoring (NSM)" menyimpulkan bahwa kebutuhan yang terdapat pada *management* jaringan dari suatu komputer dapat menjadi prioritas, karena jaringan yang terdapat pada komputer tersebut bisa dipakai dan difungsikan secara optimal. *Monitoring traffic* atau pengawasan pada jaringan menjadi salah satu proses yang wajib dilaksanakan pada *management* jaringan. *Network Security Monitoring* (NSM) merupakan suatu metode yang dipakai untuk *monitoring* jairngan. Dalam proses berjalannya, NSM terdiri *collaborative tools* dari Snort, Bro, CapMe, Elsa, Barnyard2, Squert dan Squil. Snort, Bro, CapMe berfungsi sebagai mesin penangkap paket *traffic* jaringan. Squil dipakai untuk mengolah informasi yang ada di dalam perangkat-perangkat keras jaringan . Prosesnya dapat berjalan secara *automatic* ataupun *manual*. Laporan hasil pengawasannya akan ditampilkan secara baik sehingga mudah dipahami salah satu contohnya dengan cara laporan grafik atau *traffic fluctuation*.

Dalam satu contoh kasus yang terdapat pada penilitian (Syaimi, Utami, Lidyawati, & Ramadhan, 2013) yang berjudul "Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd" menjelaskan bahwa kelemahan atau celah yang ada pada sistem 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. Oleh karena ini penelitian bertujuan untuk mencari solusi untuk melakukan tindakan pencegahan dan perlindungan dari penyerangan yang dilakukan penyusup dengan memakai aplikasi Snort IDS dan Honeyd. Cara kerja Snort IDS adalah dengan cara mendeteksi serangan yang akan datang ataupun yang telah dilaksanakan oleh *intruder*. Setelah penyerangan tersebut berhasil dideteksi oleh Snort IDS, selanjutnya dilakukan pencegahan dengan cara 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%. Setelah dilaksanakannya proses deteksi serangan dan pembelokkan serangan, sistem *server* telah bekerja dengan aman dan lancar mengamankan jaringan pada komputer yang terhubung.

Pada penelitian yang dilakukan oleh (Rahim, 2016) yang berjudul "Rancang Model Sistem Keamanan Menggunakan *Intrusion Prevention System* dengan metode *Rule Based*: Studi Kasus KPDE Provinsi Jambi" menjelaskan bahwa sistem yang terdapat di dalam keamanan jaringan sebuah komputer, dalam sepuluh tahun terakhir ini sudah menjadi prioritas utama di dalam bidang jaringan komputer, ini terjadi karena disebabkan oleh laporan meningkatnya ancaman yang diterima bersifat mencurigakan dan juga adanya serangan internal maupun eksternal dari Internet. Keamanan jaringan pada sebuah

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

komputer merupakan salah satu aspek yang bisa mempengaruhi secara masif tingkat reliability, termasuk performance dan availability pada suatu internetwork. Ancaman pada suatu jaringan komputer dapat berasal dari jaringan itu sendiri maupun dari jaringan internet, hal ini dapat disebabkan karena terdapat sumber daya yang bersifat publik sehingga untuk menjaga sumber daya yang ada pada jaringan komputer tersebut dibutuhkan suatu sistem khusus agar jaringan serta layanan-layanan yang terdapat pada jaringan tersebut tetap dapat digunakan dengan baik. Hasil dari penelitian ini berupa sistem pencegah penyusup (IPS) yang dapat meningkatkan keamanan sumber daya jaringan komputer dari ancaman baik yang berasal dari jaringan internet maupun intranet.

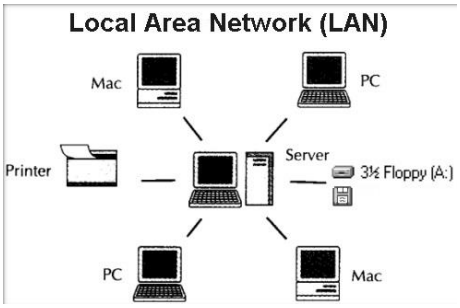
Pada penelitian yang berjudul "Perancangan *Software IDS SNORT* untuk pendeteksian serangan *Interruption (Netcut)* Pada Jaringan *Wireless*" yang dilakukan oleh (Akbar, 2018) menjelaskan bahwa Perancangan software IDS jenis SNORT ini berfungsi untuk melakukan pendeteksian serangan interruption, yang tujuannya adalah mendeteksi serangan terhadap jaringan WiFi atau wireless. Metode yang digunakan adalah perancangan software IDS yang bekerja dengan memantau berkas-berkas sistem operasi, yakni dengan cara melihat apakah ada percobaan untuk merubah berkas-berkas sistem operasi, utamanya berkasi file log. Hasil dari penelitian ini adalah software IDS yang dapat diinstal langsung ke komputer, baik dengan sistem operasi Linux maupun Windows, sehingga serangan dengan teknik interruption dapat dideteksi.

2.2 Landasan Teori

a. Jaringan Komputer

Jaringan komputer pada umumnya diartikan sebagai kombinasi dari perangkat keras atau disebut juga *hardware*, perangkat lunak atau disebut juga *software*, dan perangkat jaringan lainnya baik itu perangkat keras atau lunak. Semua perangkat tersebut memliki banyak fungsi, salah satunya adalah untuk mengkoneksikan atau menyambung komunikasi dari si pengirim dengan si penerima dengan memakai metode kabel ataupun nirkabel (Saputra, Irawan, & Ilhamsyah, 2014). Tiga jenis jaringan komputer berdasarkan lokasi geografisnya, yaitu:

Area Jaringan Lokal atau istilah dalam bahasa Inggris *Local Area Network* (LAN) adalah jaringan komputer yang secara geografisnya hanya mencakup area kecil saja, dengan contoh seperti jaringan yang ada di dalam sebuah kampus, sebuah gedung, satu perusahaan kantor dengan dengan kecepatan atau *speed* komunikasi dan pengiriman datanya hingga 1000 Mbit/s. (Varianto & Badrul, 2015). Gambar dari jaringan LAN dapat dilihat berikut dari Gambar 2.1:

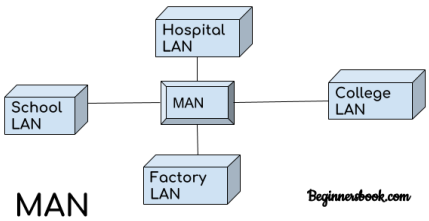


Gambar 2.1 Gambaran dari bentuk jaringan *LAN*

MAN atau kepanjangannya *Metropolitan Area Network* adalah jaringan yang memiliki cakupan area yang lebih luas dari LAN. Cakupan yang semakin luas juga menambah kecepatan dari komunikasi dan kecepatan data daripada yang dapat dilakukan oleh jaringan LAN. (Lukman, 2016). Cakupan area yang

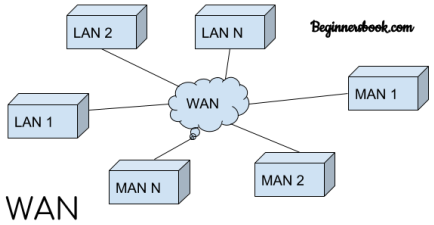
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

dapat dicapai oleh MAN dapat dilihat dari Gambar 2.2:



Gambar 2.2 Metropolitan Area Network (MAN)

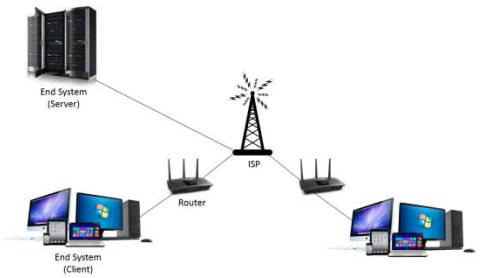
Jika dari lihat cakupan area LAN dan MAN, terdapat jaringan yang memiliki cakupan area lebih luat daripada kedua jaringan tersebut, yaitu *Wide Area Network* (WAN). Jaringan ini biasanya digunakan untuk mencakup daerah yang tingkatnya hingga wilayah, antar kota, antar provinsi ataupun antar negara ataupun sesama negara tetangga. Biasanya metode yang digunakan sudah menggunakan bantuan satelit dan perangkat yang pemancarnya lebih besar. (Chelara & Hermanto, 2014). Berikut gambaran WAN dengan cakupan areanya yang ada pada Gambar 2.3:



Gambar 2.3 Wide Area Network (WAN)

b. *Internet*

Internet biasanya atau pada umumnya menggunakan konsep jaringan global atau secara istilah biasa jaringan dunia yang dapat menghubungkan satu jaringan dengan jaringan lainnya, jaringan pribadi ataupun jaringan yang berbasis perusahaan diseluruh dunia melalui media yang disebut dengan *server* yang memanfaatkan aturan komunikasi pengiriman dan penerimaan data atau komunikasi yang telah disetujui bersama. Sehingga tidak terjadi tabrakan antar jaringan yang ada di dalam dunia *Internet* (Nurdin, 2015). *Internet* dapat dilihat pada Gambar 2.4:



Gambar 2.4 Internet

c. Topologi Jaringan

Topologi jaringan atau dalam bahasa Inggris disebut *Network Topology*, dapat diartikan sebagai struktur penggambaran atau pendenahan jaringan komputer yang akan dibangun atau dibuat pada suatu tempat tertentu. Fungsinya adalah untuk mensimulasikan jaringan yang digambar tersebut apakah menghasilkan jaringan yang efektif dan efisien bagi penggun. (Nirsal & Ali, 2017). Topologi jaringan komputer memiliki lima jenis atau lima macam, yaitu :

1. Topologi *Bus*, topologi yang memiliki kelemahan pada proses komunikasi dan *transfer data* nya karena adanya kemungkinan terjadinya tabrakan, selain itu jika pada topologi ini ada satu perangkat yang terjadi gangguan, semua perangkat ikut mengalaman gangguan tersebut. Khusus topologi diwajibkan adanya konektor *T-Bone Connector*.
2. Topologi *Star*, merupakan topologi yang di-*upgrade* dari topologi sebelumnya, yaitu Topologi *Bus*. Karena di dalam topologi ini memakai aspek yang terhubung secara sentral, yaitu ada satu perangkat yang diletakkan di tengah-tengah diantara perangkat-perangkat yang terhubung, sehingga

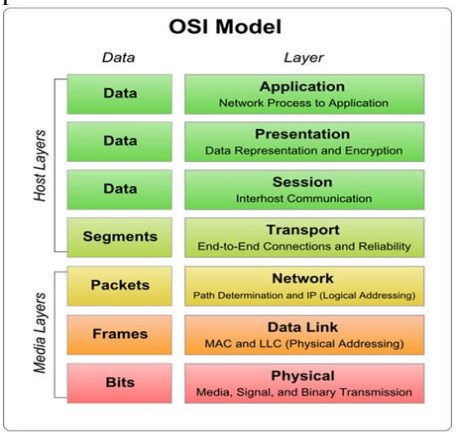
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

tabrakan data jarang dapat terjadi.

