ANALISA KEAMANAAN JARINGAN KOMPUTER MENGGUNAKAN SISTEM DETEKSI INTRUSI SHOREWALL

SKRIPSI

OLEH

SUGI APRIANTI
NPM. 18020025

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN BENGKULU
2022

ANALISA KEAMANAAN JARINGAN KOMPUTER MENGGUNAKAN SISTEM DETEKSI INTRUSI SHOREWALL

SKRIPSI

SUGI APRIANTI
NPM. 18020025

Diajukan sebagai salah satu syarat untuk mendapat gelar Sarjana Komputer di Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu

PROGRAM STUDI REKAYASA SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS DEHASEN BENGKULU
2022

ANALISA KEAMANAAN JARINGAN KOMPUTER MENGGUNAKAN SISTEM DETEKSI INTRUSI SHOREWALL

SKRIPSI

OLEH:

SUGI APRIANTI
NPM. 18020025

Disetujui Oleh:

Pembimbing I,	Pembimbing II,
Riska, S.Kom., M.Kom	**Hendri Alamsyah, S.Kom., M.Kom**
NIDN.0224019201	NIDN. 0211039102

Mengetahui,
Ketua Program Studi
Rekayasa Sistem Komputer

Toibah Umi Kalsum, S.Kom., M.Kom
NIDN.02.060573.01

ANALISA KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN SISTEM DETEKSI INTRUSI *SHOREWALL*

SKRIPSI

SUGI APRIANTI
NPM: 18020025

Telah dipertahankan di depan TIM penguji Universitas Dehasen Bengkulu pada:

Hari : Jumat

Tanggal : 16 Juni 2023

Skripsi ini telah diperiksa dan disahkan oleh:

Penguji	Nama	NIDN	Tanda Tangan
Ketua Penguji	Riska, S.Kom., M.Kom.	02.240192.01	
Anggota	Hendri Alamsyah, S.Kom., M.Kom.	02.110391.02	
Anggota	Toibah Umi Kalsum, S.Kom., M.Kom.	02.060573.01	
Anggota	Yessi Mardiana, S.Kom., M.Kom	02.030288.02	

Mengetahui,

Dekan Fakultas Ilmu Komputer

Siswanto, S.E., S.Kom., M.Kom
NIDN. 02.240363.01

BAB 1 RIWAYAT HIDUP
BAB 2

Penulis bernama Sugi Aprianti, dilahirkan di Kembang Seri Kecamatan Bermani llir, Kabupaten Kepahiang, Provinsi Bcngkulu, pada tanggal 6 Juni 1993, anak kelima dari lima bersaudara, Ayah bemama Zainudin dan lbu bernama Ratnawati. Menyelesaikan pendidikan di Sekolah Dasar Negeri (SDN) 03 Kembang Seri pada tahun 2005. Kemudian penulis melanjutkan pendidikan pada Sekolah Menengah Pertama Negeri (SMP) 01 Keban Agung Bermani llir pada tahun 2008 dan selanjutnya mcnyelesaikan pendidikan MAS 01 Darussalam pada tahun 2011. Kemudian penulis melanjutkan Pendidikan ke Perguruan Tinggi yaitu pada Universitas Dchasen (UNIVED) Bengkulu dengan mengambil jurusan Rekayasa Sistem Komputer pada Fakultas llmu Komputer, untuk jenjang Strata Satu (S-1) pada tahun 2018.

BAB 3 MOTTO DAN PERSEMBAHAN

BAB 4

BAB 5 MOTTO

BAB 6

Tidak ada satupun perjuangan yang tidak melelahkan. “Dan Kami pasti akan menguji kamu dengan sedikit ketakutan, kelaparan, kekurangan harta, jiwa, dan buah-buahan. Dan sampaikanlah kabar gembira kepada orang-orang yang sabar, (yaitu) orang-orang yang apabila ditimpa musibah, mereka berkata "Innā lillāhi wa innā ilaihi rāji'ūn" [1] (sesungguhnya kami milik Allah dan kepada-Nyalah kami kembali)”. QS. Al Baqarah: 155-156.

PERSEMBAHAN

BAB 7 Dengan mengucapkan alhamdulillah atas semua limpahan rahmat dan kasih sayang-Mu, akhirnya tercapai juga amanah, kewajiban dan tujuan serta cita – cita. Aku yakin ini bukan akhir dari perjalanan dan perjuanganku, namun langkah awal untuk mewujudkan mimpi dan membahagiakan orang yang aku kasihi dan mengasihiku. Aku persembahkan karya kecilku ini dengan sepenuh cinta untuk:

- Kedua orang tuaku, Ayah dan Ibuku tercinta
- Keluargaku serta kakakku yang sangat aku sayangi
- Kedua Dosen Pembimbing
- Teman – teman seperjuanganku
- Serta almamater tercinta.

ABSTRAK

ANALISA KEAMANAAN JARINGAN KOMPUTER MENGGUNAKAN SISTEM DETEKSI INTRUSI SHOREWALL

Oleh :

Sugi Aprianti(1)

Riska, M.Kom(2)

Hendri Alamsyah, M.Kom(2)

Penelitian ini bertujuan untuk membangun sistem pendeteksi gangguan dalam jaringan berbasis Network Intrusion Detection System (NIDS) menggunakan Shorewall, serta mengetahui cara kerja dari shorewall dalam mencegah dan mengatasi sistem keamanan jaringan komputer SMK N 3 Kepahiang. Penelitian ini menggunakan metode penelitian eksprimen. Pada penelitian ini dilakukan analisa yang akan dijadikan sebagai bahan untuk Implementasi sistem deteksi intrusi menggunaakn metode Network Intrusion Detection System (NIDS) dengan memanfaatkan tools shorewall. Hasil eksprimen selanjutnya didokumentasikan untuk melakukan analisis sehingga dihasilkan rekomendasi yang tepat untuk sistem keamanan menggunakan deteksi intrusi shorewall. Hasil penelitian ini menunjukkan Shorewall dapat diterapkan pada jaringan menggunakan 2 interface yang dapat digunakan untuk terhubung ke jaringan internet dan juga jaringan lokal, shorewall juga dapat digunakan sebagai sistem deteksi intrusi untuk Mac clone dan DDoS attack yang dapat dilakukan dalam jaringan sehingga dapat melakukan reject terhadap aktifitas mac clone dan DDoS attack. Penerapan shorewall sebagai sistem deteksi intrusi tidak mempengeruhi kualitas layanan, dimana dari hasil pengujian Berdasarkan ITU G.114 masih dikategorikan baik dengan nilai dari delay sebesar 1.92 ms, jitter sebesar 33.3 ms, packet loss sebesar 0%, dan throughput sebesar 548 kb.

Kata kunci : Shorewall, NIDS, Mac *Clone*, DDoS, Kualitas Layanan.

1) Penulis
2) Dosen Pembimbing

BAB 8 ***ABSTRACT***

BAB 9

BAB 10 ***AN ANALYSIS OF COMPUTER NETWORK SECURITY USING SHOREWALL INTRUSION DETECTION SYSTEM***

BAB 11

BAB 12 **By:**

BAB 13 **Sugi Aprianti(1)**

BAB 14 **Riska(2)**

BAB 15 **Hendri Alamsyah(2)**

BAB 16

BAB 17 *This study aims to build a network intrusion detection system based on the Network Intrusion Detection System (NIDS) using Shorewall, and to find out how the shorewall works in preventing and overcoming the computer network security system at SMK N 3 Kepahiang. This study uses experimental research methods. In this study, an analysis was carried out which would serve as material for the implementation of an intrusion detection system using the Network Intrusion Detection System (NIDS) method by utilizing shorewall tools. The experimental results are then documented to carry out analysis so that appropriate recommendations are produced for security systems using shorewall intrusion detection. The results of this study indicate that Shorewall can be applied to networks using 2 interfaces that can be used to connect to the internet network and also local networks, shorewall can also be used as an intrusion detection system for Mac clones and DDoS attacks that can be carried out on the network so that it can reject activities mac clone and DDoS attacks. Application of shorewall as an intrusion detection system does not affect service quality, where based on ITU G.114 test results it is still categorized as good with a delay value of 1.92 ms, jitter of 33.3 ms, packet loss of 0%, and throughput of 548 kb.*

BAB 18 Keywords : Shorewall, NIDS, Mac Clone, DDoS, Quality of Service.

BAB 19 1) Author

BAB 20 2) Supervisor

PROGRAM STUDI INFORMATIKA
FAKULTAS KOMPUTER
UNIVERSITAS DEHASEN BENGKULU

SURAT PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan dibawah ini :

Nama : Sugi Aprianti

NPM : 18020025

Program Studi : Rekayasa Sistem Komputer

Menyatakan dengan sesungguhnya bahwa :

1. Selama melakukan penelitian dan pembuatan skripsi ini saya tidak melakukan pelanggaran etika akademik dalam bentuk apapun atau pelanggaran lain yang bertentangan dengan etika akademik.
2. Skripsi yang saya buat merupakan karya ilmiah saya sebagai penulis, bukan jiplakan atau karya orang lain.
3. Apabila di kemudian hari ditemukan bukti yang meyakinkan bahwa dalam proses pembuatan skripsi ini terdapat pelanggaran etika kademik atau skripsi ini hasil jiplakan atau skripsi ini hasil kerja orang lain, maka saya bersedia menerima sanksi akademik yang ditetapkan oleh Universitas Dehasen.

Demikian Surat Pernyataan ini saya buat dengan sebenarnya untuk dipergunakan bilamana perlu.

