**PROPOSAL**

**IMPLEMENTASI *INTRUSION DETECTION SYSTEM* (IDS) DAN**

***INTRUSION PREVENTION SYSTEM* (IPS) MENGGUNAKAN JEJARING SOSIAL SERTA EMAIL SEBAGAI MEDIA NOTIFIKASI**

Diajukan Untuk Memenuhi

Salah Satu Syarat Memperoleh Gelar Sarjana Teknik



**OLEH:**

**YULINA**

**E1E1 15 093**

**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS HALU OLEO**

**KENDARI**

**2019**

i

**DAFTAR ISI**

## HALAMAN JUDUL ........................................................................................ DAFTAR ISI ...................................................................................................... xii DAFTAR GAMBAR ...................................................................................... . xv DAFTAR TABEL .............................................................................................xvii

**BAB I PENDAHULUAN**  ................................................................................. 1

1.1 Latar Belakang .................................................................................. 1

1.2 Rumusan Masalah ............................................................................. 2

1.3 Batasan Masalah ................................................................................ 2

1.4 Tujuan Penelitian ............................................................................... 2

1.5 Manfaat Penelitian ............................................................................. 3

1.6 Sistematika Penulisan ........................................................................ 3

1.7 Tinjauan Pustaka ............................................................................... 4

**BAB II LANDASAN TEORI**  .......................................................................... 6

2.1 Jaringan Komputer ............................................................................ 6

2.2 Topologi jaringan Komputer ............................................................. 7

2.3 Internet .............................................................................................. 8

2.4 *Wireless Local Area Network* (WLAN) ............................................ 10

2.5 Topologi *Wireless* LAN .................................................................... 11

2.5.1 *Independent Basic Service Sets* (IBSS) …………………….. 11

2.5.2 *Basic Service Sets* (BSS) ……………………..…………….. 12

2.5.3 *Extended Service Sets* (ESS)………………………………... 12

2.6 IP *Address* ......................................................................................... 13

2.6.1 IP *Address* versi 4 ………………………………………….. 13

2.7 *Intrusion Detection System* (IDS) ..................................................... 15

2.8 *Intrusion Prevention System* (IPS) .................................................... 17

2.9 Keamanan *Wireless Local Area Network* (LAN) ............................. 18

2.10 Jejaring Sosial dan E-mail ............................................................... 20

2.11 *Server* .............................................................................................. 23

2.12 *Hypertext Preprocessor* (PHP) ....................................................... 25

2.13 *Basic Security and Analysis Engine* (BASE) ……………………. 26

2.14 *Linux Ubuntu ………………………………………………….. ………* 27

2.15 *Snort ……………………………………………………………………..* 28

2.16 IPTables …………………………………………………………. 29

2.17 *Port ……………………………………………………………………...* 30

2.18 *Security Policy Development Life Cycle (SPDLC) ……………….* 31

**BAB III METODOLOGI PENELITIAN**  ...................................................... 33

3.1 Metode Pengumpulan Data ............................................................... 33

3.2 Metode Pengembangan Sistem ......................................................... 33

3.3 Waktu dan Tempat Penelitian ........................................................... 34

3.3.1 Waktu Penelitian ..................................................................... 34

3.3.2 Tempat Penelitian .................................................................... 34

**DAFTAR PUSTAKA**

## DAFTAR GAMBAR

Gambar 2.1 Topologi *Star* ................................................................................. 8

Gambar 2.2 Pemanfaatan WLAN Pada *Small Office Home Office* ................... 10

Gambar 2.3 Topologi IBSS ............................................................................... 11

Gambar 2.4 Topologi BSS ................................................................................. 12

Gambar 2.5 Topologi ESS ................................................................................. 13

Gambar 2.6 Topologi IPS .................................................................................. 18

Gambar 2.7 *Security Policy Development Life Cycle* (SPDLC) ........................ 31

**DAFTAR TABEL**

[Tabel 3.1 Fase pengembangan *system* 33](#_Toc70278)

[Tabel 3.2 Tabel waktu kegiatan 34](#_Toc70279)

**BAB I**

**PENDAHULUAN**

## 1.1 Latar Belakang Masalah

Perkembangan teknologi informasi disemua bidang semakin berkembang pesat, sehingga dapat memudahkan dalam mencari informasi yang dibutuhkan dari mana saja, kapan saja dan dari siapa saja. Perkembangan teknologi informasi ini juga dapat mempercepat adanya arus informasi, mempermudah pencarian informasi dan dapat segera mengupdate informasi terbaru, yang tentunya menjadikan keamanan informasi menjadi sangatlah penting, terlebih lagi pada suatu jaringan yang terkoneksi dengan internet.

Perkembangan teknologi ini masih belum mampu menjamin keamanan teknologi itu sendiri, hal ini dikarenakan ketidakseimbangan antara setiap perkembangan teknologi tidak diiringi dengan perkembangan pada sistem keamanannya, dengan demikian banyak sistem-sistem yang masih lemah dan harus ditingkatkan keamanannya. Serangan yang biasanya mengancam keamanan jaringan tersebut adalah serangan dari *hacker* dan *cracker* yang bermaksud merusak jaringan komputer yang terkoneksi dengan internet ataupun mencuri informasi penting yang ada pada jaringan tersebut.

Serangan *hack* dan *crack* biasanya diatasi melalui penempatan seorang *administrato*r. Seorang administrator bertugas untuk mengawasi dan melakukan tindakan pencegahan ketika terjadi aksi penyusupan dan serangan. Masalah akan timbul ketika sang administrator sedang tidak berada pada posisi siap sedia, misalnya sakit, berada di luar jam kerja, atau adanya kepentingan mendadak, sedangkan serangan terhadap server bisa terjadi kapan saja. Berdasarkan permasalahan tersebut, administrator membutuhkan suatu sistem yang dapat membantu mengawasi jaringan, menginformasikan serangan, dan mengambil tindakan tepat untuk pencegahan yang akan membantu mengautomatisasi fungsi kerja dasar administrator.