3. Topologi *Ring*, sama seperti topologi *Star*, bedanya topologi ini tidak ada perangkat yang menjadi sentral, disusun keliling antar perangkat yang terhubung, yang benar benar berbentuk sebuah cincin. Topologi ini kelemahannya sama seperti topologi *Bus*, karena jika satu perangkat bermasalah, semua perangkat ikutan bermasalah.
4. Topologi *Mesh*, setiap permasalahan setiap jenis topologi tidak akan ditemukan pada topologi ini, karena topologi ini dibuat berdasarkan kesalahan yang terjadi ditopologi sebelumnya. Sehingga di topologi ini tidak akan adanya tabrakan data, tidak akan adanya kelumpuhan jaringan jika satu perangkat bersamalah dan menggunakan konektor yang hemat *resource*.
5. Topologi *Tree*, topologi yang memadukan antara topologi *Bus* dan topologi *Star*, bentuknya tetap memakai konsep sentralitas tetapi setiap perangkat dihubungkan melauin konektor *T-Backbone connector*. Permasalahan yang mungkin terjadi tetap sama dengan masalah yang ada pada kedua topologi tersebut, tentu saja tabrakan data dan kelumpuhan jaringan secara menyeluruh jika terdapat perangkat yang bermasalah.

d. *OSI Layer*

Open Systems Interconnection (OSI) adalah satu salah layer yang digunakan sebagai koordinator standar pertukaran dan sekaligus sebagai pengembangan data di suatu jaringan. *OSI layer* berbeda dengan sebuah protokol karena *OSI layer* bertindak sebagai standar dan acuan yang ada dalam jaringan komputer (Supatmi, Nizar, & Fahlevi, 2014). Bagan *OSI layer* pada Gambar 2.5:



Gambar 2.5 OSI Layer

OSI Model terbagi atas tujuh tingkat atau lapisan yang setiap tingkatnya memiliki fungsi yang saling berkaitan satu sama lain, ketujuh tingkat tersebut yaitu:

1. *Application Layer* atau tingkat ketujuh yang diposisikan paling atas pada OSI Model, layer ini bertugas sebagai *interface* dari sebuah aplikasi dengan memberikan akses jaringan kepada aplikasi.
2. *Presentation Layer*, memiliki tugas untuk mengecek data-data yang akan di dikirim oleh aplikasi apakah sudah dikonversi ke dalam format yang dapat dimengerti oleh proses lapisan aplikasi melalui jaringan.
3. *Session Layer*, bertugas untuk mengatur cara agar koneksi dapat terhubung untuk berkomunikasi antar aplikasi atau proses yang terjadi di jaringan.
4. *Transport Layer*, tugasnya adalah mengirimkan paket data dari si pengirim ke si penerima dan juga mengecek apakah paket data tersebut sampai ke penerima dengan utuh dan baik.
5. *Network Layer*, mempunyai tugas untuk mendefinisikan alamat *IP* dan kemudian juga

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

bertugas untuk melakukan *routing* pada jaringan menggunakan perangkat seperti *Router* dan *Switch* layer-3 *(Switch Manage).*

6. *DataLink Layer*, Spesifikasi *IEEE 802* membagi Layer ini menjadi dua Layer lagi, kedua layer tersebut adalah lapisan *Logical Link Control (LLC)* dan satu lagi adalah lapisan *Media Access Control (MAC).* Layer ini berfungsi untuk menuntun *bit – bit* data dikonversi menjadi format yang bernama *frame.*
7. *Physical Layer*, pada *layer* ini terjadi proses menentukan media yang digunakan untuk transmisi jaringan, terdapat juga aktifitas untuk menentukan sinyal yang digunakan serta cara bagaimana untuk sinkronisasi *bit*, penggambaran arsitektur *blueprint* jaringan, dan juga topologi jaringan dan tipe dan jenis kabel yang digunakan.

e. Internet Protocol (IP)

IP Address memiliki defisini sebagai prosedur pengalamatan melalui cara yang menyebarkan sebaris *numeric* untuk perangkat jaringan sehingga dapat diterapkan di antarmuka dari perangkat tersebut. Pada umumnya, *IP Address* fungsinya adalah mendeteksi masalah yang timbul saat pengiriman dan penerimaan paket data. Saat berlangsungnya komunikasi antar data-data, *IP Address* memberlakukan dua *rules* yaitu, *addressing* dan *fragmentation* (Wardoyo, Ryadi, & Fahrizal, 2014).

Alamat IP atau disebut juga dengan *IP address* atau dapat juga disebut lagi dengan *Internet Protocol Address* yang memakai pengertian *identity* yang ada di perangkat-perangkat seperti *Personal Computer*, laptop dan perangkat keras jaringan, bahkan *handphone* atau *smartphone*. *Identity* itu cara penulisannya adalah kumpulang angka unik yang sudah diacak secara *random*. Karena susunan angkatnya acak dan unik, maka setiap perangkat dipastikan tidak memakai *identity* yang sama atau dalam istilah umumnya *IP Conflict*. (Tambunan, Raharjo, & Purwadi, 2013). *IP address* berdasarkan sifat dan karakternya terbagi atas 4 macam, yaitu:

1. *Static IP Address*, alamat IP yang penggunaannya hanya dimasukkan *user* sendiri, tidak otomatis.
2. *Dynamic IP Address*, alamat IP kebalikan dari *Static IP Address* karena setiap perangkat dapat mempunyai alamat IP secara otomatis melalui *server* yang disebut *DHCP Server*.
3. *Public IP Address*, alamat IP yang digunakan secara masif oleh perangkat perangkat yang di dunia, dengan syarat setiap perangkat terhubung ke jaringan yang sama, tentu saja jaringan tersebut adalah jaringan *Internet*.
4. *Private IP Address*, jika perangkat-perangkat tersebut tidak terhubung ke *Internet*, maka *Private IP* menjadi solusi untuk jaringan lokal ataupun interlokal.

Selain pembagian alamat IP berdasarkan sifat dan karakternya, dapat juga dibagi atas kelas-kelas alamat IP itu berada, kelas-kelas tersebut adalah sebagai berikut:

1. *A Class IP address* atau dalam Bahasa Indonesia alamat IP kelas A. IP kelas A memakai 8 bit angka dalam alamat IP nya sebagai *net ID* dan 24 bit angka lainnya sebagai *host ID.*
2. *B Class IP address,* di kelas B pembagian antaran *net ID* dan *host ID* dibagi secara adil, karena keduanya dibagi 16 bit angka masing-masing.

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

3. *C Class IP Address,* pada kelas C perbandingannya adalah kebalikan dari IP kelas A, karena di kelas C 8 bit angka diberikan ke *host ID* sehingga perangkat yang mendapatkan dan menggunakan IP kelas C dapat lebih banyak dari kelas lainnya.

f. Media Access Control (MAC)

Alamat MAC merupakan salah satu jenis alamat dari suatu jaringan yang terdapat pada lapisan *data-link OSI Layer*. Dapat ditemukan juga pada jaringan berbasis *ethernet*, *MAC address* termasuk sebagai alamat yang unik karena memiliki panjang 48-bit (6 *byte*) yang bisa memberikan identatis unik bagi komputer, *interface router*, ataupun perangkat lainnya sehingga MAC juga memiliki istilah sebagai *Ethernet address*, *Physical address*, atau *Hardware address* (Susianto & Yulianti, 2015).

g. *Server*

Server memiliki bentuk fisik yang tidak berbeda jauh dengan bentuk fisik komputer *client*. Bedanya adalah jika *personal computer server* memiliki spesifikasi yang lebih mumpuni daripada *personal computer client*, karena proses kerja yang akan dijalankan *server* lebih banyak daripada komputer biasa. Selain itu *server* juga bertugas sebagai penyedia layanan (sesuai dengan namanya) dimana layanan yang ditawarkan dari *server* bermacam-macam jenisnya bak itu *web server*, *dns server*, *dhcp server* dan banyak lainnya lagi tergantung dengan pemakaiannya dan tergantung konfigurasi yang dilakukan *administrator server* (Bawafie & Muslihudin, 2013).

h. Linux

Linux ternasuk sebagai program atau perangkat lunak yang memanfaatkan kernel sebagai sistem operasi yang berisikan skrip yang ada pada Internet pada tahun 1991. Selain itu, terdapat juga banyak pengguna yang berperan besar dalam pengembangan Linux ini di berbagai wilayah yang ada di dunia. Keseluruhan bagian dari sistem operasi ini adalah sistem yang berbasis *General Public License* (GPL) yang diresmikan pada tahun 1983 oleh Richard Stallman. Kontribusi GNU yang paling besar adalah pelopor munculnya nama alternatif GNU/Linux (Harjono, 2016).