Bengkulu, 06 Juni 2023
Yang Menyatakan,

Sugi Aprianti
NPM.18020025

BAB 21

BAB 22

BAB 23 KATA PENGANTAR

Puji syukur alhamdulillah penulis panjatkan kehadirat Allah SWT, karena berkat ridho, rahmat, dan hidayah-Nya maka skripsi yang berjudul "Analisa Keamanaan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall" dapat diselesaikan sebagaimana mestinya. Yang mana skripsi ini merupakan salah satu syarat untuk mendapat gelar Sarjana Komputer di Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

Dalam menyelesaikan skripsi ini, penulis menyadari masih banyak mengalami kesulitan, namun atas kerja keras dan bimbingan, petunjuk serta pengarahan dari berbagai pihak akhirnya penulis dapat menyelesaikan penelitian ini.

Pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah banyak membantu, memberikan bimbingan, dan semangat serta doa sehingga penelitian ini dapat diselesaikan, oleh sebab itu izinkanlah penulis menyampaikan rasa terima kasih kepada :

1. Prof. Dr. Husaini, SE., M.Si, Ak, CA, CRP selaku Rektor Universitas Dehasen (UNIVED) Bengkulu.
2. Bapak Siswanto, S.E., S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer di Universitas Dehasen (UNIVED) Bengkulu.
3. Ibu Toibah Umi Kalsum, S.Kom., M.Kom selaku Ketua Program Studi Rekayasa Sistem Komputer di Universitas Dehasen (UNIVED).
4. Bapak Riska, S.Kom., M.Kom Selaku Pembimbing I (satu) dalam skripsi ini.

5. Bapak Hendri Alamsyah, S.Kom., M.Kom Selaku Pembimbing II (dua) dalam skripsi ini.
6. Kedua orang tuaku yang memberikan dorongan serta semangat dan doa kepadaku.
7. Rekan - rekan dan semua pihak yang turut memberikan saran dan kritikan sehingga skripsi ini dapat diselesaikan dengan baik.

Penulis menyadari bahwa dalam penulisan skripsi ini jauh dari sempurna, sehingga banyak kekurangan dan kesalahan, maka dari itu penulis sangat memerlukan kritik dan saran yang sifatnya membangun dari berbagai pihak untuk kesempurnaan skripsi ini.

Akhirnya penulis berharap agar skripsi ini dapat berguna dan bermanfaat bagi mahasiswa Universitas Dehasen Bengkulu khususnya dan pembaca pada umumnya.

Bengkulu, 2022

Penulis

DAFTAR ISI

Halaman

BAB 24 DAFTAR GAMBAR

Gambar Halaman

BAB 25

DAFTAR TABEL

BAB 26

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam penggunaan jaringan komputer saat ini, faktor keamanan terhadap jaringan komputer menjadi salah satu hal yang penting untuk dilakukan sebagai upaya pencegahan dari penyalahgunaan *resource* atau sumber daya pada jaringan yang tidak sah, serta mengantisipasi resiko ancaman terhadap jaringan baik secara langsung ataupun tidak langsung. Hal ini dilakukan untuk memastikan terjaganya lalu lintas data dalam jaringan komputer untuk menghindari serangan yang dapat menyebabkan kenaikan trafik atau lalu lintas data di dalam jaringan.

SMK Negeri 3 Kepahiang merupakan salah satu Instansi Pendidikan di tingkat menengah kejuruan yang dalam kegiatasn pembelajaran juga sudah menggunakan jaringan komputer. Dimana hasil observasi dan wawancara yang sudah dilakukan SMK Negeri 3 Kepahiang ini memiliki sumber jaringan internet dengan *bandwidth* sebesar 20 Mbps. Jaringan internet yang ada di SMK Negeri 3 Kepahiang ini dapat diakses untuk kegiatan belajar dan mengajar, baik oleh Guru, Staf dan juga Siswa – Siswi di Sekolah tersebut. Dalam penggunaan jaringan internet ini, SMK Negeri 3 Kepahiang belum menggunakan sistem keamanan jaringan hanya memanfaatkan sistem keamanan yang ada pada Komputer ataupun laptop *client* saja, yang mana *client* tersebut langsung terhubung ke Modem yang disediakan oleh ISP atau penyedia layanan internet. Dalam keadaan ini tentu saja jaringan internet yang ada pada SMK Negeri 3 Kepahaiang ini tidak terlepas dari adanya

kesalahan jaringan ataupun gangguan seperti terjadi *loss* akses yang menyebabkan tidak dapat terhubung lagi ke jaringan internet yang berkemungkinan terjadi gangguan berupa MAC *clone*, selain itu berdasarkan hasil wawancara yang telah dilakukan, pernah terjadi blank screen terhadap komputer laboratorium, yang setelah ditelusuri itu terjadi karena ulah dari siswa – siswi yang sedang menggunakan komputer melakukan uji coba membanjiri jalur akses atau sering disebut dengan DDOS *attack* untuk menjaili temannya.

Untuk mengatasi masalah ini, dapat diterapkan suatu sistem yang dapat mendeteksi adanya kesalahan di dalam jaringan atau yang biasa disebut sistem intrusi deteksi yang dapat mengawasi lalu lintas data dalam jaringan dengan menggunakan metode *Network Intrusion Detection System* (NIDS). NIDS ini merupakan teknik yang dapat digunakan untuk melihat ataupun memantau *Traffic* keluar dan masuk ataupun *Traffic* di antara *host* atau di antara segmen jaringan lokal. Dalam melakukan pemantauan menggunakan NIDS ini, seorang administrator jaringan dapat membuka *log* dari NIDS yang terletak pada NIDS *Server* baik menggunakan perintah *Command Line* (CLI) ataupun *log* yang sudah di intergrasikan pada aplikasi berbasis *web*.

Salah satu aplikasi ataupun tools yang dapat digunakan sebagai NIDS ini adalah shorewall. Shorewall adalah salah satu *tools firewall* pada linux yang berbasiskan *iptables*, shorewall juga menerapkan konsep zona ataupun wilayah yang dapat memudahkan dalam menentukan aturan dari *firewall* untuk mengamankan jaringan komputer. Dengan menggunakan shorewall ini, jaringan komputer bukan saja dapat di mengawasi ataupun mendeteksi

adanya intrusi tetapi juga dapat menerapkan aturan untuk memutus ataupun melakukan pembatasan terhadap koneksi yang tidak sah.

Dari uraian latar belakang di atas, penulis tertarik untuk mengangkat judul penelitian "*Analisa Keamanaan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall"*.

1.2 Rumusan Masalah

Dari latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah bagaimana menganalisis dan mengimplementasikan Keamanaan Jaringan Komputer Menggunakan Sistem Deteksi Intrusi Shorewall?

1.3 Batasan Masalah

Dari latar belakang dan rumusan masalah yang sudah penulis jabarkan diatas, batasan masalah dalam penelitian ini adalah sebagai berikut.

1. *Server* menggunakan Sistem Operasi Linux Ubuntu *Server* 20.04 64bit
2. Pengujian keamanan difokuskan pada:
    a. Deteksi Serangan Mac *Clone*.
    b. Deteksi DDoS *Attack*.
    c. *Rules* atau Aturan Pembatasan.

1.4 Tujuan Penelitian

A. Tujuan Umum

Untuk memenuhi syarat melanjutkan skripsi pada Program Studi Rekayasa Sistem Komputer Fakultas Ilmu Komputer Universitas Dehasen Bengkulu.

B. Tujuan Khusus

1. Membangun sistem pendeteksi gangguan dalam jaringan berbasis Network Intrusion Detection System (NIDS) menggunakan Shorewall.
2. Mengetahui cara kerja dari shorewall dalam mencegah dan mengatasi sistem keamanan jaringan komputer SMK N 3 Kepahiang.

1.5 Manfaat Penelitian

A. Bagi Penulis

Dapat dijadikan sebagai bahan pembelajaran dalam perancangan infrastruktur keamanan jaringan dengan *Network Intrusion Detection System* (NIDS) menggunakan shorewall.

B. Bagi Pembaca

Dapat dijadikan sebagai referensi untuk penulisan berikutnya yang berhubungan dengan jaringan komputer terutama perancangan infrastruktur keamanan jaringan dengan *Network Intrusion Detection System* (NIDS) menggunakan shorewall.

BAB II
LANDASAN TEORI

2.1 Analisa

Menurut Arifin. dkk. (2022:1), Analisa merupakan penelitian terhadap suatu sistem yang telah ada dengan tujuan untuk merancang sistem baru atau yang akan diperbaharui sehingga dapat menyelesaikan suatu permasalahan dengan cara membagi – baginya menjadi bagian – bagian yang saling berkaitan.

Menurut Fau. dkk (2017:12), analisa adalah Analisa adalah merupakan suatu proses merinci terhadap objek dengan alat bantu tertentu, kedalam beberapa komponen yang saling berhubungan dengan menilai dan mengetahui perbedaan dari kedua objek tersebut yang berbeda.

2.2 Sistem Keamanan Jaringan

Menurut Riza (2016:1), sistem keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi pengguna yang tidak sah (penyusup) dari jaringan komputer. Tujuannya adalah untuk mengantisipasi resiko jaringan komputer yang dapat berupa ancaman fisik maupun logik. Yang dimaksud ancaman fisik itu adalah yang merusak bagian fisik komputer atau hardware komputer sedangkan ancaman logik yaitu berupa pencurian data atau penyusup yang membobol akun seseorang.