1

*Intrusion Detection System* (IDS) dapat didefenisikan sebagai sebuah sistem atau perangkat lunak yang dapat mendeteksi aktivitas mencurigakan dalam sebuah sistem jaringan. IDS memberikan pertahanan pertama yang sangat penting dalam menghadapi penyusupan, jika penyusup berusaha masuk ke server jaringan, bukti dapat ditemukan di dalam sistem *log*. *Intrusion Prevention System* (IPS) adalah perangkat lunak yang digunakan untuk mencegah dan memblok serangan yang masuk pada sistem jaringan. IPS bekerja dengan cara mencegah serangan yang akan masuk kejaringan dengan memeriksa dan mencatat semua paket data serta mengenali paket, disaat serangan telah teridentifikasi.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan sebelumnya, rumusan masalah yang dapat dipaparkan yaitu bagaimana cara mengimplementasikan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) pada sebuah server dengan menggunakan jejaring sosial serta *email* sebagai media notifikasi.

## 1.3 Batasan Masalah

Yang menjadi batasan masalah dalam penulisan tugas akhir ini adalah:

1. Media notifikasi yang digunakan adalah jejaring sosial (*telegram dan whatsapp*) serta *email* (*Google E-mail*).
2. Jenis serangan yang dapat dideteksi dan diblokir adalah ICMP *ping flood*, *port scanner*, SSH, Telnet dan FTP.
3. Tipe jaringan komputer yang digunakan adalah *Wireless* *local area network (*WLAN).

## 1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang disebutkan sebelumnya, maka tujuan dari penelitian ini adalah mengimplementasikan *Intrusion Detection System* (IDS) dan

*Intrusion Prevention System* (IPS) pada sebuah server dengan menggunakan jejaring sosial (*telegram* dan *whatsapp*) serta *email* sebagai media notifikasi.

## 1.5 Manfaat Penelitian

Manfaat yang diharapkan dapat diperoleh dari penulisan tugas akhir ini adalah mengautomatisasi fungsi kerja dasar administrator dalam mengawasi dan memblokir serangan pada jaringan server dengan menggunakan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) dan jejaring sosial (*telegram* dan *whatsapp*) serta *email* sebagai media notifikasi.

**1.6 Sistematika Penulisan**

Laporan ini terdiri dari enam bab dengan sistematika berikut:

## BAB I PENDAHULUAN

Bab ini berisi tentang deskripsi umum isi laporan yang meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

## BAB II TINJAUAN PUSTAKA

Bab ini berisi teori-teori yang menjadi landasan dan mendasari penelitian yang mendukung penelitian ini yaitu teori *IDS* ***(Intrusion Detection System)****, PHP* ***(Hypertext Preprocessor),*** *Jejaring Sosial* ***(Telegram*** dan ***Whatsapp)*** serta *Email, Snort, BASE (****Basic Analysis and Security****)*.

## BAB III METODOLOGI PENELITIAN

Bagian ini memuat prosedur dan pengumpulan data, prosedur pengembangan perangkat lunak serta waktu dan tempat penelitian.

## BAB IV ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini membahas tentang analisa permasalahan dan kebutuhan Metode *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) dengan

bahasa pemrograman *PHP* yang menggunakan jejaring sosial (*telegram dan whatsapp*) serta *email* sebagai media notifikasi dan adanya perancangan system secara fungsional.

## BAB V IMPLEMENTASI DAN PEMBAHASAN

Bagian ini menyajikan implementasi serta hasil penelitian dan pembahasan. Bagian implementasi menguraikan tentang implementasi secara detail dan runut, bagian hasil penelitian dan pembahasan hasil dari implementasi disertai dengan penjelasan yang terkait.

## BAB VI PENUTUP

Bagian ini memuat kesimpulan dari penelitian yang telah dilakukan serta saran untuk penelitian selanjutnya.

### 1.7 Tinjauan Pustaka

Penelitian ini dibuat berdasarkan penelitian yang pernah dilakukan oleh

Nugroho dkk (2015)dengan judul **“Perancangan dan Implementasi IDSdi Jaringan Universitas Diponegoro*”.*** Dalam penelitian ini *administrator* hanya dapat memantau kondisi jaringan dan menganalisa paket-paket yang berbahaya melalui sensor *cisco* dan web. **“Deteksi Penyusupan Pada Jaringan Komputer Menggunakan IDS *Snort*”** adalah judul penelitian yang dilakukan oleh Fathoni W, dkk pada tahun 2016. Penelitian ini berfokus untuk mendeteksi adanya serangan dengan memperhatikan *snort* yang dibuat.

Padatahun 2017, Fadlin Arsin S.T mahasiswa Teknik Informatika UHO melakukan penelitian yang sama, dengan judul **“Implementasi *Security System* Menggunakan Metode IDPS *(Intrusion Detection & Prevention System)* Dengan**

**Layanan *Realtime Notification”.*** Dalam penelitian ini dibuat sebuah aplikasi berbasis *mobile* yang dapat memantau adanya serangan secara *real time*. Dengan kesimpulan port SSH merupakan port yang memiliki tingkat waktu terbanyak menerima serangan dibanding port lain seperti FTP, ICMP dan Telnet selama proses pengujian.

Penelitian selanjutnya dilakukan oleh Muh. Sadam Husain S.T (2018), yang juga meneliti **“Implementasi Keamanan *Server* Pada Jaringan *Wireless* Menggunakan Metode *Intrusion Detection* and *Prevention System* (IDPS) (Studi**

**Kasus: Techno’s Studio)”**. Sistem yang dibangun pada penelitian ini telah dilengkapi dengan adanya notifikasi, namun notifikasi yang muncul hanya sebatas pada terminal dan web BASE *administrator* dan pada penelitian ini lebih fokus pada analisis *log*.

**BAB II**

**LANDASAN TEORI**

## 2.1 Jaringan Komputer

Jaringan komputer adalah sistem yang terdiri dari komputer-komputer serta piranti-piranti yang saling terhubung sebagai satu kesatuan, dengan dihubungkan piranti-piranti tersebut, alhasil dapat saling berbagi sumber daya antara satu piranti dengan piranti lainnya (Sopandi, 2008).