i. Keamanan Jaringan Komputer

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)

j. Serangan Keamanan Jaringan

Dalam pembahasan penulis sebelumnya, disebutkan adanya terjadi kasus kriminalitas digital yang terjadi dalam keamanan jaringan komputer. Kriminalitas digital tersebut dalam disebut juga sebagai

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

serangan-serangan yang ada dalam keamanan jaringan. Serangan tersebut memiliki banyak variasi dan fungsinya masing-masing, serangan-serangan tersebut menurut (Manuaba, Hidayat, & Kusumawardani, 2012) adalah sebagai berikut:

1. *Reveal SSID*, serangan yang ditujukan pada jaringan *wireless* ketika ada *access point* yang menggunakan fitur *hide SSID* maka *reveal SSID* ini yang mematikan fitur tersebut.
2. *MAC Address Spoofing*, serangan yang dilancarkan ketika *MAC Address* seseorang terdaftar pada *list rules MAC Address Filtering* pada sebuah *accest point* atau *router* yang mengakibatkan *MAC Address* tersebut tidak dapat terhubung ke jaringan, sehingga penyerang menggunakan *MAC Address Spoofing* untuk melakukan *bypass* ke dalam jaringan.
3. Eavesdropping, sesuai dengan namanya serangan ini melakukan metode "menguping" pada setiap paket-paket data komunikasi yang dikirim ataupun diterima setiap *users* pada komputer-komputer yang terhubung ke jaringan yang diserang.
4. Session Hijacking, serangan yang menggunakan metode mengambil hak sah seorang *user* dalam mengakses situs atau konten *premium* dan penyerang mengambil sesi nya untuk digunakan secara cuma-cuma.
5. Man In The Middle Attack, serangan ini memiliki jenis seperti penipuan, dimana saat penyerangan terjadi, si penyerang akan membuat suatu situs *login page* atau berpura-pura menjadi seorang *administrator* dari suatu situs, dan meminta pengguna untuk memasukkan *username* dan *password* untuk masuk ke situs tersebut.
6. Denial of Service, Serangan yang ini adalah serangan paling umum yang dilakukan *hacker* ataupun *hijacker* dalam melakukan kriminalitasnya. Karena serangan ini mudah untuk dilakukan serta bisa diunduh di situs *internet*. Serangan ini berfokus untuk menyerang *server* dengan mengirimkan trasmisi data yang masif.

k. S*ecurity Onion*

Security Onion dapat diartikan sebagai sebuah sistem yang bermanfaat untuk mengetahui dan mendeteksi masalah-masalah yang ada di dalam sebuah jaringan. *Security Onion* merupakan salah satu distro dari sistem operasi berbasis *Linux*. *Security Onion* umumnya digunakan sebagai *tools* atau *buldle packet* untuk *Network Security Monitoring (NSM)*. *Security Onion* dapat difungsikan menjadi dua jenis sistem operasi, pertama sebagai sistem operasi *standalone* dimana *Security Onion* akan berfungsi sebagai penyaji data sedangkan jenis kedua sebagai *server* untuk merekam, mengelolah dan menyajikan data yang didapat dari sistem sensornya. (Muhartin, 2017)

l. Sguil

Sguil berbasiskan aplikasi yang bertugas untuk *Network Security Monitoring* yang terdapat didalam paket instalasi *Security Onion*. *Sguil* adalah satu dari tiga aplikasi yang bertugas sebagai *IDS* dan *IPS* di dalam keamanan jaringan komputer. *Sguil* bertugas untuk mengelolah data dari yang ditangkap oleh sensor, yaitu *Snort*. *Snort* akan dijelaskan pada pembahasan selanjutnya dan data-data yang direkam oleh *Snort* akan dikelolah oleh *Sguil* lalu akan divisualisasikan

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

oleh *Kibana*. *Sguil* menggunakan tampilan grafik yang intuitif sehingga *Sguil* menyediakan data *event* nya secara akurat dan langsung serta sesi waktu dari *event* tersebut serta data-data paket yang ditransmisikan di dalam event tersebut, semua data tersebut dikelolah oleh *Sguil*. Sehingga data-data yang dikelolah oleh *Sguil* akan bersifat data *raw*. (Muhartin, 2017)

m. *Snort*

Snort dikategorikan kedalam perangkat lunak atau aplikasi sama seperti *Sguil*. Namun, *Snort* termasuk ke dalam aplikasi berbasiskan *Open Source* atau yang dimaksud juga gratis bgai setiap kalangan yang mengunduh dan melakukan instalasinya. Keunggulaan *Snort* adalah bisa menganalisa *real time alert* yang metode pemasukkan *alert* atau alarm peringatannya berupa *user syslog*, *database* ataupun *file* (Muhartin, 2017). *Snort* terbagi atas 2 jenis atau *mode*, yakni:

a) *Sniffer Mode*, digunakan untuk melihat atau merekam paket-paket data yang masuk ke jaringan. Metode ini jarang digunakan pada topik-topik penelitian keamanan jaringan, karena metode ini tidak bisa melakukan *logging*.
b) *Packet Logger Mode*, fungsinya adalah untuk meluhat dan merekam paket-paket data yang masuk ke jaringan, namun setelah itu datanya dianalisa. Oleh karena ini metode ini dapat melakukan *logging* dan dapat digunakan dalam penelitian keamanan jaringan.

n. Kibana

Kibana merupakan *tool* atau aplikasi yang terdapat dalam paket instalasi di *Security Onion*. *Kibana* bertugas untuk menvisualisasikan atau menampilkan hasil data yang telah direkam oleh *Snort* dan diolah oleh *Sguil*. *Kibana* memiliki tampilan dalam situs atau *web* dan dapat dioperasikan dengan mudah atau *user-friendly*. Hasil visualisasi data dari *Kibana* dapat digunakan untuk melakukan pengecekkan masalah yang ada dari data hasil olahan tersebut sehingga pencarian solusi untuk masalah keamanan jaringan lebih mudah. (Putra, 2018)

o. MikroTik Router

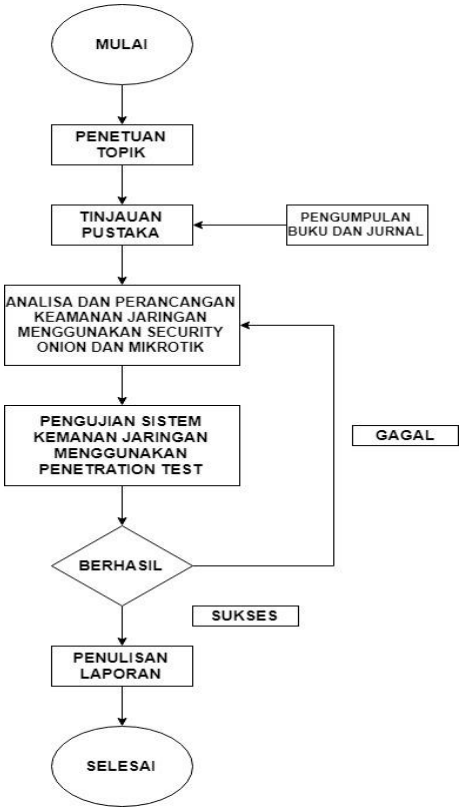
MikroTik Router awal mulanya diciptakan dari sebuah sistem operasi perangkat lunak yang berbasiskan untuk konfigurasi jaringan komputer. Seiiring berkembangnya zaman, *MikroTik* mulai menciptakan perangkat keras jaringan seperti salah satunya *router* yang berisikan sistem operasinya sendiri yaitu *MikroTik*. *Mikrotik Router* memiliki banyak fungsi dan keunggulan daripada kompetitor-kompetitor lainnya seperti *Cisco*. Keunggulannya salah satunya adalah dapat melakukan konfigurasi koneksi ke *Internet* secara mudah dalam aspek pengelolaannya dan lebih terpusat.. Selain itu *MikroTik Router* juga memiliki fitur pembagian *bandwidth*, konfigurasi *Firewall NAT* dan masih banyak lainnya. Keunggulannya dari sisi *resource* juga banyak, seperti biayanya dan kemudahan penggunaan *interface MikroTik* itu sendiri.

III.METODOLOGI PENELITIAN

3.1 Alur Penelitian

Proses atau gambaran aliran dari suatu penelitian yang terdapat pada laporan ini yang diperlihatkan dalam bentuk rangka atau bagan disebut juga sebagai Alur Penelitian. Gambar dibawah ini adalah gambar alur penelitian yang ada dalam laporan ini:

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -



Gambar 3.1: Alur Penelitian

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Dibawah ini adalah penjelasan dari setiap bagian yang ada di dalam gambar alur penelitian laporan ini:

1. Pada proses pertama kali yang dilakukan adalah melakukan penentuan judul, topik, sumber apa saja yang akan digunakan dalam pembuatan laporan ini sehingga memiliki predikat sebagai laporan yang memiliki fakta akurat.
2. Pada proses inilah penulis banyak melakukan pencarian jurnal-jurnal di ranah *internet* secara menyeluruh baik itu dalam negeri ataupun luar negeri. Sehingga jurnal yang mendukung laporan ini bersifat resmi dan bersifat dokumen yang legal.
3. Setelah mendapatkan jurnal-jurnal tersebut, selanjutnya penulis mencari masalah yang terdapat pada topik tersebut, sehingga proyek yang akan dirancang nanti dapat menyelesaikan masalah pada topik tersebut secara baik dan benar. Masalah yang didapatkan adalah keamanan jaringan lokal, sehingga laporan ini menjelaskan bagaimana proyek yang dirancang dapat menjadi solusi pada masalah tesebut.
4. Setelah proyek selesai dirancang serta juga masalah sudah dianalisa dengan baik, maka pada proses inilah penulis melakukan *test and drive* sehingga dapat diketahui apakah proyek yang dirancang berhasil menjadi solusi pada masalah tersebut.
5. Jika pada proses *test and drive* nya berhasil berjalan dengan sempurna, selanjutnya penulis menunggu dan mengawasi proses berjalannya proyek tersebut, dilihat apakah ada kemungkinan munculnya permasalahan pada proyek itu sendiri.
6. Semisalnya jika terdapat masalah pada proyek yang penulis rancang, maka penulis harus melakukan analisa kembali untuk melihat penyebab masalah yang ada di proyek penulis tersebut. Jika terdapat celah pada proyek tersebut maka penulis akan memperbaikinya dan akan melakukan *test and drive* lagi.
7. Jika semua proses selesai dijalankan dan tidak memiliki masalah lagi, tahap terakhir adalah penulis melakukan penulisan laporan ini sebagai formalitas bukti pekerjaan yang dilakukan penulis pada proyek ini apa saja.