Menurut Ikhwan dan Elfitri (2014:119), keamanan jaringan pada intinya adalah mengendalikan akses terhadap sumberdaya jaringan. Akses

jaringan dikontrol agar bisa diakses oleh siapa saja yang berhak dan menghalangi orang atau subjek yang tidak terdaftar untuk mengaksesnya.

Prinsip keamanan jaringan di klasifikasikan menjadi 3 bagian :

A. *Confidentiality* (Kerahasiaan)

Confidentiality mengacu pada kerahasiaan sebuah objek, dimana sebuah objek dijaga agar tidak diakses oleh subjek yang tidak berhak. Istilah ini juga mengacu pada data pribadi yang diberikan kepada pihak lain untuk keperluan tertentu dan hanya digunakan untuk keperluan tersebut. Contoh data-data yang sifatnya pribadi itu adalah nama, nomor kartu kredit, nomor paspor, nomor telepon, *password* komputer, agama, status perkawinan dan lain-lain. Ada banyak *tool* yang digunakan untuk menjaga agar kerahasiaan sebuah subjek terjaga dengan baik, diantaranya Enkripsi, Akses Kontrol, otentifikasi, otorisasi dan keamanan fisik.

B. *Integrity* (Integritas)

Integrity mengacu pada objek yang tetap asli (original), dimana objek tidak berubah di perjalanan hingga sampai ke tujuan dari objek tersebut. Sebagai contoh, email yang dikirim oleh seseorang bisa dicegat ditengah jalan kemudian diubah isinya dan selanjutnya baru dikirim ke penerima sebenarnya sehingga data yang diterima oleh penerima telah berubah dari yang diinginkan oleh pengirim. Bentuk serangan terhadap aspek *integrity* diantaranya adalah virus, trojan horse, atau pemakai lain yang berada ditengah komunikasi. Untuk mengatasi hal tersebut, maka perlu dibuat mekanisme proteksi agar data tidak bisa diubah oleh pihak-pihak yang tak diizinkan. *Tool* yang digunakan untuk menjaga hal itu

terlaksana diantaranya adalah *Checksums*, Data *correcting codes* dan *backup*.

C. *Availability* (Ketersediaan)

Availability mengacu pada ketersediaan *resource* dengan tepat, dimana user mempunyai hak akses tepat waktu dan tidak terkendala apapun. Salah satu serangan terhadap aspek *availability* adalah serangan *Distributed Denial of Service* (DDoS *Attack*). Tujuan utama dari DDoS *attack* adalah memenuhi *resource* yang dibutuhkan oleh user sehingga *user* tidak bisa menggunakan *resource* tersebut sebagaimana harusnya.

Pengiriman data yang berlebihan baik dari besar paket maupun jumlah paket kedalam suatu jaringan dan umumnya merupakan data yang tidak berguna disebut dengan *Flooding* Data, ada kalanya data ang berbeda dalam *Traffic* merupakan data yang tidak perlu. Data tersebut memang sengaja dikirim oleh seseorang meneruskan jaringan data yang ada. Pengiriman data tersebut dapat mengakibatkan lambatnya jalur *Traffic* yang ada dalam jaringan dan juga bisa mengakibatkan kerugian lain yang cukup berarti, misalnya kerusakan program karena adanya intruder yang masuk kedalam jaringan. *Traffic* data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Pada jam sibuk *Traffic* suatu data akan sangat padat, sehingga *Traffic* data tersebut akan terganggu. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan keterlambatan dalam pengiriman dan penerimaan data. *Traffic* data yang ada dalam suatu jaringan akan mengalami turun naik selama pemakaiannya. Pada

jam sibuk *Traffic*suatu data akan sangat padat, sehingga *Traffic* data tersebut akan terganggu. Baik data yang akan dikirim maupun data yang akan datang akan mengalami antrian data yang mengakibatkan kelambatan dalam pengiriman dan penerimaan data. Adapun macam – macam dari *flooding attack* yang sering di lakukan dalam jaringan adalah sebagai berikut:

1. ICMP *Flooding* (*Ping of Death)*

   ICMP *Flooding* atau yang biasa disebut dengan *Ping of Death* merupakan suatu teknik pengiriman paket *echo request* ICMP kedalam suatu jaringan secara berlebihan. Pengiriman paket ini dapat mengakibatkan sistem *crash*, hang atau *reboot*.

2. *Smurf Attack*

   Hampir sama dengan *ping of death* tetapi untuk *smurf attack* paket ICMP tidak dikirim secara langsung ke korban, melainkan melalui perantara. Pada awalnya dikirim sebuah paket ICMP *echo request* kesebuah *host* lain, paket ini bertujuan agar *host* tersebut mengirimkan paket ICMP *ping* secara terus menerus ke korban terakhirnya.

3. SYN *Flooding*

   SYN *Flooding* terjadi bila suatu host hanya mengirimkan paket SYN TCP saja secara kontinyu tanpa mengirimkan paket ACK sebagai konfirmasinya. Hal ini akan menyebabkan *host* tujuan akan terus menunggu paket tersebut dengan menyimpannya kedalam *back log*. Meskipun besaran paketnya kecil, tetapi apabila pengiriman

SYN tersebut terus menerus akan memperbesar *back log*. Hal yang terjadi apabila *back log* sudah besar akan mengakibatkan *host* tujuan akan otomatis menolak semua paket SYN yang datang, sehingga *host* tersebut tidak bisa dikoneksi oleh host yang lain.

4. UDP *Flooding*

   Pengiriman data UDP secara berlebihan kedalam suatu jaringan, pengiriman UDP *flood* ini akan membentuk suatu jalur hubungan dengan suatu servis UDP dari host tujuan. *Flood* UDP ini akan mengirimkan karakter yang akan mengetes jaringan korban. Sehingga terjadi aliran data yang tidak perlu dalam jaringan korban tersebut.

5. Serangan MAC *Clone*

   Serangan MAC-*clone* merupakan serangan yang sering terjadi pada mikrotik, dimana satu *user* dapat digunakan untuk login lebih dari satu orang atau dapat disebut duplikasi. Jika masalah MAC-*clone* tidak segera ditangani maka akan berdampak negatif pada sistem keamanan *user*, sehingga autoritas pemilik *user* sudah tidak menjadi bahan pertimbangan. Berdasarkan data yang didapat, dalam satu bulan bisa terjadi serangan sampai tiga puluh kali bahkan bisa lebih dari itu. Hal ini sangat merugikan pemilik user, terutama dalam segi *bandwidth*, koneksi, serta pada kecepatan akses internet. Jika serangan MAC-*clone* tidak segera ditangani hal tersebut akan sangat mengganggu aktivitas *user*, memang tidak berdampak pada *Server*, melainkan berdampak pada *user*. Secara tidak langsung dampak

negatif akibat serangan MAC-*clone* dapat dirasakan, seperti tidak lancarnya proses pencarian pada *browser* dan proses pencarian yang lain sehingga menghambat kegiatan belajar mengajar disaat menggunakan akses wifi yang tersedia.

2.3 *Intrusion Detection System* (IDS)

Menurut Alamsyah et al.(2020:18), IDS (*Intrution Detection System*) adalah sebuah sistem yang melakukan pengawasan terhadap *Traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Jika ditemukan kegiatan yang mencurigakan berhubungan dengan *Traffic* jaringan maka IDS akan memberikan peringatan kepada sistem atau administrator jaringan

Menurut Muqorobin et al. (2019:2), IDS adalah sebuah aplikasi perangkat keras atau perangkat lunak yang otomatis bekerja untuk memonitor kejadian pada sebuah jaringan komputer dan sekaligus menganalisais masalah keamanan jaringan. Sasaran IDS adalah memonitoring aset jaringan sehingga dapat mendeteksi perilaku yang tidak lazim, kegiatan yang tidak sesuai, searngan atau menghentikan serangan (penyusupan) dan bahkan menyediakan informasi untuk menelusuri penyerang.

Menurut Atmojo (2018:176), Informasi yang diperlukan dari sebuah IDS adalah informasi mengenai adanya serangan yang terjadi saat itu sehingga system administrator dapat melakukan pencegahan terhadap dampak dari serangan tersebut. Di satu sisi, peringatan ini bermanfaat, tapi di sisi lain diperlukan petugas yang melakukan pengawasan terhadap IDS ini secara terus menerus. IDS *(Intrution Detecting System*) adalah sebuah perangkat

lunak atau perangkat keras yang bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan menganalisis masalah keamanan jaringan. Terdapat dua jenis IDS berdasarkan penempatannya, yaitu:

A. *Host Based IDS* (HIDS)

HIDS hanya melakukan pemantauan tertentu dalam jaringan. HIDS biasanya pada perangkat komputer akan memantau kejadian seperti kesalahan *login* berkali-kali dan melakukan pengecekan pada file. Hal yang perlu diperhatikan pada implementasi IDS adalah perihal *false positive* dan *false negative*. *False positive* adalah peringatan serangan yang dihasilkan oleh IDS akan sebuah paket normal pada sistem yang dimonitor. *False negative* adalah sebuah serangan yang benar – benar terjadi namun terlewatkan oleh IDS sehingga IDS tidak akan menghasilkan peringatan apapun atas serangan tersebut. IDS dapat melewatkan serangan karena serangan tersebut tidak dikenali oleh IDS atau karena penyerang berhasil menggunakan sebuah metode serangan yang dapat menghindari IDS

B. *Network Based* IDS (NIDS)

NIDS akan melakukan pemantauan terhadap seluruh bagian pada jaringan dengan mengumpulkan paket-paket data yang terdapat pada jaringan tersebut serta melakukan analisa dan menentukan apakah paket paket tersebut merupakan paket normal atau paket serangan.