Ada banyak tipe jaringan komputer, berikut tipe jaringan berdasarkan ruang lingkupnya:

1. LAN (*Local Area Network*) : LAN adalah sebuah Jaringan komputer yang cakupan areanya kecil, seperti sebuah rumah, kantor, atau sekolah. Karakteristik khusus dari LAN yang membedakan dengan jenis jaringan yang lain adalah transfer data yang lebih besar, namun cakupan area yang lebih sempit. Teknologi yang dipakai untuk membuat LAN ada beberapa macam, ada ARCNET dan Token Ring, namun yang lazim digunakan sekarang adalah Ethernet dan kabel UTP.
2. MAN (*Metropolitan Area Network*) : MAN adalah jaringan komputer yang cakupan luasnya mencapai satu kota atau lebih. Sebuah MAN biasanya menghubungkan antara beberapa LAN lokal dengan menggunakan teknologi backbone, seperti fiber optik, dan beberapa penyedia layanan internet yang sering di sebut ISP (*Internet Service Provider*).
3. WAN (*Wide Area Network*) :WAN adalah jaringan komputer yang cakupannya cukup luas, seperti antar regional atau antar negara. Salah satu contoh koneksi dalam jaringan WAN adalah Leased Line, merupakan koneksi point-to-point antara 2 komputer atau Local Area Network (LAN) dengan area yang cukup jauh (antar negara) (Nugroho, 2013).

6

## 2.2 Topologi Jaringan Komputer

Topologi dapat diartikan sebagai *layout* atau arsitektur jaringan dari komputer. Topologi merupakan suatu aturan bagaimana jaringan komputer (*node*) secara fisik, topologi berkaitan dengan komponen-komponen jaringan seperti *server*, *workstation*, *switch*, *router* dan lainnya yang saling berkomunikasi melalui media transmisi data (Sofana, 2013).

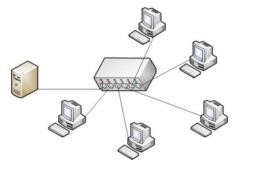
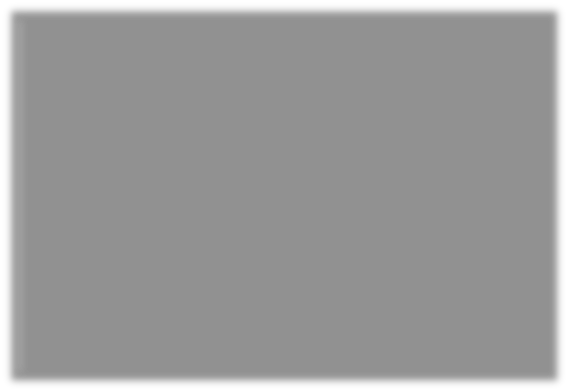
Topologi jaringan memiliki dua kategori, yaitu *phisycal topology* (topologi fisik) dan *logical topology* (topologi logika). Topologi fisik berkaitan dengan bentuk jaringan, sedangkan topologi logika berkaitan dengan bagaimana data mengalir di dalam topologi fisik. Topologi sendiri umumnya terdiri dari beberapa bagian, yaitu:

1. Topologi *Bus*
2. Topologi *Ring*
3. Topologi *Tree*
4. Topologi *Mesh*
5. Topologi *Star*

Menurut Iwan Sofana (2013) topologi *star* adalah topologi yang sering digunakan dan lebih mudah dikonfigurasi. Topologi ini membuat tiap perangkatnya di hubungkan pada perangkat penghubung (sentral). Topologi *Star* ini merupakan salah satu topologi yang sering dijumpai dalam sebuah jaringan komputer, apabila mempunyai tiga atau lebih komputer dan sebuah perangkat penghubung, dengan menggunakan *hub*, *switch*, atau *router*, maka ketiga komputer bisa saling terkoneksi.

Karakteristik topologi *star* antara lain adalah:

1. Kabel yang digunakan berjenis *coaxial*, UTP, dan STP.
2. Menggunakan penghubung berupa *hub*, *switch* dan *router*.
3. Jika salah satu segmen kabel putus pada satu atau lebih *node*, maka hanya segmen itu saja yang akan lumpuh sementara jaringan dapat tetap berfungsi.
4. Pengiriman data menggunakan metode CSMA/CD (*Carrier Sense Multiple Access*/*Collision Detection*) *baseband*.
5. Data mengalir pada sebuah kabel secara bolak-balik.
6. Sering terjadi banjir data dan *collision* (tabrakan data) sehingga dapat menurunkan performa jaringan, terutama pada penghubung hub.
7. Relatif lebih mahal dibandingkan dengan topologi *bus*, namun proses instalansi mudah dan cocok diimplementasikan pada jarinngan kecil maupun besar.



**Gambar**

**2.1**

**Topologi**

***Star***

**(**

**Sofana,**

**2013)**

## 2.3 Internet

Internet merupakan jaringan terbesar yang menghubungkan jaringan komputer yang terbesar di seluruh dunia dan tidak terikat pada suatu organisasi lain. Kehadiran internet telah membawa perubahan yang signifikan terhadap berbagai aspek kehidupan umat manusia, terutama dari sisi kebebasan untuk memperoleh dan menyebarkan informasi tanpa mengenal batas geografis.Saat ini ada tiga pendapat yang mengatakan bahwa internet adalah singkatan dari kata *International Network, Internetworking, Interconnected Network* (Yuhefizar, 2008).

Dari definisi diatas, dapat disimpulkan bahwa layanan utama internet sebagai media adalah sebagai berikut :

1. Menyebarkan dan memperoleh informasi, umum disajikan dalam bentuk website, informasi dapat merupa teks, grafik, suara, video
2. Berkomunikasi, baik melalui media *chatting* berbasis teks (*IRC)*, grafik (*Yahoo Messager*) maupun berkomunikasi suara (*skype*) layaknya menggunakan telepon kabel

1. Berkirim surat (*e-mail*)
2. Bertukar data, salah satunya dengan menggunakan aplikasi *FTP*, website maupun *peer to peer*.
3. *Remote login*, mampu mengeksekusi komputer dari jarak jauh.

Internet merupakan koneksi jaringan komputer dunia, komputer- komputer tersebut saling bekerja sama untuk bertukar data dengan menggunakan program aplikasi yang dapat dimengerti oleh semua komputer. Internet memiliki berbagai manfaat sebagai berikut.