3.2 Analisa Permasalahan

Tahun modern ini, semakin banyak perusahaan dan instansi yang mengubah sistem mereka untuk menggunakan jalur digital, salah satunya adalah memanfaatkan *internet* sebagai media untuk pembelajaran anak-anak dan murid sekolah, dapat juga digunakan hiburan seperti nonton film dan mendengarkan musik dan tentu saja termasuk juga sebagai keperluan untuk bekerja sehingga media *internet* di era digital ini sudah menjadi salah satu dari sekian banyaknya kebutuhan primer manusia. Oleh sebab itu jika kita mengunjungi banyak tempat dan negara ataupun lokasi sudah terdapat jaringan *nternet* dimana-mana contohnya saja adalah *free wifi*, yaitu adalah salah satu jenis jaringan internet yang bisa diakses tanpa kabel seperti yang dikoneksikan ke sebuah komputer.

Seiiring berkembangnya penggunaan *internet* di dunia ini, semakin berkembang juga tindakan kejahatan yang dilakukan. Para penjahat pun terjun ke dunia *internet*

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

untuk melakukan tindakan kriminalitas. Seperti pencuriat data, data pribadi ataupun data keuangan, pembajakan juga dapat dikategorikan sebagai kriminalitas di dalam dunia *internet*. Selain itu terdapat juga kriminalitas yang bersifat menyerang seperti masuk paksa ke jaringan seseorang atau perusahaan lalu menyebarkan *virus* di perangkat-perangkat mereka ataupun juga menghapus data-data kantor yang penting. Dari contoh kasus krimnalitas yang banyak tersebut maka dipikirkanlah bagaimana solusi terbaik untuk menjaga jaringan *internet* ini, salah satunya adalah sistem keamanan jaringan (pada laporan ini mengambil contoh jaringan lokal) yang memanfaatkan fitur-fitur dari sistem *Security Onion* dan mengkombinasikannya dengan perangkat keras jaringan *Router MikroTik*.

3.3 Analisa Perancangan

Tahap ini adalah tahap yang paling penting yang penulis jelaskan pada paragraf sebelumnya. Dikarenakan di tahap ini penulis harus melakukan banyak hal untuk memastikan agar masalah yang timbul sudah dianalisa dengan baik dan benar. Selain itu penulis juga melakukan analisa pada proyek yang akan dirancang dan diterapkan. Penulis harus melakukan analisa apakah proyek yang dirancang efektif untuk menanggulangi masalah yang menjadi topik laporan ini ataupun memastikan apakah proyek yang dibangun sudah memiliki alur yang jelas agar selesai tepat pada waktunya.

Untuk menghasilkan rancangan proyek yang kompeten dan sesuai dengan topik masalah ini, metode penelitian yang penulis pakai di dalam penelitian yang berjudul "**Analisa dan Perancangan Kemamanan Jaringan Lokal Menggunakan *Security Onion* dan *MikroTik***" ini adalah metode *Penetration Testing. Penetration Testing* adalah metode yang sudah digunakan pada khalayak umum, terutama pada kalangan *network tester* dimana tujuan metode ini adalah untuk melakukan tes tekanan pada proyek yang kita rancang (pada kasus ini adalah kemanan jaringan lokal) dan setelah dilakukan tes melalaui penyerangan jaringan dilakukan analisa celah apa yang ada pada proyek tersebut.

Tujuan umum dari metode *penetration testing* ialah menguji atau mengetes keamanan dan kekuatan lapisan keamanan dari sistem yang dirancangan ini atau pada jaringan lokal tersebut. *Penetration testing* ini dapat menolong penulis untuk mengetahui celah keamanan di dalam sistem keamnan jaringan lokal ini sehingga penulis dapat memperbaiki dan menutupi celah keamanan tersebut.

Gambar 3.2 Alur *Penetration Test*

Penjelasan dari gambar diatas dapat dijelaskan dibawah ini sebagai berikut:

1. *Planning* atau sesuai dengan nama proses nya adalah perencanaan. Namun penulis pada laporan ini lebih tepatnya melakukan pengumpulan data-data pendukung agar membantu penulis mengetahui apa saja yang dilakukan untuk melaksanakan *penetration testing* ini.
2. Setelah data-data tersebut selesai dikumpulkan dan penulis juga sudah mengetahui apa yang akan dilakukan, selanjutnya penulis mengumpulkan informasi-informasi yang ada pada jaringan lokal yang akan dites tersebut. Seperti contohnya mengetahui komputer mana saja yang

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

terhubung ke jaringan lokal ini beserta *IP Address* dan *IP Gateway* masing masing dan mengumpulkan informasi siapa saja yang melakukan komunikasi di dalam jaringan lokal tersebut.

3. Pada tahap ketiga inilah penulis akan menemukan celah –celah keamanan pada proyek yang sudah penulis rancang. Jika penulis menemukan celah tersebut, penulis menelaah lebih dalam apakah celah tersebut disebabkan oleh serangan luar atau *human error* dari dalam sistem. Penulis juga menganalisa apakah celah keamanan tersebut dapat diserang secara otomatis menggunakan perangkat lunak atau dapat diserang secara manual menggunakan *command line* salah satu contohnya.
4. Di tahap keempat ini penulis melanjutkan *penetration test* dimana penulis memposisikan diri sebagai penyerang dari luar sehingga dinamakan proses eksploitasi karena penulis benar-benar melakukan banyak jenis serangan dan cara untuk menembus sistem keamanan jaringan lokal ini sehingga sistem tersebut kebal menerima serangan yang sudah dites.
5. Pada tahap terakhir ini lebih kurang sama dengan tahap terakhir pada alur penelitian, yaitu membuat laporan sebagai formalitas proses *penetration testing* yang dilakukan penulis pada proyek ini.

3.3.1 Analisa Kebutuhan Perangkat Keras

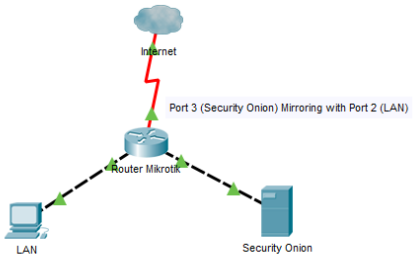
Untuk melakukan rancangan proyek sistem pengamanan jaringan lokal, penulis tentu menggunakan bantuan dari perangkat keras serta perangkat lunak yang ada. *Hardware* yang penulis gunakan adalah sebuah laptop dan perangkat keras jaringan *router MikroTik*. Laptop yang penulis gunakan adalah laptop Lenovo Thinkpad yang memiliki spesifikasi *Processor* Intel® Core ™ i5-4300U CPU @1.90Hz – 2.49Hz, *RAM* sebesar 8 GB dan *Harddisk* 500 GB. Untuk *router MikroTik* penulis menggunakan level lisensi 4, *RAM* sebesar 32 MB dan memiliki 5 buat *port Ehternet*.

3.3.2 Analisa Kebutuhan Perangkat Lunak

Pada perangkat lunak penulis menggunakan aplikasi untuk menjalankan sistem operasi virtualisasi yaitu *Oracle VM VirtualBox*. VirtualBox merupakan aplikasi yang umumnya digunakan untuk mensimulasikan atau melakukan virtualisasi sistem operasi di dalam sistem operasi sehingga sumber daya yang digunakan lebih hemat. Selain itu tentu saja perangkat lunak sistem keamanan jaringan *Security Onion* yang dikombinasikan dengan *Sguil* sedangkan pada sisi LAN atau pada *client* penulis menggunakan sistem operasi *Linux Ubuntu Server*.

3.3.3 Analisa Topologi Jaringan

Pada perancangan proyek ini penulis tentu saja memiliki topologi atau *blueprint* dari jaringan yang penulis rancang dan sekaligus yang penulis uji. Topologi yang penulis rancangn tidak memiliki banyak *resources* karena hanya seputar jaringan LAN meskipun tetap terhubung ke *Internet*. Berikut topologi yang penulis gunakan dalam perancangan proyek ini:



Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Gambar 3.3 Topologi Jaringan Lokal

IV. IMPLEMENTASI

4.1 Instalasi dan Konfigurasi Proyek

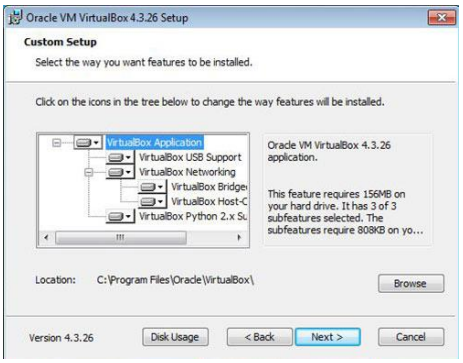
Sebelum penulis melakukan implementasi proyek yang telah dirancang sebelumnya, terlebih dahulu dilakukan instalasi baik dari perangkat keras ataupun perangkat lunaknya. Setelah proses instalasi akan dilakukan proses konfigurasi, pertama-tama penulis akan membahas instalasinya terlebih dahulu.