Menurut Muqorobin et al. (2019:2), *Network Intrusion Detection System* (NIDS) merupakan salah satu IDS yang ditempatkan di salah satu titik sebuah jaringan dan berfungsi untuk memantau serta menganalisis

lalu lintas paket data dalam jaringan. NIDS merupakan strategi yang efektif untuk melihat *Traffic* masuk keluar ataupun *Traffic* di antara *host* atau di antara segmen jaringan lokal. NIDS biasanya dikembangkan di depan dan di belakang *firewall* dan VPN *gateway* untuk mengukur keefetifan peranti-peranti keamanan tersebut dan berinteraksi dengan mereka untuk memperkuat keamanan jaringan.

Menurut Masse, dkk (2015:5), Semua lalu lintas yang mengalir ke sebuah jaringan akan dianalisis untuk mencari apakah ada percobaan serangan atau penyusupan ke dalam sistem jaringan. NIDS umumnya terletak di dalam segmen jaringan penting di mana *Server* berada atau terdapat pada "pintu masuk" jaringan. Kelemahan NIDS adalah bahwa NIDS agak rumit diimplementasikan dalam sebuah jaringan yang menggunakan *switch ethernet*, meskipun beberapa vendor *switch ethernet* sekarang telah menerapkan fungsi IDS di dalam *switch* buatannya untuk memonitor *port* atau koneksi.

2.4 Shorewall

Menurut Yanti and Effendi (2020:16), Shorewall (*Shoreline Firewall*) merupakan salah satu *firewall* yang handal dan murah untuk digunakan di sistem operasi Linux selain *Ipchains* dan *Iptables*, shorewall juga mudah dikonfigurasi bagi penggunanya dan mengatur data yang diterima dan pengiriman data. Serta melakukan Ping pesan ICMP dalam proses Ping ACCEPT, DROP dan *REJECT*.

Menurut Supendar. dkk, (2019:126), Shorewall adalah salah satu *tools firewall* pada linux yang berbasiskan *iptables*. Dalam shorewall terdapat

konsep “zone” yang memudahkan untuk menentukan *policy firewall* dari pada melakukan konfigurasi secara manual dengan *iptables*. shorewall dapat menggambarkan persyaratan *firewall*/*gateway* menggunakan entri dalam satu set file konfigurasi. Shorewall membaca file-file konfigurasi dan dengan bantuan dari *iptables*, *iptables-restore*, ip dan *utilitas.* Untuk mengkonfigurasi Showrell, diperlukan setting beberapa file berikut:

1. etc/shorewall/zone.

   Berfungsi sebagai pendefinisi daerah asal *traffic* pada suatu *network*. *Server* tempat shorewall diinstal dikenal sebagai zona yang disebut fw. Pada file ini, *local* yang merupakan *interface* yang terhubung dengan jaringan *local* dan *net* merupakan *interface* yang terhubung dengan jaringan *network*.

2. /etc/shorewall/policy

   File ini berisi aturan untuk semua trafik yang lewat pada *firewall* diatur pada /etc/shorewall/*rules*, lakukan pemeriksaan file tersebut tidak terdefinisi pada /etc/shorewall/policy.

3. /etc/shorewall/*interface*

   Berfungsi sebagai penentu *interface* mana yang akan dihubungkan ke suatu zona, pada file ini, eth0 terkoneksi dengan jaringan internet dan eth1 terkoneksi dengan jaringan lokal.

4. /etc/shorewall/masq

   File ini untuk mendefinikan *masquerade* jaringan lokal dengan jaringan internet. Untuk men-*setting* apakah trafik yang melalui eth1 akan dibungkus (di-*masquerade*) dengan dengan IP pada eth0.

5. /etc/shorewall/*rules*

   File ini berisi aturan-aturan dari semua trafik yang melewati *firewall* dalam jaringan komputer yang satu segmen dengan shorewall *Server*.

6. /etc/shorewall/shorewall.conf

   Berfungsi sebagai proses aktivasi Showrell supaya dapat dilakukan load saat startup dengan konfigurasi Startup_ENABLE = Yes.

2.5 Linux Ubuntu *Server*

Menurut Niko (2014:1), Linux merupakan sistem operasi yang bersifat *multi user* dan *multi tasking*. Artinya lebih dari satu *user* dapat masuk ke Linux yang sama pada waktu yang sama dan aplikasi yang berbeda. Linux juga *multi-tasking*, artinya *user* dapat mengeksekusi lebih dari satu proses (program) pada waktu yang sama. Linux menggunakan sebuah *license* yang bernama GNU *General Public License* (GNU/GPL). GNU *General Public License* memungkinkan suatu aplikasi (termasuk sistem operasi) secara bebas digunakan dan disebarluaskan dimana pengguna/penerima *software* berhak menerima kode asal (*source code*) dari aplikasi tersebut beserta semua hak yang diijinkan oleh penulis asli.

Menurut Akbar (2011:5), Ubuntu adalah distro Linux turunan Debian yang dikembangkan dengan tujuan utama menjadi distro Linux destop yang mudah digunakan dengan rilis stabil setiap 6 bulan sekali. Ubuntu berasal dari kata dalam bahasa Afrika kuno ubuntu yang maknanya kemanusiaan untuk semua (*humanity towards others*). Ubuntu sangat populer karena kemudahannya dan dukungan komuntas yang besar. Ubuntu berkomitmen

akan selalu gratis dan didistrisbusikan sebagai perangkat lunak bebas sumber terbuka (*free and opensource software*).

Ubuntu populer dengan sistem manajemen paket yang sangat anggun bernama apt (*Advanced Package Tool*) yang diwarisi dari Debian. Sistem manajemen paket ini otomatis mencarikan dependensi untuk suatu aplikasi yang akan diinstal dan menginstalkannya dari repositori ke sistem. Ubuntu selain memiliki apt yang amat praktis, juga mewarisi dpkg (*Debian Packager*) dan GDebi untuk mengelola program (paket) di dalam sistem. Ubuntu juga mewarisi katana bernama *Synaptic* yang merupakan tampilan grafis untuk apt yang mampu mempermudah pemakaian apt sehingga pengguna bisa cari cawang instal program dengan sangat gampang. *Synaptic* menjadi aplikasi yang diandalkan untuk instalasi program di Ubuntu. Tidak cuma mewarisi, Ubuntu juga punya *Ubuntu Software Center* yang jauh lebih intuitif daripada *Synaptic* dengan kemudahan dan kesederhanaan sekali klik untuk instal. Ubuntu adalah hasil kolaborasi raksasa tim pengembang dari *Canonical* dan pengguna di seluruh dunia baik melalui dunia nyata maupun melalui internet. Ubuntu tersedia dalam versi destop, *Server*, dan *netbook*. Arsitektur yang didukung 32bit dan 64bit serta mendukung lebih dari 55 bahasa termasuk Indonesia.

Menurut Putra (2012:1), Ubuntu *Server* adalah salah satu varian dari distro linux Ubuntu. Ubuntu *Server* merupakan linux ubuntu yang didesain untuk di install di *Server*. Perbedaan mendasar, di Ubuntu *Server* tidak tersedia GUI. Bagi orang awam pemakai desktop, jelas tidak ada manfaatnya, tapi bagi admin jaringan, warnet, kantor, *Server* dan perusahaan *webhosting*,

ubuntu *Server* merupakan solusi mudah dan *free* untuk membangun layanan seperti file *sharing*, *printer sharing* atau *webhosting*.

Jadi linux ubuntu *Server* merupakan sistem operasi yang bersifat *multi user* dan *multi tasking* yang didesain untuk di install di *Server* serta menggunakan sebuah *license* yang bernama GNU *General Public License* (GNU/GPL). Perbedaan mendasar, di Ubuntu *Server* tidak tersedia GUI.

2.6 Jaringan Komputer

Menurut Madcoms dalam Rahadjeng dan Ritapuspitasari (2018:53), Jaringan komputer merupakan kumpulan dari beberapa komputer dan peralatan penunjang lainnya yang terhubung dalam satu kesatuan dan saling terkoneksi.

Menurut Foruzen dalam Pratama (2014:21), Jaringan komputer merupakan hasil dari koneksi (hubungan) dari sejumlah perangkat atau komputer yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (komputer *desktop*, komputer jinjing, smartphone, PC *tablet*) dan perangkat penghubung (*router, switch, modem, wireless access point*).

A. Sifat – Sifat Dasar Jaringan Komputer

Menurut Pratama (2014:21), Jaringan komputer memiliki empat buah sifat dasar utama. Keempat sifat tersebut adalah sebagai berikut.

1. *Scalability*

   Jaringan komputer dapat disesuaikan dengan kebutuhan pengguna, dapat berkembang, dan mampu menghilangkan batasan – batasan geografis/lokasi.

2. *Resource Sharing*

   Jaringan komputer dapat digunakan untuk pemakaian bersama sumber daya yang ada (*resource sharing*). Sumber daya ini meliputi perangkat keras (*hardware*) dan perangkat lunak (*software*).

3. *Connectivity*

   Jaringan komputer mudah dihubungkan dan pengguna mudah terhubung ke dalam jaringan komputer. Untuk menciptakan hubungan ini, terdapat sejumlah perangkat penghubung di dalamnya. Perangkat – perangkat tersebut antara lain berupa *switch, modem, router, hub*.