1. Sarana informasi

Melalui web di internet, sebuah organisasi mampu menampilkan berbagai bentuk informasi agar dapat dibaca oleh setiap orang diseluruh dunia. Bahkan perseorangan juga dapat membuat halaman web sendiri untuk menampilkan informasinya.

1. Sarana kegiatan bisnis

Banyak penyedia jasa informasi di Indonesia bersifat komersil atau bisnis, yang menyediakan ruang di website untuk pemasangan iklan produk-produk tertentu. Bahkan ada website yang khusus menjual berbagai produk. Jika mengklik iklan tersebut, maka dapat dihubungkan ke situs tertentu yang memuat produk yang lebih lengkap dengan penawaran terbaik.

1. Sarana komunikasi

Komunikasi tidak hanya berbicara lisan, tetapi pertukaran file dan data juga merupakan bentuk komunikasi. Pengambilan file dari internet disebut *download* atau ‘*unduh*’. Sebagai contoh dari website [www.ilmukomputer.com](http://www.ilmukomputer.com/)  dapat diunduh artikel teknologi informasi yang ditulis dan tersedia.

1. Sarana pendidikan

Karena internet menyediakan berbagai macam dan bentuk informasi, dapat dicari informasi yang sesuai dengan kebutuhan. Pelajar dapat mengakses berbagai ilmu pengetahuan untuk memperkaya ilmu yang telah diterima dikelas. Bahka kini berkembang sistem kuliah jarak jauh melalui internet (*e-learning*) dengan memanfaatkan layanan fasilitas konferensi video.

1. Sarana hiburan

Dengan adanya internet dapat diperoleh manfaat hiburan seperti mendengar siaran radio, nonton televisi secara *online*, melihat video, memutar lagu, bermain game secara *online* juga.

1. Kesehatan

Informasi kesehatan dapat ditemukan di beberapa situs internet seperti olahraga, makanan sehat, obat tradisional, obat modern, konsultasi dokter, serta alamat-alamat rumah sakit bahkan pengobatan alternatif pun terdapat pada internet.

## 2.4 *Wireless Local Area Network* (WLAN)

*Wireless Local Area Network* (disingkat *Wireless* LAN atau WLAN) adalah jaringan komputer yang menggunakan frekuensi radio dan *infrare*d sebagai media transmisi data. *Wireless* LAN sering disebut sebagai jaringan nirkabel atau jaringan *wireless* (Rajab, 2010).

Proses komunikasi tanpa kabel ini dimulai dengan bermunculannya peralatan berbasis gelombang radio, seperti *walkie talkie*, *remote control*, *cordless phone*, telepon selular, dan peralatan radio lainnya. Lalu adanya kebutuhan untuk menjadikan komputer sebagai barang yang mudah dibawa (*mobile*) dan mudah digabungkan dengan jaringan yang sudah ada. Hal-hal seperti ini akhirnya mendorong pengembangan teknologi *wireless* untuk jaringan computer (Rajab, 2010).



## Gambar 2.2 Pemanfaatan WLAN Pada *Small Office Home Office*

**(Rajab, 2010)**

### 2.5 Topologi *Wireless* LAN

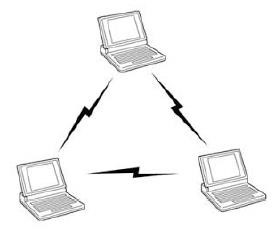
Topologi adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan.Terdapat tiga bentuk konfigurasi jaringan *wireless* LAN yang masing-masing bentuk tersebut memiliki set peralatan yang berbeda-beda. Tiga bentuk konfigurasi tersebut adalah :

1. *Independent Basic Service Sets* (IBSS)
2. *Basic Service Sets* (BSS)
3. *Extended Service Sets* (ESS)

#### 2.5.1 Independent Basic Service Sets (IBSS)

*Independent Basic Service Set*disebut pula jaringan *wireless* yang menggunakan metode *ad-hoc*. Sebuah IBSS tidak memerlukan *access point* atau *device* lain untuk mengakses ke sistem distribusi, tetapi hanya melingkupi satu *cell* dan memiliki sebuah SSID (Rajab, 2010). *Client* pada IBSS secara bergantian bertanggung jawab mengirimkan *beacon* yang biasa dilakukan oleh *access point*.

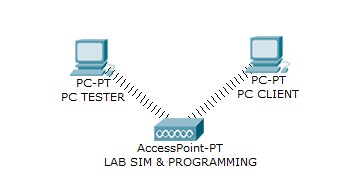
Agar dapat mengirimkan data ke luar IBSS, sebuah *client* harus bertindak sebagai *gateway* atau *router* dengan menggunakan *software* khusus untuk mengimplementasikan tujuan. Pada IBSS, *client* membuat koneksi secara langsung ke *client* lainnya, sehingga jenis demikian disebut jaringan *peer-to-peer.*



## Gambar 2.3 Topologi IBSS (Rajab, 2010)

### 2.5.2 *Basic Service Sets* (BSS)

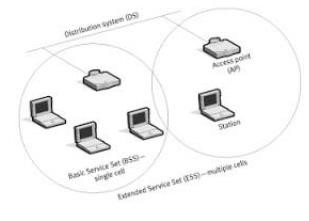
BSS menggunakan mode infrastruktur, yaitu sebuah mode yang membutuhkan sebuah *access point* dan semua trafik *wireless* melewati *access point*. Setiap *client wireless* harus menggunakan *access point* untuk berkomunikasi dengan *client wireless* lainnya atau dengan *host* yang terdapat pada jaringan kabel (Rajab, 2010). *Basic Service Set* membentuk sebuah *cell* atau area frekuensi radio, yang mengelilingi *access point* dengan beragam *rate zone* dan *speed* diukur dengan Mbps. *Rate* data akan semakin kecil jika semakin jauh dari *access point*. Sebuah *Basic Service Set*akan memiliki 1 SSID.