4.1.1 Instalasi Aplikasi *VirtualBox*

Aplikasi VirtualBox merupakan aplikasi yang digunakan penulis untuk melakukan virtualisasi sistem operasi yang akan digunakan dalam proyek ini. Langkah pertama dalam instalasi ini adalah mengunduh aplikasi dari situs resminya dengan alamat situs di https://www.virtualbox.org/wiki/Downloads. Setelah selesai diunduh, dibuka dokumen instalasinya makan akan muncul seperti gambar dibawah ini:

Gambar 4.1 Tampilan Instalasi Aplikasi *VirtualBox*

Setelah itu lanjutkan instalasi dengan menekan tombol *Next* di setiap jendela instalasi, karena penulis melakukan instalasi secara *default* sehingga mengikuti konfigurasi resmi dan menekan tombol *next* saja. Pada pertengahan instalasi akan muncul jendela seperti dibawah ini:



Gambar 4.2 Instalasi Paket dan Lokasi Instalasi *VirtualBox*

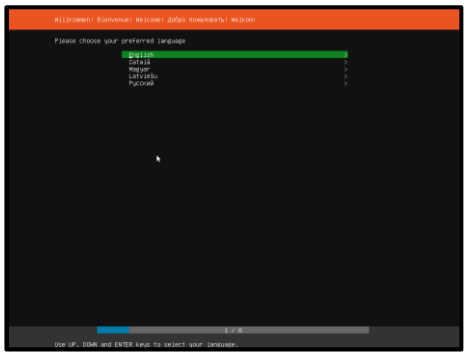
Setelah selesai melakukan instalasi hingga menekan tombol *finish*, silahkan dibuka aplikasi tersebut dan tampilan aplikasinya adalah sebagai berikut:

Gambar 4.3 Tampilan Aplikasi *VirtualBox*

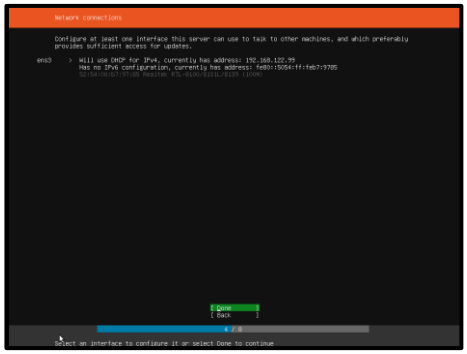
4.1.2 Instalasi dan Konfigurasi *Ubuntu Server*

Setelah melakukan instalasi aplikasi *VirtualBox*, selanjutnya ada sistem operasi Linux yang akan digunakan penulis pada proyek ini. Penulis menggunakan *Linux Ubuntu Server* sebagai sistem operasi uji coba dan sebagai *client* juga. Berikut adalah tampilan instalasi *Ubuntu Server* hingga tampilan awal dari *Ubuntu Server* tersebut.

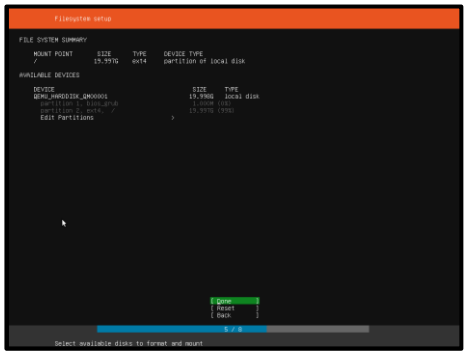
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -



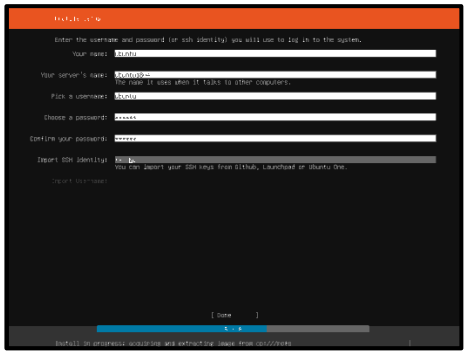
Gambar 4.4 Proses Pemilihan Bahasa *Ubuntu Server*



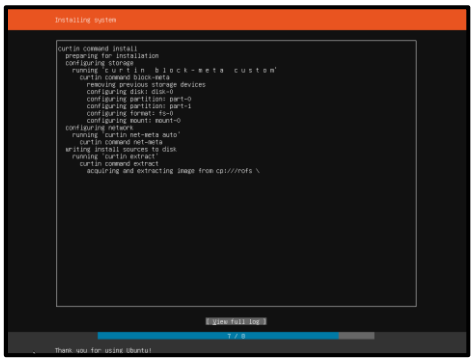
Gambar 4.5 Konfigurasi Jaringan *Ubuntu Server*



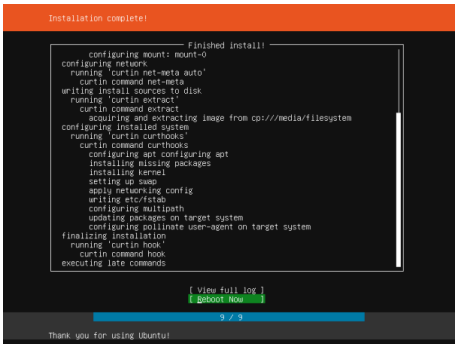
Gambar 4.6 Proses Partisi *Ubuntu Server*



Gambar 4.7 Konfigurasi *Username* dan *Password Ubuntu Server*



Gambar 4.8 Proses Instalasi *Ubuntu Server*



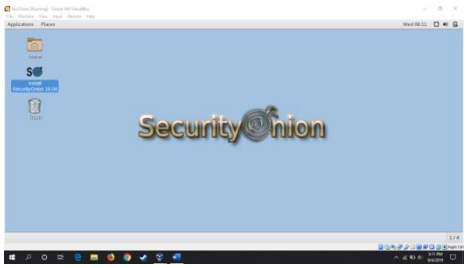
Gambar 4.9 Proses Instalasi *Ubuntu Server* Selesai

Gambar 4.10 Tampilan Antarmuka *Ubuntu Server*

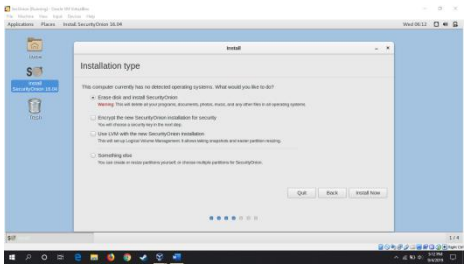
4.1.3 Instalasi dan Konfigurasi *Security Onion*

Perangkat lunak yang menjadi *main focus* pada proyek ini adalah Security Onion yang akan dilakukan instalasi pada *Server*. Bertindak sebagai sistem yang mengawasi dan mengamankan jaringan lokal yang terhubung ke *server* tersebut. Berikut proses instalasinya:

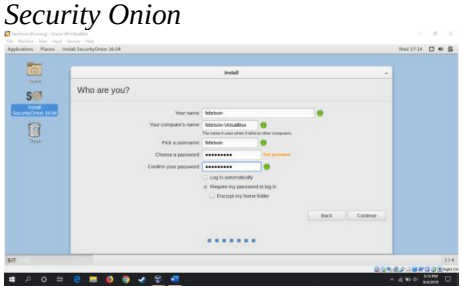
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -



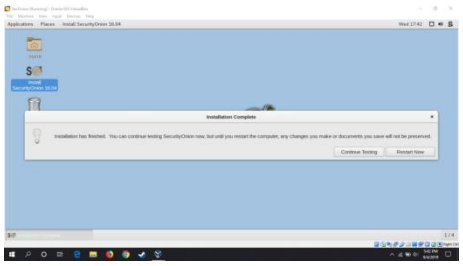
Gambar 4.11 Tampilan *Security Onion* Sebelum Instalasi



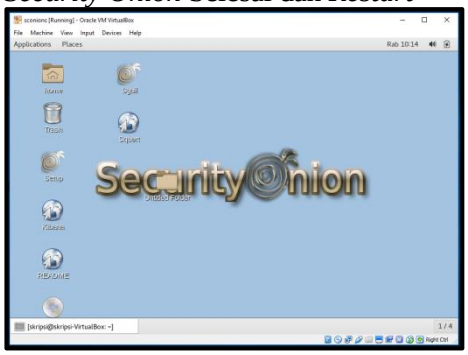
Gambar 4.12 Proses Instalasi *Security Onion*



Gambar 4.13 Proses Konfigurasi *Username* dan *Password Security Onion*



Gambar 4.14 Proses Instalasi *Security Onion* Selesai dan *Restart*



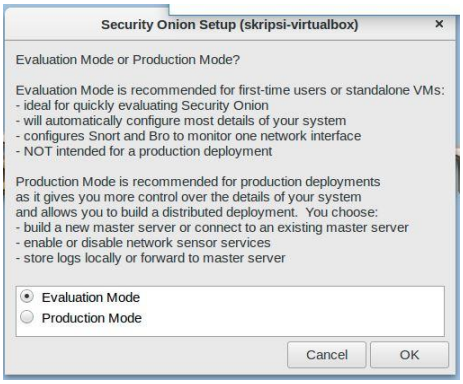
Gambar 4.15 Tampilan *Security Onion* Setelah Instalasi

Setelah proses instalasi selesai, penulis melakukan konfigurasi aplikasi yang akan digunakan serta jaringan atau *IP Address* pada *Security Onion* tersebut. Langkah awal klik menu *Setup* lalu masukkan *password* yang telah dimasukkan saat instalasi. Lalu akan muncul seperti gambar dibawah ini:

Gambar 4.16 Proses Pemilihan *Services Security Onion*

Gambar 4.17 Proses Konfigurasi Jaringan *Security Onion*

Karena penulis menggunakan jaringan yang memakai *DHCP Server*, maka penulis memilih menu *Yes, skip network configuration!* yang artinya penulis langsung menggunakan *IP Address* yang didapatkan dari *DHCP Server*.