4. Reliability

   Sebuah jaringan komputer memiliki keandalan di dalamnya untuk melayani para pengguna. Performansi sebuah jaringan komputer dapat diukur.

B. Jenis – Jenis Jaringan Komputer

Menurut Wongkar, dkk (2015:64), Dalam jaringan komputer, terdapat jenis-jenis jaringan yang berbeda. Diantaranya:

1. PAN (*Personal Area Network*)

   PAN adalah singkatan dari *personal area network*. Jenis jaringan komputer PAN adalah hubungan antara dua atau lebih sistem komputer yang berjarak tidak terlalu jauh. Biasanya Jenis jaringan yang satu ini hanya berjarak 4 sampai 6 meter saja. Jenis jaringan ini sangat sering kita gunakan.

2. LAN (*Lokal Area Network*)

   LAN adalah singkatan dari *lokal area network*. Jenis jaringan LAN ini sangat sering kita temui di warnet-warnet, kampus, sekolah ataupun perkantoran yang membutuhkan hubungan atau koneksi antara dua komputer atau lebih dalam suatu ruangan. Jaringan LAN juga merupakan jaringan yang sangat di pengaruhi oleh topologi jaringannya.

3. MAN (*Metropolitan Area Network*)

   MAN singkatan dari *metropolitan area network*. Jenis jaringan komputer MAN ini adalah suatu jaringan komputer dalam suatu kota dengan transfer data berkecepatan tinggi yang menghubungkan suatu lokasi seperti sekolah, kampus, perkantoran dan pemerintahan. Sebenarnya jaringan MAN ini adalah gabungan dari beberapa jaringan LAN. Jangkauan dari jaringan MAN ini bisa mencapai 10 - 50 kilo meter.

4. WAN (*Wide Area Network*)

   WAN singkatan dari *wide area network*. WAN adalah jenis jaringan komputer yang mencakup area yang cukup besar. contohnya adalah jaringan yang menghubugkan suatu wilayah atau suatu negara dengan negara lainnya.

C. Wireless *Local Area Network* (WLAN)

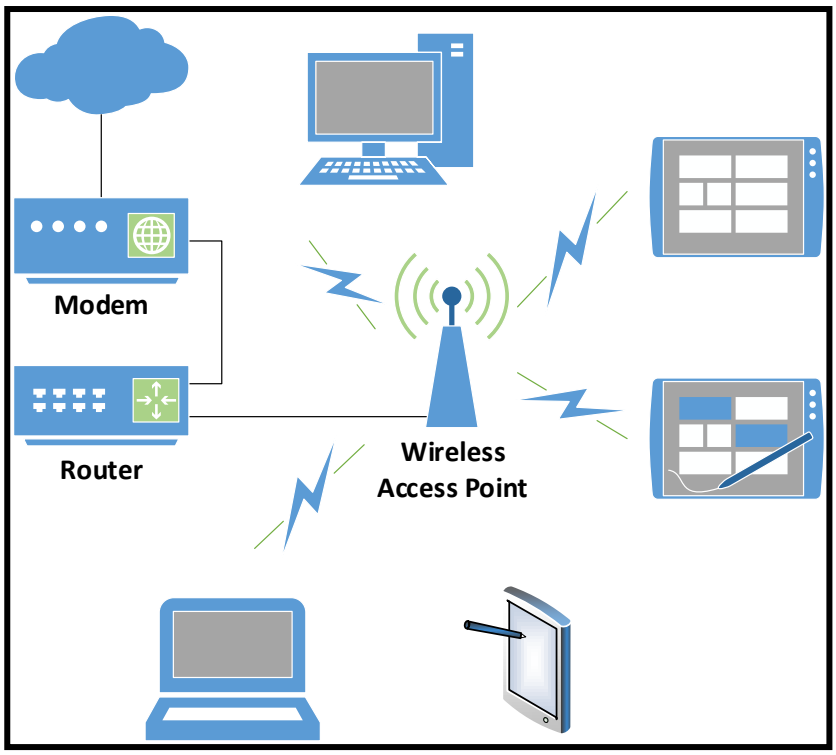
Menurut Wongkar (2017:64), *Wireless* LAN yang biasa disingkat dengan WLAN adalah sebuah sistem komunikasi data yang fleksibel yang dapat diaplikasikan sebagai ekstensi ataupun sebagai

alternatif pengganti untuk jaringan LAN kabel. *Wireless* LAN menggunakan teknologi frekuensi radio, mengirim dan menerima data melalui media udara, dengan meminimalisasi kebutuhan akan sambungan kabel. Dengan begitu, *wireless* LAN telah dapat mengkombinasikan antara konektivitas data dengan mobilitas user.

Menurut Sofana dalam Sharon, dkk (2014:36), pada dasarnya jaringan *wireless local area network* sama dengan jaringan LAN biasa, hanya saja proses transmisinya tidak memakai kabel tetapi memakai gelombang elektromagnetik atau infrared. Tetapi belakangan ini gelombang elektromagnetik lebih dominan digunakan. Jaringan *wireless* menggunakan *electromagnetic airwaves* untuk bertukar data ataupun informasi yang dibutuhkan. Gelombang radio biasa digunakan sebagai pembawa karena dapat dengan mudah mengirimkan daya ke penerima. Data ditransmisikan dengan cara ditumpangkan pada gelombang pembawa sehingga bisa diekstrak pada ujung penerima. Data ini umumnya digunakan sebagai pemodulasi dari pembawa oleh sinyal informasi yang sedang ditransmisikan.

Menurut Sharon, dkk (2014:36), Dalam konfigurasi biasa, pemancar dengan antena, yang disebut titik akses nirkabel atau *access point* (AP), terhubung ke LAN kabel dari lokasi tetap atau piring satelit yang menyediakan koneksi internet (ISP). AP menyediakan layanan internet untuk sejumlah *client* pada ruang lingkup geografis kecil (kisaran ratusan kaki / meter) itulah yang kita kenal dengan "*Hotspot*

Zone" atau *Hotspot*. (untuk memperluas jangkauan perlu menambah jumlah AP yang ada).



Gambar 2.1 Ilustrasi Jaringan WLAN

Sebagian besar WLAN saat ini berjalan pada standar yang dikenal sebagai 802.11b. standar ini juga dikenal sebagai Wi-Fi (*Wireless Fidelity*). WLAN menggunakan standar ini untuk melakukan komunikasi dengan kecepatan 11 Mbps. Sementara jaringan berkabel mempunyai kecepatan 100 Mbps. Tetapi standar baru dari Wi-Fi seperti 802.11a dan 802.11g, sudah mampu mentransmisi data dengan kecepatan 54Mbps.

D. Topologi Jaringan Komputer

Menurut Turban dalam Sharon, dkk (2014:36), Topologi jaringan adalah tata letak atau susunan fisik dan konektivitas pada sebuah ruang lingkup jaringan. Topologi jaringan komputer

menggambarkan struktur dari suatu jaringan atau bagaimana sebuah jaringan didesain. Dalam definisi topologi terbagi menjadi dua, yaitu topologi fisik (*physical topology*) yang menunjukan posisi pemasangan kabel secara fisik dan topologi logic (*logical topology*) yang menunjukkan bagaimana suatu media diakses oleh host.

1. Topologi Jaringan LAN

   LAN dapat dikembangkan dengan mudah dan mendukung kecepatan transfer data cukup tinggi. Ada 4 bentuk dasar LAN atau disebut juga topologi fisik LAN, antara lain sebagai berikut:

   a. Topologi *Bus*

      Topologi *bus* menggunakan sebuah kabel *backbone* dan semua *host* terhubung secara langsung pada kabel tersebut.

   b. Topologi *Ring* (Cincin)

      Topologi *ring* menghubungkan host dengan *host* lainnya hungga membentuk *ring* (lungkaran tertutup).

   c. Topologi *Star*

      Topologi *star* menghubungkan semua komputer pada sentral atau konsentrator. Biasanya konsentrator adalah sebuah *hub* atau *switch*.

   d. Topologi *Mesh* atau *Fully Mesh*

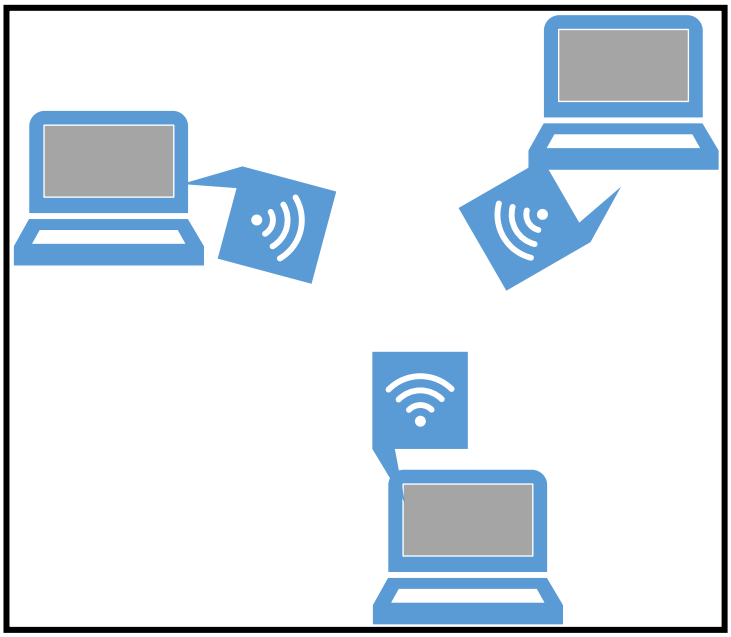
      Topologi mesh menghubungkan setiap komputer secara p*oint to point*. Artinya semua komputer akan saling terhubung satu – satu sehingga tidak dijumpai ada *link* yang putus.