## Gambar 2.4 Topologi BSS (Rajab, 2010)

### 2.5.3 *Extended Service Sets* (ESS)

*Extended service set* didefinisikan sebagai dua atau beberapa *basic service set* yang dihubungkan dengan sebuah sistem distribusi bersama (Rajab, 2010). Sistem distribusi dapat berupa kabel, *wireless*, LAN, WAN, atau bentuk jaringan lain. Sebuah *extended service set*harus memiliki paling sedikit 2 *access point* yang bekerja dalam mode infrastruktur. Semua paket harus melewati salah satu *access point* yang tersedia. Karakteristik lain ESS, penggunaan standar 802.11, ESS melingkupi beberapa *cell* mengizinkan kemampuan *roaming* dan tidak membutuhkan SSID yang sama diantara kedua BSS (*Basic Service Set*).



## Gambar 2.5 Topologi ESS (Rajab, 2010)

### 2.6 *IP Address*

*IP address* merupakan pengenal yang digunakan untuk memberi alamat pada tiap-tiap komputer dalam jaringan. Alamat IP merupakan representasi dari 32 bit bilangan biner yang ditampilkan dalam bentuk desimal dengan dipisah tanda titik. *IP address* terdiri atas *network* ID dan *host* ID. *Network* ID menunjukkan nomor jaringan sedangkan *host* ID mengidentifikasikan *host* dalam satu jaringan (Sugeng, 2010).

#### 2.6.1 IP Address versi 4

Suatu jenis pengalamatan jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan *protocol IP* versi 4. Panjang totalnya adalah 32bit, dan secara teoritis dapat mengalamati hingga 4 miliar *host* komputer atau lebih tepatnya 4.294.967.296 *host* di seluruh dunia (Sugeng, 2010).

Alamat IP versi 4 terbagi menjadi beberapa jenis, yakni sebagai berikut :

1. Alamat unicast, merupakan alamat IP versi 4 yang ditentukan untuk sebuah antarmuka jaringan yang dihubungkan ke sebuah *Internetwork IP*. Alamat unicast digunakan dalam komunikasi *point-to-point* atau *one-to-one*.
2. Alamat *Broadcast*, merupakan alamat IP versi 4 yang didesain agar diproses oleh setiap node IP dalam segmen jaringan yang sama. Alamat *broadcast* digunakan dalam komunikasi *one-to-everyone*.
3. Alamat *multicast*, merupakan alamat ipv4 yang didesain agar diproses oleh satu atau beberapa node dalam segmen jaringan yang sama atau berbeda. Alamat *multicast* digunakan dalam komunikasi *one-to-many*.

Alamat IP versi 4 ini juga dibagi menjadi beberapa kelas, yaitu:

1. Kelas A, alamat-alamat kelas A diberikan untuk jaringan skala besar. Nomor urut bit tertinggi di dalam alamat IP kelas A selalu diset dengan nilai 0 (nol). Tujuh bit berikutnya untuk melengkapi oktet pertama akan membuat sebuah *network identifier*. 24 bit sisanya (atau tiga oktet terakhir) merepresentasikan *host identifier.* Ini mengizinkan kelas A memiliki hingga 126 jaringan, dan 16,777,214 *host* tiap jaringannya. Alamat dengan oktet awal 127 tidak diizinkan, karena digunakan untuk mekanisme *Interprocess Communication* (IPC) di dalam mesin yang bersangkutan.
2. Kelas B, alamat-alamat kelas B dikhususkan untuk jaringan skala menengah hingga skala besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diset ke bilangan bine 10. 14 bit berikutnya (untuk melengkapi dua oktet pertama), akan membuat sebuah *network identifier*. 16 bit sisanya (dua oktet terakhir) merepresentasikan *host identifier.* Kelas B dapat memiliki 16,384 *network*, dan 65,534 *host* untuk setiap *network-*nya.
3. Kelas C, alamat IP kelas C digunakan untuk jaringan berskala kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diset ke nilai biner 110. 21 bit selanjutnya (untuk melengkapi tiga oktet pertama) akan membentuk sebuah *network identifier.* 8 bit sisanya (sebagai oktet terakhir) akan merepresentasikan *host identifier*. Ini memungkinkan pembuatan total 2,097,152 buah *network*, dan 254 *host* untuk setiap *network*-nya.
4. Kelas D, alamat IP kelas D disediakan hanya untuk alamat- alamat IP *multicast,* sehingga berbeda dengan tiga kelas di atas. Empat bit pertama di dalam IP kelas D selalu diset ke bilangan biner 1110. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host.*
5. Kelas E, alamat IP kelas E disediakan sebagai alamat yang bersifat "eksperimental" atau percobaan dan dicadangkan untuk digunakan pada masa depan. Empat bit pertama selalu diset kepada bilangan biner 1111. 28 bit sisanya digunakan sebagai alamat yang dapat digunakan untuk mengenali *host.*

### 2.7 *Intrusion Detection System* (IDS)

*Intrusion Detection System* (IDS) adalah suatu tindakan untuk mendeteksi adanya trafik paket yang tidak diinginkan dalam sebuah jaringan atau *device*. Sebuah IDS dapat diimplementasikan melalui *software* atau aplikasi yang terinstall dalam sebuah *device*, dan aplikasi tersebut dapat memantau paket jaringan untuk mendeteksi adanya paket-paket ilegal seperti paket yang merusak kebijakan aturankeamanan, dan paket yang ditujukan untuk mengambil hak akses suatu pengguna (Wu, 2009).

Beberapa jenis dari teknologi IDS adalah *Network-Based*, *Wireless* IDS, *Network Behavior Anomali Detection* dan *Host-Based*. Pengembangan dan implementasi teknologi IDS ke dalam sebuah sistem jaringan tergantung dari variasi konfigurasi jaringan itu sendiri. Pada dasarnya setiap jenis teknologi IDS mempunyai keuntungan dan kekurangan dalam hal pendeteksian, konfigurasi dan biaya, tetapi secara umum teknologi IDS yang paling sering digunakan adalah *Network-Based* dan *Host-Based* (Wu, 2009).

1. *Network Intrusion Detection System* (NIDS)

*Network Intrusion Detection System* adalah salah satu tipe IDS yang populer atau paling banyak diimplementasikan kedalam sebuah sistem jaringan. Tipe ini menganalisa paket-paket jaringan pada semua lapisan *Open System Interconnection* (OSI) dan membuat sebuah tindakan kepada paket tersebut. Kebanyakan NIDS lebih mudah diterapkan kedalam suatu jaringan dan dapat memantau paket dari banyak sistem sekaligus (Wu, 2009).