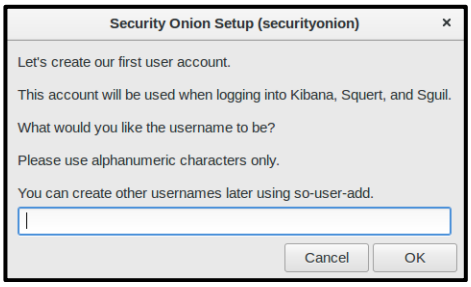
Gambar 4.18 Proses Pemilihan *Setup Security Onion*

Penulis memilih menu *Evaluation Mode* karena sesuai

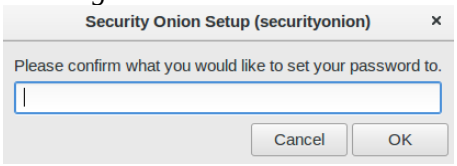
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

dengan kebutuhan penulis yang ingin menggunakan *Security Onion* dengan konfigurasi *default* dan *simple* siap digunakan. *Evaluation Mode* juga membantu penggunanya melakukan konfigurasi otomatis yang akan berjalan secara *background* saat kita menjalan *setup* di dalam *Security Onion*.

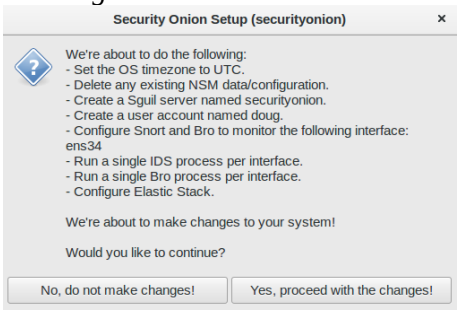
Gambar 4.19 Pemilihan *Interface Network Monitored*



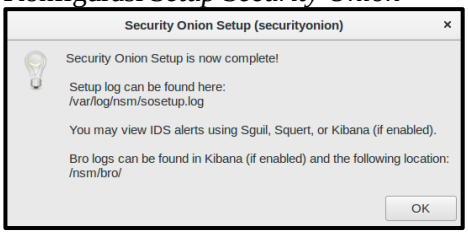
Gambar 4.20 Proses *Input Username* untuk *Sguil Tool*



Gambar 4.21 Proses *Input Password* untuk *Sguil Tool*



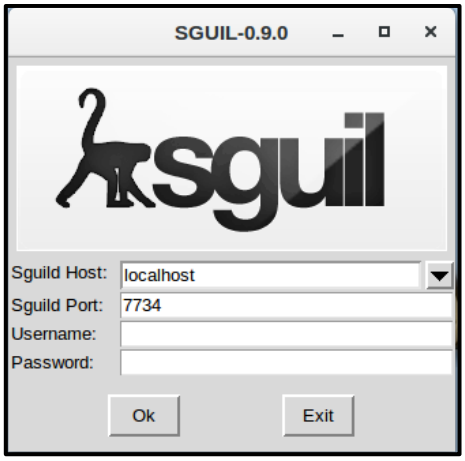
Gambar 4.22 Konfirmasi Konfigurasi *Setup Security Onion*



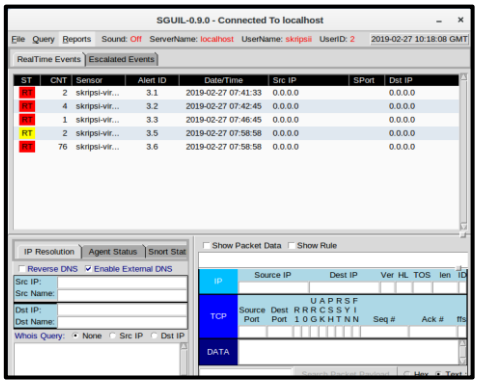
Gambar 4.23 Pemberitahuan Konfigurasi *Security Onion* Selesai

4.1.4 Konfigurasi *Sguil Tool*

Sguil Tool merupakan salah satu aplikasi yang terdapat didalam *Security Onion*, instalasi *Sguil Tool* dilakukan bersamaan dengan instalasi *Security* Onion. Cara menjalankannya adalah buka aplikasi *Sguil* yang ada pada *desktop Security Onion* dan masukkan *username* dan *password* yang telah diinput pada saat proses konfigurasi *Security Onion*.



Gambar 4.24 Tampilan *Login Sguil Tool*



Gambar 4.25 Tampilan Antarmuka *Sguil Tool*

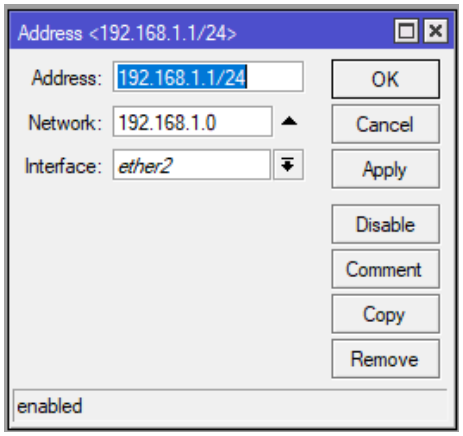
4.1.5 Konfigurasi *MikroTik Router*

MikroTik Router biasanya sudah dijual secara siap pakai, artinya tidak memiliki proses instalasi lagi. Pada *router* ini penulis hanya melakukan konfigurasi jaringannya agar terhubung ke *Internet* dan juga terhubung ke *personal computer client (Ubuntu Server)* serta ke *server Security*

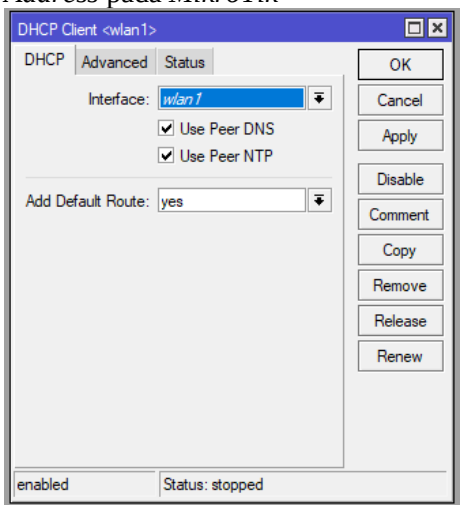
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Onion. Untuk melakukan akses kedalam *MikroTik Router* menggunakan aplikasi yang bernama *WinBox* yang dapat diunduh melalui situs resminya di alamat https://mikrotik.com/download.
Berikut tampilan *WinBox* dan proses konfigurasi dasarnya:

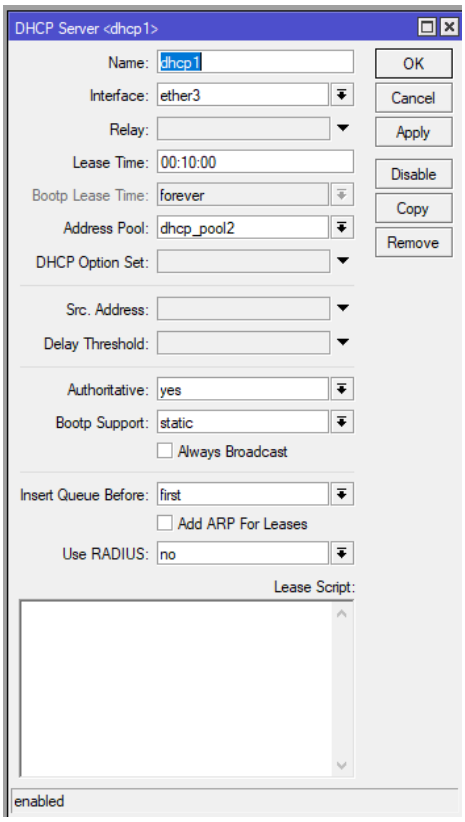
Gambar 4.26 Tampilan Antarmuka *WinBox*



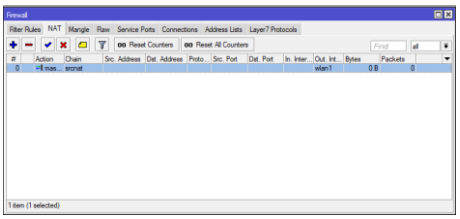
Gambar 4.27 Konfigurasi *IP Address* pada *MikroTik*



Gambar 4.28 Konfigurasi *DHCP Client MikroTik*

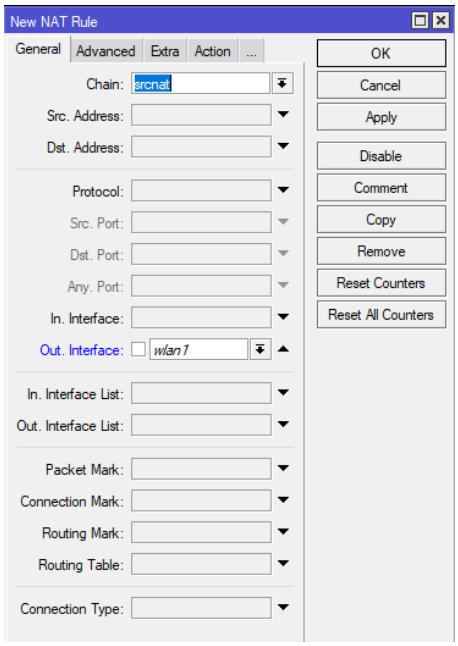


Gambar 4.29 Alur Konfigurasi *DHCP Server MikroTik*

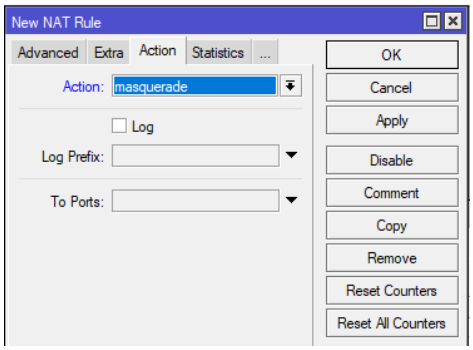


Gambar 4.30 Konfigurasi *Firewall NAT MikroTik*

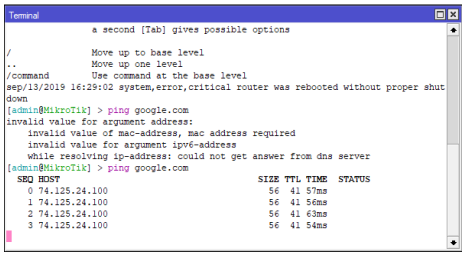
Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -



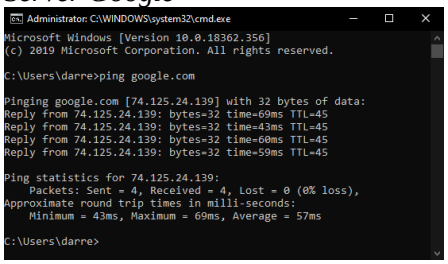
Gambar 4.31 Konfigurasi *Interface NAT Rule MikroTik*



Gambar4.32 Konfigurasi *Firewall NAT Rule MikroTik*



Gambar 4.33 Tampilan Tes *PING* ke *Server Google*



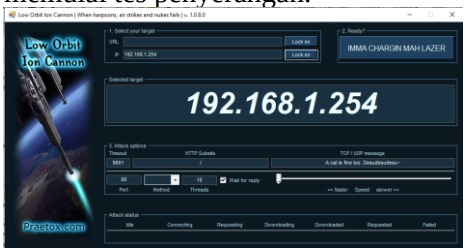
Gambar 4.34 Tampilan Tes *PING* ke *Server Google (CMD)*

4.2 *Penetration Test* Menggunakan *DDOS*

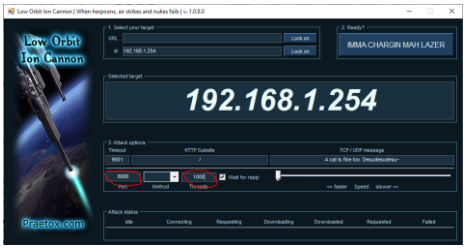
Pada *penetration test* ini penulis memakai aplikasi buatan pengguna yang disebar secara gratis di *Internet* yang bernama *LOIC (Low Orbit Ion Cannon)*. Berikut tampilan dari aplikasi *LOIC*:

Gambar 4.35 Tampilan Antarmuka Aplikasi *LOIC*

Cara penggunaannya adalah dengan memasukkan *IP Address* yang akan diserang (dalam kasus ini, *IP Address client* pada proyek penulis) lalu memilih *port* dan *thread* yang akan diserang dari komputer *client* lalu tekan *start* untuk memulai tes penyerangan.

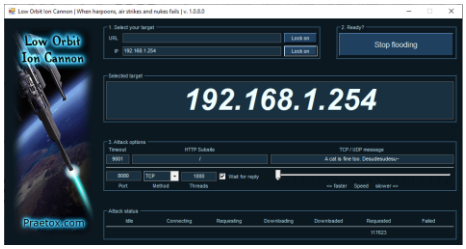


Gambar 4.36 Proses Memasukkan *IP Address Client*



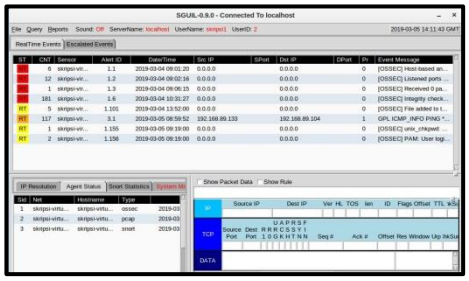
Gambar 4.37 Proses Memilih *Port* dan *Thread*

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -



Gambar 4.38 Proses Simulasi Serangan

Setelah melakukan proses penyerangan ke komputer *client* yang sudah terhubung ke *Internet* namun *port* yang digunakan untuk koneksi ke komputer *client* telah dikonfigurasi menggunakan *port mirroring* ke *port Security Onion*, maka identitas penyerang (dalam kasus ini LOIC) akan terbaca dan muncul di *Sguil* yang berada dalam *Security Onion*. Seperti gambar dibawah ini:



Gambar 4.39 Proses *Monitoring* Komputer *Client*

4.3 Implementasi dan Hasil Proyek

Dari hasil *penetration test* yang sudah dilakukan, terlihat hasil bahwa identitas atau *IP Address* si penyerang terdeteksi di *Sguil Tool* yang ada di dalam *Security Onion*. Seperti pada gambar dibawah ini:

Gambar 4.40 Monitoring IP Address Attacker

Dari hasil pengujian atau *penetration test* tersebut, penulis dapat menarik hasil proyek ini adalah berhasil mendeteksi serangan yang masuk ke komputer *client* yang berada di jaringan lokal. Penulis menggunakan aplikasi LOIC untuk melakukan serangan *DDOS* ke komputer *client* yang sudah terhubung ke jaringan lokal dan diawasi oleh *Security Onion*. Semua jaringan lokal ini dihubungkan melalui *MikroTik Router*.

Saat *penetration test* dilakukan, *IP Address* dari aplikasi LOIC tersebut terdeteksi dan muncul di daftar hasil *monitoring Sguil Tool* di *Security Onion*. Meskipun hasil dari penyerangan metode *DDOS* tersebut berhasil menyerang komputer atau *personal computer client* dan mengirimkan serangan *DDOS* ke *server*, penyerangan tersebut dibelokkan di *port* tiga yang tak lain adalah *port* yang terhubung ke *server Security Onion*. Sehingga serangan tersebut masuk ke *server* dan berhasil dicegah serta masuk ke daftar *monitoring Security Onion*.

Dari hasil *penetration test* yang berjalan dengan lancar penulis memberikan *status* proyek ini berhasil dirancang dan dapat diimplementasikan ke jaringan lokal. Oleh sebab itu penelitian yang berjudul "Analisa dan Perancangan Keamanan Jaringan Lokal Menggunakan *Security Onion* dan *MikroTik*" berhasil dianalisa dan dirancang oleh penulis dan juga sukses berhasil diimplementasikan. Penulis optimis hasil proyek ini dapat diimplementasikan ke jaringan lokal yang terdapat di kampus, kantor ataupun tempat yang memilii luas wilayah kecil sesuai dengan cakupan area jaringan LAN.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan dari penelitian yang dilakukan oleh peneliti dengan topik "Analisa dan Perancangan

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Keamanan Jaringan Lokal Menggunakan *Security Onion* dan *MikroTik*", maka peneliti menyimpulkan beberapa manfaat dari sistem keamanan yang telah dirancang adalah sebagai berikut:

1. Hasil luaran pada penelitian ini merupakan sebuah perancangan keamanan jaringan lokal menggunakan *Security Onion* dan *MikroTik* dapat menjadi solusi untuk serangan *DDOS*.
2. Dari hasil pengujian dengan *penetration test* ini, terbukti bahwa penelitian ini berhasil dilakukan dengan baik. Dimana hasil akhir dari pengujian ini adalah berupa keamanan jaringan lokal yang dapat merekam dan mendeteksi serangan *DDOS.*

5.2 Saran

Dalam peracangan dan pembuatan sistem keamanan jaringan ini, masih terdapat keterbatasan-keterbatasan yang dapat menjadi rekomendasi untuk pengembangan selanjutnya. Berikut adalah saran yang dapat diberikan oleh penulis :

1. Seharusnya sistem keamanan ini ditingkatkan menjadi keamanan jaringan yang lebih luas seperti MAN dan WAN.
2. Sebaiknya serangan yang dapat diawasi pada jaringan tidak hanya serangan dari luar tetapi juga serangan dari dalam.

DAFTAR PUSTAKA

Akbar, M. (2018). PERANCANGAN SOFTWARE IDS SNORT UNTUK PENDETEKSIAN SERANGAN INTERRUPTION (Netcut) PADA JARINGAN WIRELESS. *Jurnal INSTEK (Informatika Sains Dan Teknologi)*, *3*(1), 121–129.

Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *It Journal Research and Development*, *3*(1), 94–104.

Bawafie, N., & Muslihudin. (2013). Perancangan Sistem Monitoring Bandwidth Internet Berbasis SMS, *1*, 241–247.

Chelara, G., & Hermanto, D. (2014). Analisis Site to Site Virtual Private Network (VPN) pada PT . Excel Utama Indonesia Palembang. *Seminar Perkembangan Dan Hasil Penelitian Ilmu Komputer (SPHP-ILKOM)*, *1*(1), 35–44.

Fathoni, W., Fitriyani, & Nurkahfi, G. N. (2016). Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort. *E-Proceeding of Engineering*, *3*(1), 1169–1172.

Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *SinkrOn Jurnal & Penelitian Teknik Informatika*, *1*(1), 30–35.

Heru, B., Benny, Defendy, & Hento, W. (2014). KEAMANAN JARINGAN MENGGUNAKAN UNIFIED THREAT MANAGEMENT PADA SERVER BERBASISKAN LINUX, *1*, 48–59.

Lukman, N. (2016). Studi Implementasi Aplikasi Manajemen Ruang Kelas "Netop School" Berbasikan Local Area Network (LAN). *Jurnal Sains Dan Teknologi Utama*, *XI*(152), 1–14.

Manuaba, I. B. V. H., Hidayat, R., & Kusumawardani, S. S. (2012). Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas. *Jnteti*, *1*(1), 5. https://doi.org/10.22146/JNTETI.V1I1.3

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Muhartin, A. (2017). IMPLEMENTASI SISTEM MONITORING JARINGAN WIRELESS DENGAN METODE NETWORK SECURITY MONITORING (NSM). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Nirsal, & Ali, M. (2017). DESAIN DAN IMPLEMENTASI UIAN NASIONAL BERBASIS KOMPUTER PADA SMA NEGERI 6 PALOPO. *Prosiding Seminar Nasional*, *03*(1), 241–352.