2. Topologi Jaringan WLAN

Menurut Zam (2014:16), Topologi pada jaringan *wireless* terbagi dua jenis, yaitu: AdHoc dan Infrastruktur.

a. Topologi AdHoc

Dalam topologi AdHoc ini, komputer yang terhubung melalui *wireless* tidak menggunakan perantara, boleh dibilang sebagai koneksi *peer to peer*. Di mana koneksi jaringan yang dilakukan langsung antar komputer atau laptop. Topologi AdHoc ini dikenal pula dengan nama *Independent Basic Service Sets* (IBSS).

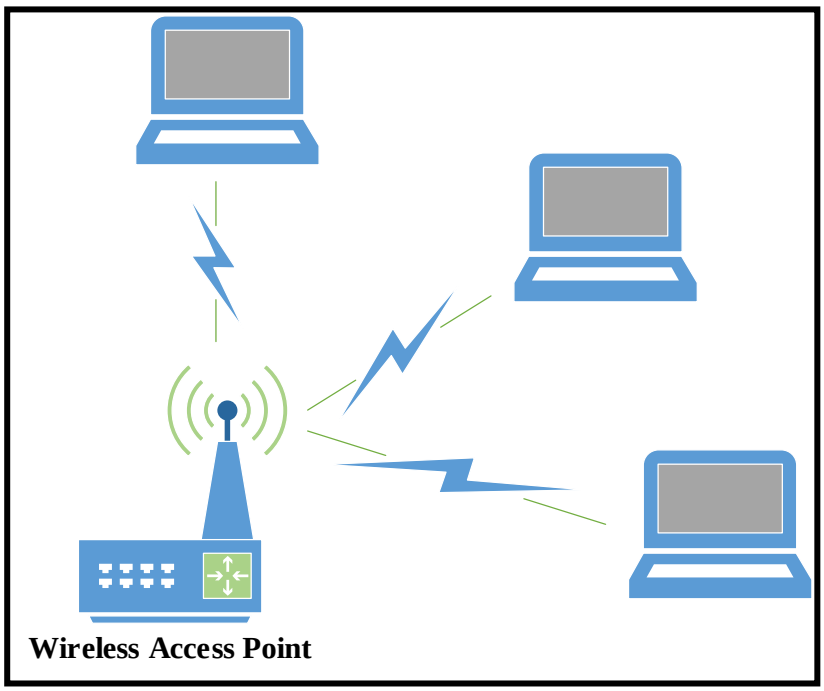


Gambar 2.2 Topologi AdHoc

Topologi AdHoc ini memiliki kelemahan *wireless client* tidak bisa mengatur prioritas dari perangkat mana yang harus didahulukan. Hal ini menyebabkan tabrakan atau *collision* yang tentu dapat membuat komunikasi jadi lambat.

b. Topologi Infrastruktur

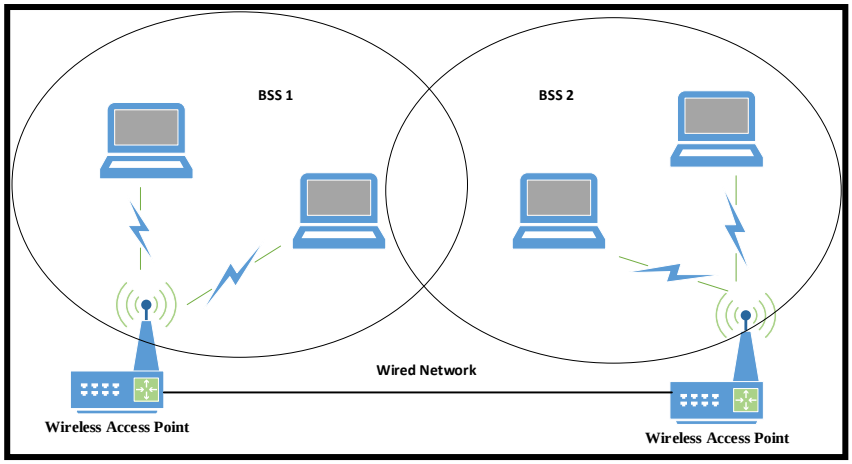
Dalam topologi Infrastruktur, komputer yang terhubung melalui wireless menggunakan perantara, yang dinamakan dengan *Access Point* atau *Wireless Access Point*. Topologi infrastruktur ini dikenal pula dengan nama *Basic Service Sets* (BSS).



Gambar 2.3 Topologi Infrastruktur BSS

Pengembangan dari *Basic Service Sets* (BSS) disebut sebagal *Extended Service Sets* (ESS), yaitu kumpulan dari beberapa topologi BSS yang saling *overlap*. Pada topologi ESS terdapat lebih dari satu *Access Point* (AP) yang dihubungkan. Topologi ini terdiri dari dua atau lebih BSS yang terkoneksi pada satu jaringan kabel. Tujuan dipakainya topologi ini adalah untuk memperluas daya jangkau *Access Point* dan juga

karena meningkatnya beban yang hanya dilayani oleh satu *Access Point*.



Gambar 2.4 Topologi Infrastruktur ESS

Salah satu hal yang harus diperhatikan dalam sebuah topologi ESS adalah hubungan antara *Access Point* harus beroperasi dengan *channel* yang berbeda agar tidak saling menginterferensi, serta menggunakan SSID yang sama.

2.7 *Quality Of Service*

Menurut Croll, dkk dalam Diwi, dkk (2014:209), *Quality Of Service* (QOS) adalah kemampuan suatu jaringan untuk memberikan layanan yang lebih baik pada trafik data tertentu pada berbagai jenis platform teknologi.

Menurut Cahyadi, dkk (2013:636), QOS merupakan kemampuan suatu jaringan untuk menyediakan layanan yang baik dengan menyediakan kapasitas jaringan, mengatasi *jitter* dan *delay* (waktu tunda). QoS dirancang untuk membantu pengguna menjadi lebih produktif dengan memastikan bahwa pengguna mendapatkan kinerja yang handal dari aplikasiaplikasi berbasis jaringan. QoS mengacu pada kemampuan jaringan untuk

menyediakan layanan yang lebih baik pada trafik jaringan tertentu melalui teknologi yang berbeda-beda. QoS merupakan suatu tantangan yang besar dalam jaringan berbasis IP dan internet secara keseluruhan.

Terdapat banyak hal bisa terjadi pada paket ketika melakukan perjalanan dari asal ke tujuan, yang mengakibatkan masalah-masalah dan sering disebut sebagai parameter-parameter QoS, antara lain:

1. *Delay*

   Delay Merupakan akumulasi berbagai waktu tunda dari ujung ke ujung pada jaringan Internet. Delay mempengaruhi kualitas layanan (QoS) karena waktu tunda menyebabkan suatu paket lebih lama mencapai tujuan. ITU-T G.114 merekomendasikan Delay tidak lebih besar dari 150 ms untuk berbagai aplikasi, dengan batas 400 ms untuk komunikasi multimedia yang masih dapat diterima. Sementara itu untuk aplikasi Voice seperti VoIP dan Conference Call batasan delay maksimal adalah 300 ms.

   Tabel 2.2 Standar Delay Berdasarkan ITU G.114

Delay (ms)	Kualitas
0 - 150	Baik
150 – 400	Cukup, masih dapat diterima
> 400	Buruk

2. *Jitter*

   Jitter merupakan perbedaan selang waktu kedatangan antar paket di terminal tujuan. jitter dapat disebabkan oleh terjadinya kongesti, kurangnya kapasitas jaringan, variasi ukuran paket, serta ketidakurutan paket. Tabel 2.3 di bawah ini menunjukkan standar nilai jitter yang mempengaruhi kualitas layanan multimedia.

Tabel 2.3 Standar Nilai Jitter Berdasarkan ITU G.114

Jitter (ms)	Kualitas
0 - 20	Baik
20 – 50	Dapat diterima
> 50	Tidak dapat diterima

3. Packet Loss

Packet Loss (Paket Hilang) merupakan penyebab utama pelemahan audio dan *video streaming*, VoIP dan *Conference Call*. *Packet Loss* dapat disebabkan oleh pembuangan paket di jaringan (*network loss*) atau pembuangan paket di *gateway*/terminal sampai kedatangan terakhir (*late loss*). *Network loss* secara normal disebabkan kemacetan (*router buffer overflow*), perubahan *rute* secara seketika, kegagalan link dan *lossy link* seperti saluran nirkabel. Kemacetan atau kongesti pada jaringan merupakan penyebab utama dari *packet loss*. Tabel 2.4 menunjukkan standar nilai *packet loss* yang mempengaruhi kualitas layanan (QoS).

Tabel 2.4 Standar Packet Loss Berdasarkan ITU G.114

Packet Loss (%)	Kualitas
0 – 1 %	Baik
1 – 5 %	Dapat diterima
> 10 %	Tidak dapat diterima

4. *Throughput*

Throughput merupakan rate (kecepatan) transfer data efektif, yang diukur dalam *bit per second* (bps). *Throughput* merupakan jumlah total kedatangan paket yang sukses yang diamati pada sisi *client*/tujuan selama selang waktu tertentu dibagi oleh durasi selang waktu tersebut.