1. WLAN IDS

*Wireless Local Area Network* (WLAN) IDS menyerupai NIDS yang dapat menganalisa paket-paket jaringan. WLAN ini dapat menganalisa paket wireless secara spesifik, termasuk pemindaian pengguna eksternal yang mencoba untuk terhubung ke *Access Point* (AP). Karena WLAN IDS sendiri sebenarnya adalah NIDS dengan menggunakan *wireless* maka aturan-aturan keamanan yang diterapkan lebih luas (Wu, 2009).

1. *Host-Based*

*Host-based Intrusion Detection System* (HIDS) menganalisa paket jaringan dan pengaturan sistem secara spesifik seperti *software calls*, *local security policy*, *local log audits*, dll. HIDS harus diinstal di setiap mesin dan membutuhkan konfigurasi secara spesifik pada sistem operasi dan software (Wu, 2009).

Menurut Wu dalam bukunya *Information Assurance Tools Report* yang diterbitkan pada tahun 2009 terdapat beberapa jenis-jenis pendeteksian adanya serangan dalam implementasi IDS. Jenis-jenis tersebut adalah *Signature-Based Detection*, *AnomalyBased Detection*, dan *Stateful Protocol Inspection*. Berikut penjelasan mengenai macam-macam jenis pendeteksiannya.

1. *Signature-Based Detection*

Sebuah IDS dapat menggunakan pendeteksian *Signature-Based Detetection* dari sebuah paket, bergantung data paket yang diketahui untuk menganalisa potensi terjadinya paket ilegal. Tipe pendeteksi ini sangat cepat dan mudah dikonfigurasi. Bagaimanapun juga seorang penyerang dapat dengan mudah memodifikasi sebuah serangan untuk menyiasati agar tidak terkenali oleh *Signature-Based* IDS. Meskipun kemampuan tipe ini terbatas dalam mendeteksi banyaknya serangan, tipe ini mempunyai kelebihan dalam hal keakuratan (Wu, 2009).

1. *Anomaly-Based Detection*

IDS yang dapat memantau paket jaringan dan mendeteksi data yang tidak valid, atau umumnya tidak normal menggunakan jenis deteksi *Anomaly-Based*. Metode ini berguna untuk mendeteksi paket-paket yang tidak diinginkan (Wu, 2009).

1. *Stateful Protocol Inspection*

*Stateful Protocol Inspection* menyerupai pendeteksi berbasis *anomali*, tetapi jenis ini dapat menganalisa paket lapisan 3 OSI yaitu lapisan *Network* dan lapisan 4 yaitu lapisan *protokol* (Wu, 2009).

### 2.8 *Intrusion Prevention System* (IPS)

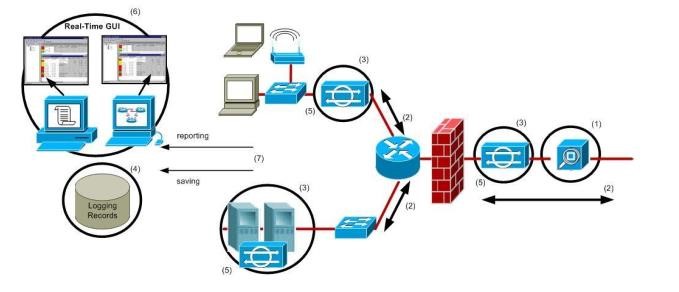
*Intrusion Prevention System* (IPS), adalah pendekatan yang sering digunakan untuk membangun sistem keamanan komputer, IPS mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS) dengan sangat baik. Teknologi ini dapat digunakan untuk mencegah serangan yang masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor, disaat *attack* telah teridentifikasi. IPS akan menolak akses dan mencatat (*log*) semua paket data yang teridentifikasi tersebut. Jadi IPS bertindak sepeti layaknya *firewall* yang melakukan *allow* dan *block* yang dikombinasikan seperti IDS yang dapat mendeteksi paket secara detail (E. Carter, 2006).

*Intrusion prevention system* (IPS) bertugas untuk memonitor paket-paket data (data packet) jaringan dari adanya aktivitas mencurigakan dan mencoba melakukan aksi-aksi tertentu menggunakan kebijakan (policy) tertentu (Xinyau Zhang, 2007). IPS menggunakan *signatures* untuk mendeteksi di aktivitas *traffic* di jaringan dan terminal, dimana pendeteksian paket yang masuk dan keluar (*inbound-outbound*) dapat di cegah sedini mungkin sebelum merusak atau mendapatkan akses ke dalam jaringan lokal. Jadi *early detection* dan *prevention* menjadi penekanan pada IPS ini (E. Carter, 2006).

*Intrusion Prevention System* (IPS) memiliki beberapa tipe yaitu:

1. *Host Based* IPS yang berada pada spesifik *IP address*, biasanya terdapat pada satu komputer.
2. *Network* IPS yang berguna untuk mencegah penyusupan pada spesifik *network*.
3. *Content Spesific* IPS yang memeriksa kontent dari suatu paket dan mencegah berbagai macam serangan seperti serangan *worm*.
4. *Protocol Analysis* Menganalisa berbagai macam *application layer network protocol* seperti *http* dan *ftp*.
5. *Rated Based* berguna mencegah *denial of service*. Berguna untuk memonitoring dan mempelajari keadaan normal *network*. RBIPS dapat memonitoring *traffic* TCP,

UDP, ARP Packets, koneksi per detik, paket per koneksi



## Gambar 2.6 Topologi IPS (Deris S dkk, 2010)

### 2.9 Keamanan *Wireless Local Area Network* (WLAN)

Sebuah sistem yang aman (*secure system*) diasumsikan sebagai sebuah sistem dimana seorang *intruder* harus mengorbankan banyak waktu, tenaga, dan biaya besar yang tidak dikehendakinya untuk melakukan penyusupan atau penyerangan pada sistem, dan resiko yang harus dikeluarkan sangat tidak sebanding dengan keuntungan yang akan diperoleh.