Nurdin, N. (2015). Analisis Adopsi Dan Pemanfaatan Internet Di Kalangan Mahasiswa Perguruan Tinggi Di Kota Palu. *JURNAL ELEKTRONIK SISTIM INFORMASI DAN KOMPUTER (JESIK)*, *1*(1), 1–13.

Putra, R. A. (2018). ANALISA IMPLEMENTASI ARSITEKTUR MICROSERVICES BERBASIS KONTAINER PADA KOMUNITAS PENGEMBANG PERANGKAT LUNAK SUMBER TERBUKA (OPENDAYLIGHT DEVOPS COMMUNITY), *1*, 150–162.

Rahim, A. (2016). Rancang Model Sistem Keamanan Menggunakan Intrusion Prevention System Dengan Metode Rule Based : Studi Kasus KPDE Provinsi Jambi. *Jurnal Ilmiah Media SISFO*, *10*(2), 190–205.

Riadi, I. (2014). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *JUSI, Universitas Ahmad Dahlan Yogyakarta*, *1*(1), 71–80. https://doi.org/10.2307/2137776

Saputra, T. T., Irawan, B., & Ilhamsyah. (2014). Aplikasi Antrian Nasabah Bank Menggunakan Teks Dan Suara Berbasis Jaringan Wireless Lokal Area Network (WLAN). *Jurnal Coding Sistem Komputer Universitas Tanjungpura*, *02*(2), 1–7.

Supatmi, S., Nizar, T. N., & Fahlevi, R. (2014). Sistem Kontrol Peralatan Rumah Dan Monitoring Kondisi Rumah Melalui Internet Berbasis Web Dan Openwrt. *Jurnal Teknik Komputer Unikom – Komputika – Volume 3, No.2 - 2014 SISTEM*, *3*(2), 23–28. Retrieved from http://komputika.tk.unikom.ac.id/_s/data/jurnal/v3no2/1-srisupatmi.pdf/ori/1-srisupatmi.pdf

Susianto, D., & Yulianti, I. (2015). MENGAMANKAN WIRELESS DENGAN MENGGUNAKAN TWO FACTOR, PASSWORD DAN MAC ADDRESS FILTERING. *Expert-Jurnal Manajemen Sistem Informasi Dan Teknologi MENGAMANKAN*, *5*(2), 28–37.

Syaimi, A., Utami, P., Lidyawati, L., & Ramadhan, Z. (2013). Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd. *Jurnal Reka Elkomika TeknikElektro | Itenas Jurnal Online Institut Teknologi Nasional Jurnal Reka Elkomika*, *1*(4), 2337–2439.

Tambunan, B., Raharjo, W. S., & Purwadi, J. (2013). Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System. *1 / Vol.5 / September 2013*, *1*(0), 1–7. https://doi.org/Bosman Tambunan, Willy Sudiarto Raharjo, Joko Purwadi

Varianto, E., & Badrul, M. (2015).

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Implementasi Virtual Private Network dan Proxy Server Menggunakan Clear OS Pada PT. Valdo International. *Jurnal Teknik Komputer AMIK BSI*, *1*(1), 54–65.

Wardoyo, S., Ryadi, T., & Fahrizal, R. (2014). Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni Dan Tunneling 6to4 Berbasis Router Mikrotik. *Jurnal Nasional Teknik Elektro*, *3*(2), 106–117.

Akbar, M. (2018). PERANCANGAN SOFTWARE IDS SNORT UNTUK PENDETEKSIAN SERANGAN INTERRUPTION (Netcut) PADA JARINGAN WIRELESS. *Jurnal INSTEK (Informatika Sains Dan Teknologi)*, *3*(1), 121–129. https://doi.org/10.24252/instek.v3i1.5007

Arta, Y., Syukur, A., & Kharisma, R. (2018). Simulasi Implementasi Intrusion Prevention System (IPS) Pada Router Mikrotik. *It Journal Research and Development*, *3*(1), 94–104.

Bawafie, N., & Muslihudin. (2013). Perancangan Sistem Monitoring Bandwidth Internet Berbasis SMS, *1*, 241–247.

Chelara, G., & Hermanto, D. (2014). Analisis Site to Site Virtual Private Network (VPN) pada PT . Excel Utama Indonesia Palembang. *Seminar Perkembangan Dan Hasil Penelitian Ilmu Komputer (SPHP-ILKOM)*, *1*(1), 35–44.

Fathoni, W., Fitriyani, & Nurkahfi, G. N. (2016). Deteksi Penyusupan Pada Jaringan Komputer Menggunakan Ids Snort. *E-Proceeding of Engineering*, *3*(1), 1169–1172.

Harjono, E. B. (2016). Analisa Dan Implementasi Dalam Membangun Sistem Operasi Linux Menggunakan Metode LSF Dan REMASTER. *SinkrOn Jurnal & Penelitian Teknik Informatika*, *1*(1), 30–35.

Heru, B., Benny, Defendy, & Hento, W. (2014). KEAMANAN JARINGAN MENGGUNAKAN UNIFIED THREAT MANAGEMENT PADA SERVER BERBASISKAN LINUX, *1*, 48–59.

Lukman, N. (2016). Studi Implementasi Aplikasi Manajemen Ruang Kelas "Netop School" Berbasikan Local Area Network (LAN). *Jurnal Sains Dan Teknologi Utama*, *XI*(152), 1–14.

Manuaba, I. B. V. H., Hidayat, R., & Kusumawardani, S. S. (2012). Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas. *Jnteti*, *1*(1), 5. https://doi.org/10.22146/JNTETI.V1I1.3

Muhartin, A. (2017). IMPLEMENTASI SISTEM MONITORING JARINGAN WIRELESS DENGAN METODE NETWORK SECURITY MONITORING (NSM). *Journal of Chemical Information and Modeling*, *53*(9), 1689–1699. https://doi.org/10.1017/CBO9781107415324.004

Nirsal, & Ali, M. (2017). DESAIN DAN IMPLEMENTASI UIAN NASIONAL BERBASIS KOMPUTER PADA SMA NEGERI 6 PALOPO. *Prosiding Seminar Nasional*, *03*(1), 241–352.

Nurdin, N. (2015). Analisis Adopsi Dan Pemanfaatan Internet Di Kalangan Mahasiswa Perguruan Tinggi Di Kota Palu. *JURNAL ELEKTRONIK SISTIM INFORMASI DAN KOMPUTER (JESIK)*, *1*(1), 1–13.

Journal of Information System and Technology, Vol.01 No. 02, Nov 2020, pp.
ISSN: -

Putra, R. A. (2018). ANALISA IMPLEMENTASI ARSITEKTUR MICROSERVICES BERBASIS KONTAINER PADA KOMUNITAS PENGEMBANG PERANGKAT LUNAK SUMBER TERBUKA (OPENDAYLIGHT DEVOPS COMMUNITY), *1*, 150–162.

Rahim, A. (2016). Rancang Model Sistem Keamanan Menggunakan Intrusion Prevention System Dengan Metode Rule Based : Studi Kasus KPDE Provinsi Jambi. *Jurnal Ilmiah Media SISFO*, *10*(2), 190–205.

Riadi, I. (2014). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *JUSI, Universitas Ahmad Dahlan Yogyakarta*, *1*(1), 71–80. https://doi.org/10.2307/2137776

Saputra, T. T., Irawan, B., & Ilhamsyah. (2014). Aplikasi Antrian Nasabah Bank Menggunakan Teks Dan Suara Berbasis Jaringan Wireless Lokal Area Network (WLAN). *Jurnal Coding Sistem Komputer Universitas Tanjungpura*, *02*(2), 1–7.

Supatmi, S., Nizar, T. N., & Fahlevi, R. (2014). Sistem Kontrol Peralatan Rumah Dan Monitoring Kondisi Rumah Melalui Internet Berbasis Web Dan Openwrt. *Jurnal Teknik Komputer Unikom – Komputika – Volume 3, No.2 - 2014 SISTEM*, *3*(2), 23–28. Retrieved from http://komputika.tk.unikom.ac.id/_s/data/jurnal/v3no2/1-srisupatmi.pdf/ori/1-srisupatmi.pdf

Susianto, D., & Yulianti, I. (2015). MENGAMANKAN WIRELESS DENGAN MENGGUNAKAN TWO FACTOR, PASSWORD DAN MAC ADDRESS FILTERING. *Expert-Jurnal Manajemen Sistem Informasi Dan Teknologi MENGAMANKAN*, *5*(2), 28–37.

Syaimi, A., Utami, P., Lidyawati, L., & Ramadhan, Z. (2013). Perancangan dan Analisis Kinerja Sistem Pencegahan Penyusupan Jaringan Menggunakan Snort IDS dan Honeyd. *Jurnal Reka Elkomika TeknikElektro | Itenas Jurnal Online Institut Teknologi Nasional Jurnal Reka Elkomika*, *1*(4), 2337–2439.

Tambunan, B., Raharjo, W. S., & Purwadi, J. (2013). Desain dan Implementasi Honeypot dengan Fwsnort dan PSAD sebagai Intrusion Prevention System. *1 / Vol.5 / September 2013*, *1*(0), 1–7. https://doi.org/Bosman Tambunan, Willy Sudiarto Raharjo, Joko Purwadi

Varianto, E., & Badrul, M. (2015). Implementasi Virtual Private Network dan Proxy Server Menggunakan Clear OS Pada PT. Valdo International. *Jurnal Teknik Komputer AMIK BSI*, *1*(1), 54–65.

Wardoyo, S., Ryadi, T., & Fahrizal, R. (2014). Analisis Performa File Transport Protocol Pada Perbandingan Metode IPv4 Murni, IPv6 Murni Dan Tunneling 6to4 Berbasis Router Mikrotik. *Jurnal Nasional Teknik Elektro*, *3*(2), 106–117.