BAB III
METODELOGI PENELITIAN

3.1 Subjek Penelitian

A. Tempat dan Waktu Penelitian

1. Tempat Penelitian

   Penelitian dilaksanakan di SMK Negeri 3 Kepahiang yang beralamatkan di Jalan Protokol Kel.Keban Agung Kec. Bermani Ilir Kab. Kepahiang Prov. Bengkulu 39374.

2. Waktu Penelitian

   Penelitian ini dilakukan dengan dua tahap yaitu:

   a. Pra - Penelitian

      Pra – penelitian ini dilakukan dari bulan Juli 2022 sampai dengan bulan September 2022.

   b. Penelitian

      Penelitian ini dilakukan dari bulan September 2022 sampai dengan bulan November 2022.

B. Struktur Organisasi

Struktur Organisasi merupakan kerangka kerja dimana didalamnya menggambarkan hubungan dan tanggung jawab setiap tingkat yang berada dalam Organisasi tersebut untuk melaksanakan demi tercapainya tujuan yang telah ditetapkan. Dengan demikian orang-orang tersebut mempunyai tugas, wewenang, dan tanggung jawab sesuai tugas masing-masing.

Struktur Organisasi sangatlah penting dalam suatu perusahaan atau instansi pemerintah. Karena dengan adanya struktur organisasi akan memperlihatkan dengan jelas kedudukan seseorang, sehingga setiap karyawan atau pegawai perusahaan atau instansi yang bersangkutan dapat mengetahui aktifitas dari perusahaan atau instansi dan dapat bekerja secara baik dari segi pembagian tugas maupun hal pelimpahan wewenang yang telah ditetapkan dalam struktur. Adapun struktur SMK Negeri 3 Kepahiang dapat dilihat pada Lampiran Struktur Organisasi.

3.2 Metode Penelitian

Metode penelitian yang digunakan adalah metode *Eksperimen.* Pada penelitian ini dilakukan analisa yang akan dijadikan sebagai bahan untuk Implementasi sistem deteksi intrusi menggunaakn metode *Network Intrusion Detection System* (NIDS) dengan memanfaatkan tools shorewall. Hasil eksprimen selanjutnya didokumentasikan untuk melakukan analisis sehingga dihasilkan rekomendasi yang tepat untuk sistem keamanan menggunakan deteksi intrusi shorewall. Dari hasil analisis tersebut nantinya akan mendapatkan kesimpulan mengenai manfaat, fungsi serta kelebihan dari sistem yang sudah dibangun.

3.3 Instrumen Perangkat Lunak dan Perangkat Keras

Dalam melakukan penelitian ini, alat dan bahan yang digunakan meliputi perangkat lunak dan perangkat keras.

1. Perangkat Lunak (*Software*)

Adapun perangkat lunak (*software*) yang digunakan dalam penelitian ini dapat dilihat seperti berikut.

a. Sistem Operasi Linux Ubuntu *Server 20.04*
b. Shorewall
c. Browser
d. Putty
e. NetCut

2. Perangkat Keras (*Hardware*)

Adapun perangkat Keras (*hardware*) yang digunakan dalam penelitian ini dapat dilihat seperti berikut.

a. 1 unit PC sebagai NIDS *Server*
b. 1 unit switch
c. 1 unit Wireless Router
d. 1 Unit Laptop

3.4 Metode Pengumpulan Data

Untuk memperoleh data yang diperlukan dalam penyusunan skripsi nanti penulis menggunakan beberapa metode dalam pengumpulan data yaitu:

A. Observasi

Merupakan metode pengumpulan data yang digunakan dengan cara melakukan pengamatan langsung pada jaringan yang ada di SMK Negeri 3 Kepahiang.

B. Studi Pustaka

Merupakan metode pengumpulan data yang dilakukan dengan cara membaca buku-buku di perpustakaan kampus maupun perpustakaan daerah dan artikel di *internet* yang ada hubungannya dengan masalah yang dibahas dalam penelitian ini.

C. Studi Laboratorium

Data penelitian dikumpulkan dengan melakukan percobaan di laboratorium SMK Negeri 3 Kepahiang yang berhubungan dengan kemananan jaringan komputer dengan *Network Intrusion Detection System* (NIDS) serta tools shorewall.

D. Studi Dokumentasi

Studi dokumentasi atau yang biasa disebut dengan kajian dokumen merupakan teknik pengumpulan data yang tidak langsung ditujukan kepada subjek penelitian dalam rangka memperoleh informasi terkait objek penelitian. Dalam studi dokumentasi, peneliti biasanya melakukan penelusuran data historis objek penelitian serta melihat sejauhmana proses yang berjalan telah terdokumentasikan dengan baik. Berikut adalah penjelasan seputar pengertian Studi Dokumentasi, Kekurangan dan kelebihannya.

E. Studi Wawancara

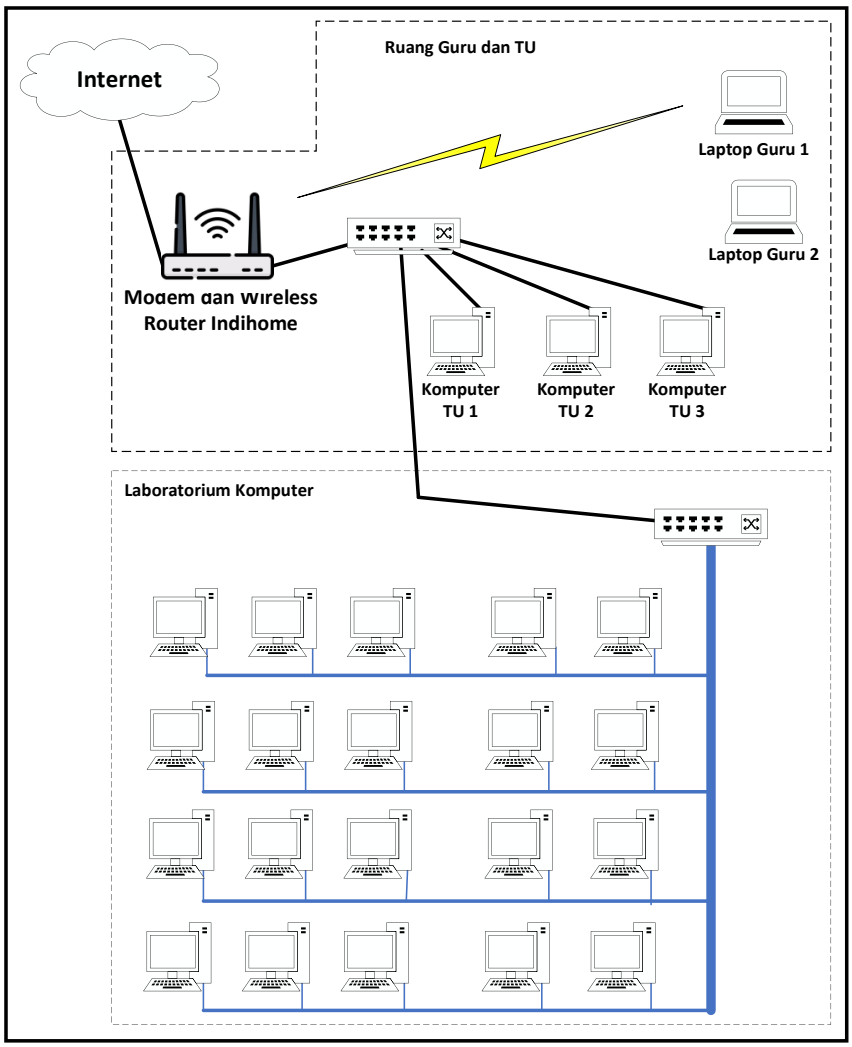
wawancara adalah pertemuan yang dilakukan oleh dua orang untuk bertukar informasi mupun suatuide dengan cara tanya jawab, sehingga dapat dikerucutkan menjadi sebuah kesimpulan atau makna dalam topik tertentu.

3.5 Metode Perancangan Sistem

A. Diagram Blok Sistem Lama

Berdasarkan dari data yang penulis peroleh dari studi observasi dan juga wawancara yang dilakukan pada SMK Negeri 3 Kepahiang, saat ini tidak ada sistem keamanan jaringan yang digunakan secara khusus untuk melakukan pemantauan