Dalam hal keamanan jaringan, sebuah jaringan dikatakan aman apabila memenuhi 6 prinsip, yaitu :

1. Kerahasiaan (*secrecy*)

*Secrecy* berhubungan dengan hak akses untuk membaca data atau informasi dari suatu sistem komputer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat dibaca oleh pihak yang telah diberi hak atau wewenang secara legal (Megawati, 2012).

1. Integritas (*integrity*)

*Integrity* berhubungan dengan hak akses untuk mengubah data atau informasi dari suatu sistem komputer. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi hanya dapat diubah oleh pihak yang telah diberi hak (Megawati, 2012).

1. Ketersediaan (*availability*)

*Availability* berhubungan dengan ketersediaan data atau informasi pada saat yang dibutuhkan. Dalam hal ini suatu sistem komputer dapat dikatakan aman jika suatu data atau informasi yang terdapat pada sistem komputer dapat diakses dan dimanfaatkan oleh pihak yang berhak (Megawati, 2012).

1. *Authentication*

Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau *server* yang kita hubungi adalah betul-betul *server* yang asli (Megawati, 2012).

1. Akses Kontrol

Akses kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana *user* dan sistem berkomunikasi dan berinteraksi dengan sistem dan sumberdaya yang lainnya. Akses kontrol melindungi sistem dan sumberdaya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkapi (Megawati, 2012).

1. *Non-Repudiation*

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Penggunaan *digital signature*, *certificates*, dan teknologi *kriptografi* secara umum dapat menjaga aspek ini.Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal (Megawati, 2012).

*Wireless* LAN menggunakan teknologi *Radio Frequency* (RF) untuk mentransmisikan data. Jauh lebih sulit untuk menjamin keamanan dalam jaringan *wireless* dari pada jaringan kabel, karena media yang digunakan adalah udara. Dalam jaringan kabel, pengguna harus terhubung langsung melalui kabel ke dalam jaringan LAN Sedangkan *Wireless* LAN bisa diakses dimanapun perangkat *wireless* diletakkan selama masih dalam jangkauan *wireless*. Akses ke dalam suatu jaringan WLAN oleh pengguna yang tidak mempunyai hak dapat mengakibatkan modifikasi data, *denial of service*, penggunaan data informasi yang ada di dalam *Wireless* LAN (Megawati, 2012).

### 2.10 Jejaring Sosial dan E-mail

Pada dasarnya media sosial merupakan perkembangan mutakhir dari teknologiteknologi web baru berbasis internet, yang memudahkan semua orang untuk dapat berkomunikasi, berpartisipasi, saling berbagi dan membentuk sebuah jaringan secara online, sehingga dapat menyebarluaskan konten mereka sendiri. Post di *blog*, *tweet*, atau video *YouTube* dapat direproduksi dan dapat dilihat secara langsung oleh jutaan orang secara gratis. Jejaring sosial mempunyai banyak bentuk, diantaranya yang paling populer yaitu *blog* dan situs *chating Whatsapp* dan *telegram* (Supratman dan Wahyudin, 2017).

Situs jejaring sosial merupakan sebuah situs berbasis pelayanan yang memungkinkan penggunanya untuk membuat profil, melihat list pengguna yang tersedia, serta mengundang atau menerima teman untuk bergabung dalam situs tersebut. Tampilan dasar situs jejaring sosial ini menampilkan halaman profil pengguna, yang di dalamnya terdiri dari identitas diri dan foto pengguna.

Setiap situs jejaring sosial memiliki daya tarik yang berbeda. Namun pada dasarnya tujuannya sama yaitu untuk berkomunikasi dengan mudah dan lebih menarik karena ditambah fitur-fitur yang memanjakan penggunanya. Dengan beberapa penjelasan di atas dapat diambil kesimpulan bahwa situs jejaring sosial merupakan layanan berbasis web dimana digunakan untuk bersosialisasi dan berkomunikasi dengan pihak lain baik dengan teman, keluarga, maupun suatu komunitas yang memiliki tujuan yang sama.

1. *Telegram*

Telegram sebagai salah satu aplikasi pesan instan, mengklaim dapat menutupi beberapa kekurangan yang ada pada *Whatsapp*. Telegram merupakan aplikasi *cloud based* dan alat enkripsi. Telegram menyediakan enkripsi *end-to-end*, *self destruction* *Messages,* dan infrastruktur *multi-data center*. Sebagai aplikasi pesan, telegram memberikan kemudahan akses bagi pengguna karena tersedia pada *platform* *mobile* maupun *desktop*.

Pada *platform* *mobile* telegram dapat digunakan di iPhone/iPad, Android dan Windows phone, sedangkan pada platform *desktop* telegram dapat digunakan di Windows, Linux, Mac OS dan juga Web-browser. Telegram mengklaim sebagai aplikasi pesan massal tercepat dan teraman yang berada di pasar. Selain itu telegram juga menyediakan wadah bagi pengembang yang ingin memanfaatkan *Open API* dan *Protocol* yang disediakan melalui pengembangan telegram *bot* yang didokumentasikan pada web resminya.

Telegram *bot* merupakan akun telegram khusus yang didesain dapat meng*handle* pesan secara otomatis. Pengguna dapat berinteraksi dengan *bot* dengan mengirimkan pesan perintah (*Command*) melalui pesan *private* maupun *group.* Akun telegram *bot* tidak memerlukan tambahan nomor telepon pada pembuatannya, akun ini hanya bertugas sebagai antarmuka dari kode yang berjalan di sebuah *Server*. Telegram *bot* dapat dibangun sesuai dengan kebutuhan, semisal digunakan dengan mengintegrasikannya ke layanan lain untuk mengendalikan *smart home,* membangun *social services,* membangun *custom* *tools,* ataupun melakukan hal lain secara virtual.

1. *Whatsapp*

*WhatsApp* adalah aplikasi pesan instan atau web *chatting*, jika dilihat dari fungsinya *WhatsApp* hampir sama dengan aplikasi SMS yang biasa digunakan pada ponsel versi lama, tetapi *WhatsApp* tidak menggunakan pulsa, melainkan data internet.

*WhatsApp* dibuat pada awal tahun 2009 oleh Ian Koum seorang imigran Ukraina yang tinggal di Mountain View, California (Supratman dan Wahyudin, 2017).