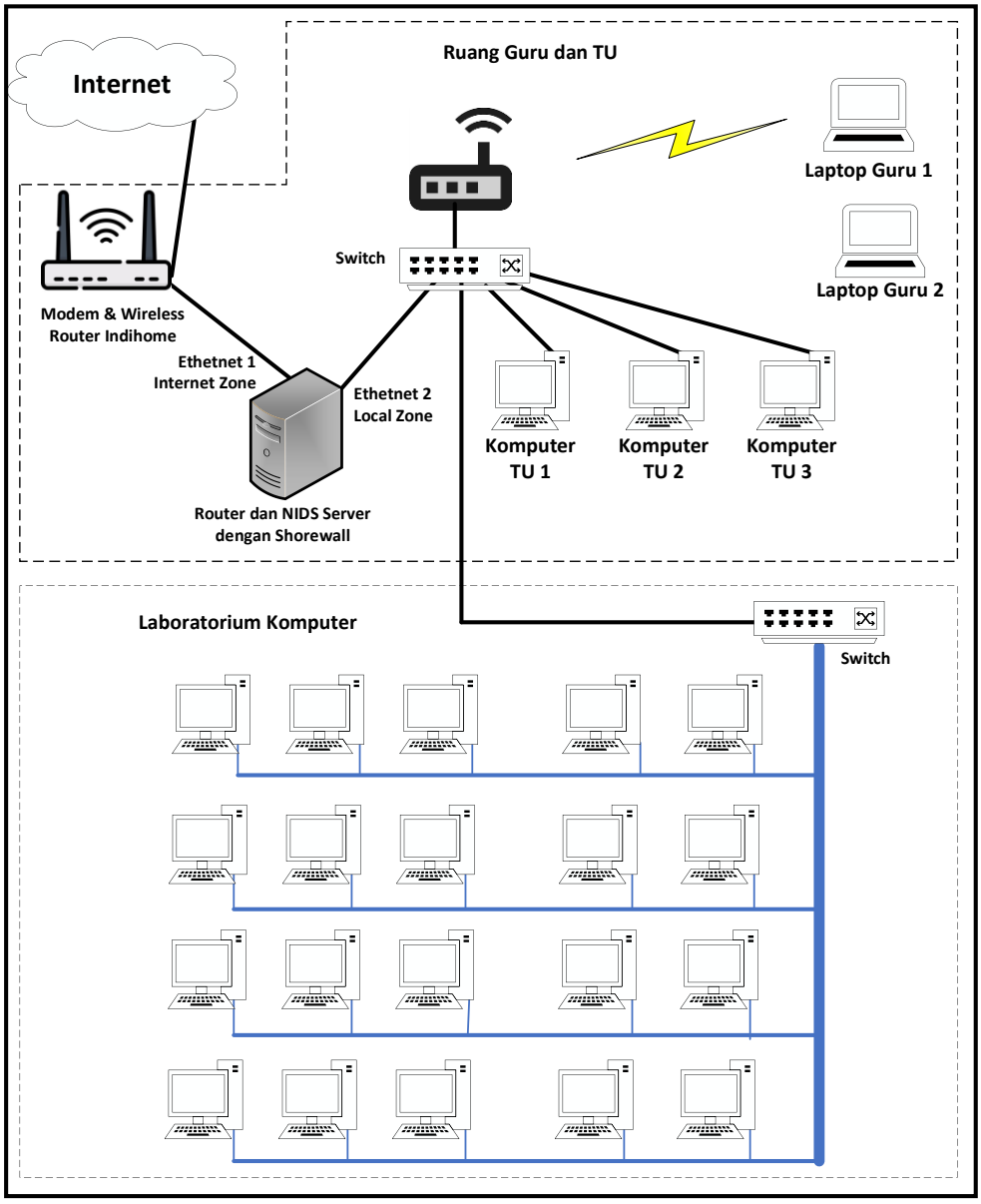
gangguan di dalam jaringan komputer pada SMK Negeri 3 Kepahiang. Adapun skema diagram blok sistem yang ada saat ini adalah sebagai berikut.



Gambar 3.1 Diagram Blok Sistem Lama

B. Diagram Blok Sistem Baru

Pada penelitian ini akan dilakukan pengembangan terhadap jaringan yang sudah ada dengan menerapkan sistem keamanan jaringan menggunakan deteksi itrusi berbasis *Network Intrusion Detection System* (NIDS) dengan tools shorewall. Adapun topologi yang akan digunakan adalah sebagai berikut.



Gambar 3.2 Diagram Blok Sistem Baru

Pada Gambar 3.2 tersebut dapat dilihat bahwa terdapat penambahan Router yang sekaligus akan berperan sebagai NIDS *Server* untuk sistem deteksi intrusi shorewall yang akan digunakan untuk memberikan alokasi internat dan juga memantau ataupun melakukan deteksi di dalam satu segmen jaringan, sehingga semua kegiatan komunikasi data yang terjadi pada jaringan SMK Negeri 3 Kepahiang akan terpantau oleh *Server* yang sudah ditanamkan *tools* shorewall. Selain itu koneksi wifi yang ada pada SMK

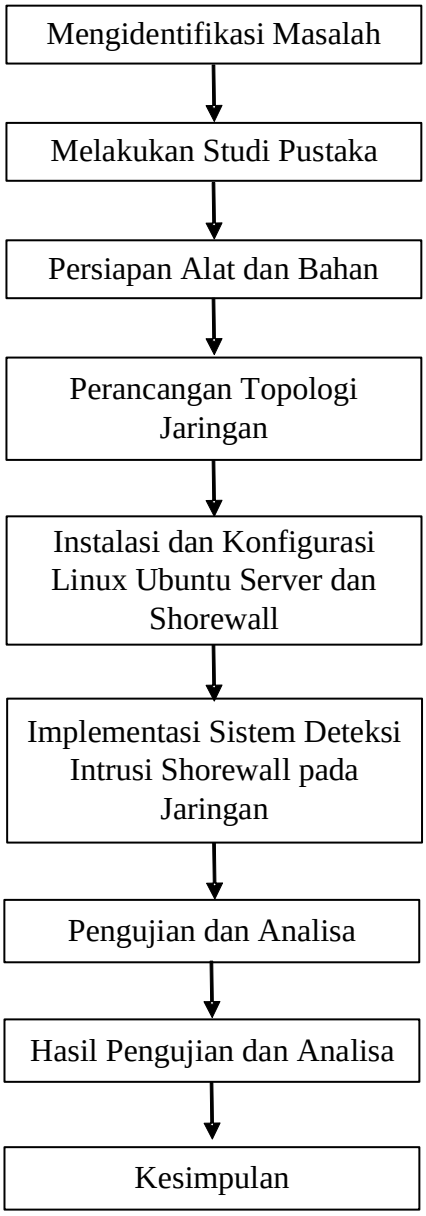
Negeri 3 Kepahiang juga akan di rubah berada di bawah *Server* shorewall, sehingga wifi yang ada pada modem dan *wireless router* ISP yidak akan digunakan lagi.

C. Prinsip Kerja Sistem

Prinsip kerja dari sistem deteksi intrusi shorewall berbasis *Network Intrusion Detection System* (NIDS) pada jaringan internet SMK Negeri 3 Kepahiang adalah dengan adalah dengan menerapkan zona yaitu zona koneksi internet dan zona koneksi lokal. Dimana masing – masing zona ini kan di atur dan dipantau oleh Shorewall yang akan menjadi *router* serta NIDS *Server* untuk memberikan koneksi internet sekaligus sebagai sistem deteksi intrusi di jaringan SMK Negeri 3 Kepahiang.

D. Rencana Kerja

Rencana kerja dari implementasi *Implementasi Network Intrusion Detection System* Menggunakan Android dengan aplikasi bot telegram adalah sebagai berikut.



Gambar 3.3 Rencana Kerja Sistem

Keterangan :

1. Mengidentifikasi Masalah

   Identifikasi permasalahan dilakukan untuk menentukan masalah-masalah yang terjadi pada tempat penelitian, kemudian dirumuskan dan diberikan batasan permasalahan yang akan diteliti.

2. Melakukan Studi Pustaka

Studi pustaka dilakukan dengan cara membaca buku-buku di perpustakaan kampus maupun perpustakaan daerah dan artikel di *internet* yang ada hubungannya dengan penelitian ini.

3. Persiapan Alat dan Bahan

Adapun alat dan bahan yang harus disiapkan, antara lain sebagai berikut:

a. 1 unit PC sebagai NIDS *Server*
b. 1 unit switch
c. 1 unit Wireless Router
d. 1 Unit Laptop
e. Sistem Operasi Linux Ubuntu *Server* 20.04
f. Shorewall
g. Browser
h. Putty
i. Netcut

4. Instalasi dan Konfigurasi Linux Ubuntu *Server* dan Shorewall

Tahapan ini dilakukan untuk melakukan instalasi terhadap *Server* yang akan digunakan serta menerapkan router dan NIDS dengan shorewall.

5. Implementasi Sistem Deteksi Intrusi Shorewall pada Jaringan

Tahapan ini dilakukan untuk menerapkan sistem deteksi intrausi shorewall pada keamanan jaringan SMK Negeri 3 Kepahiang.

6. Pengujian dan Analisa

Tahapan ini dilakukan untuk menguji sistem yang sudah diterapkan atau diimplementasikan pada jaringan. Apakah berjalan dengan baik ataupun sebaliknya.

7. Hasil Pengujian dan Analisa

   Tahapan ini adalah tahapan yang dilakukan untuk menyimpulkan hasil dari pengujian yang dilakukan.

8. Kesimpulan

   Pada tahapan ini adalah tahapan untuk menyimpulkan hasil dari penelitian yang telah dilakukan.

3.6 Rancangan Pengujian

Pengujian ini dilakukan dengan metode *blackbox*, yaitu sebuah metode yang digunakan untuk menemukan kesalahan dan mendemonstrasikan fungsional sistem saat dioperasikan, apakah *input* diterima dengan benar dan *output* yang dihasilkan telah sesuai dengan yang diharapkan, sehingga dapat membuktikan kebenarannya. Adapun rancangan pengujian dapat dilihat seperti Tabel 3.1 berikut.

Tabel 3.1 Pengaujian dan Analisa

No	Jenis Pengujian	Kriteria	Hasil	Keterangan
1.	Pengujian Deteksi Serangan Mac *Clone*.	Pengujian dilakukan menggunakan aplikasi Netcut		
2.	Pengujian Deteksi DDoS *Attack*.	Pengujian dilakukan menggunakan aplikasi Command Prompt		
3.	Pengujian Kualitas	Kulitas Jaringan		

	Layanan Jaringan	dengan Parameter Throughput		
		Kulitas Jaringan dengan Parameter *Delay*		
		Kulitas Jaringan dengan Parameter Jitter		
		Kulitas Jaringan dengan Parameter Packet Loss		