Ide awal Ian Koum dalam membuat *WhatsApp* adalah untuk memberitahukan pengguna cara berbagi status seperti “*I am busy*” atau “*At the gym*” dengan orang-orang dalam jaringan mereka. Inilah sebabnya mengapa aplikasi ini disebut “*WhatsApp*”,

Koum kemudian memilih nama itu karena terdengar seperti “*what’s up*” yang pada dasarnya awalnya dimaksudkan untuk berkomunikasi dengan kontak seseorang.

*WhatsApp* pertama kali diluncurkan pada *iPhone* dan berjuang di awal dengan hanya beberapa orang pengguna yang menggunakannya secara aktif. Kemudian *Apple* memperkenalkan pemberitahuan push pada iOS di bulan Juni 2009 dan Koum menggunakan fitur baru untuk membiarkan kontak pengguna untuk nge-ping setiap kali mereka perbaharui status. Orang-orang segera mulai menggunakan fitur ini untuk berbicara dengan teman-teman dengan memperbaharui status mereka dan hampir secara tidak sengaja *WhatsApp* berubah menjadi layanan pesan (*messaging service*) (Supratman dan Wahyudin, 2017).

*WhatsApp* bukan yang pertama sebagai *platform messaging service* dan menggunakan nomor telepon user untuk login, tidak seperti aplikasi pada *Skype* atau *Gtalk* dimana user register menggunakan *account*. BBM sebenarnya juga melakukan hal yang sama tapi hanya terbatas pada perangkat *BlackBerry*. Sejak awal tahun 2009 *WhatsApp* menggelembung menjadi raksasa dengan memperluasnya ke aplikasi *Android*, *BlackBerry*, menyediakan sebuah situs web seperti *facebook* juga *platform* lainnya dan terus menambahkan fitur yang baru.

*Electronic mail* (E-mail) berfungsi sebagai sarana untuk mengirim surat atau pesan melalui jaringan Intenet, dengan email kita hanya membutuhkan beberapa menit agar surat/pesan dapat sampai tujuan, tidak perlu menunggu berhari-hari seperti mengirim surat/pesan biasa (pos) dan dengan email isi surat/pesan dapat kita isi dengan konten gambar/suara dan video (Supratman dan Wahyudin, 2017).

Email bukan hanya untuk mengirim surat/pesan, saat ini email dapat saling terhubung dengan internet seperti mendaftar facebook, twitter, blogger dan lain-lain.

Sebuah pesan elektronis terdiri dari isi, alamat pengirim, dan alamat-alamat yang dituju. Sistem email yang beroperasi diatas jaringan berbasis pada model store and forward (Supratman dan Wahyudin, 2017).

Sistem ini mengaplikasikan sebuah system server email yang menerima, meneruskan, mengirimkan, serta menyimpan pesan pesan user, dimana user hanya perlu untuk mengkoneksikan pc mereka kedalam jaringan. Email dapat dianalogikan dengan kotak surat yang ada di kantor POS sedangkan server email dapat diibaratkan sebagai kantor POS. Dengan analog ini sebuah mail server dapat memiliki banyak *account email* yang ada didalamnya.

Salah satu layanan email yang sering digunakan adalah *Google Email* (Gmail). Berdasarkan data yang baru diumumkan di *twitter*, jumlah penggunaaktifnya kini telah mencapai 1,5 milyar. Gmailmemulai layanannya di *desktop* pada April 2004 sebagai versi beta terbatas. Titel beta tersebut berakhir pada 2009. Versi java tersedia untuk pengguna ponsel pada 2006. Pada 2012, Gmail memiliki 425 juta pengguna aktif, kemudian jumlahnya naik dua kali lipat menjadi 900 juta pada 2015. Seiring waktu jumlah pengguna akif mengalami peningkatan.

Dengan menggunakan email milik Google ini, pengguna dapat mengakses email dalam bentuk surat web HTTPS, protocol POP3 ataau IMAP4. Gmail menyedikan kapasitas penyimpanan sebanyak lebih dari 7538 *megabyte* dan terus bertambah. Jumlah ini lebih dari jumlah yang disediakan situs lain seperti *Yahoo!* dan *Hotmail*. Hal ini berarti para pengguna dapat menyimpan sampai ribuan surat elektronik. Sampai saat ini, Gmail merupakan email dengan kapasitas terbanyak (Supratman dan Wahyudin, 2017).

### 2.11 *Server*

*Server* merupakan sebuah tempat yang dipenuhi dengan berbagai macam informasi, dimana *server* memiliki tugas utama untuk memberikan sebuah *service* atau layanan bagi para klien yang terhubung dengannya. Terdapat berbagai macam jenis *server* yang ada dengan fungsi yang berbeda-beda, misalnya saja web *server* yang digunakan untuk menyimpan data dalam sebuah web, [FTP *server*](https://www.nesabamedia.com/pengertian-ftp/) yang menangani perpindahan file (transfer file), mail *server* yang melayani urusan email para klien, database *server* untuk menyimpan berbagai macam data atau file dan lain sebagainya (Aliya, 2018).

Walaupun terdapat beragam jenis *server*, namun secara umum sebuah *server* memiliki fungsi yang sama. Berikut merupakan berbagai macam fungsi *server* secara umum:

1. Melayani dan bertanggung jawab penuh terhadap permintaan data dari komputer klien.
2. Menyediakan berbagai macam *resource* untuk dapat digunakan semua komputer klien yang masuk dalam jaringan, baik itu berupa perangkat keras maupun perangkat lunak/aplikasi.
3. Bertanggung jawab dalam mengatur lalu-lintas data.
4. Menyimpan berbagai file dan data untuk dapat diakses bersama-sama menggunakan protokol FTP.
5. Mengatur hak akses (*permissions*) ke dalam sebuah jaringan, sehingga tidak semua klien mampu mengakses data yang terdapat dalam komputer *server*.
6. Menyediakan aplikasi dan database yang mampu dijalankan di semua komputer klien.
7. Memberikan perlindungan untuk komputer klien dengan pemasangan [firewall](https://www.nesabamedia.com/pengertian-firewall-dan-fungsi-firewall/) atau anti malware di komputer klien.

Dengan menggunakan sebuah komputer *server*, berbagai biaya dan juga waktu dapat dipangkas, sehingga sebuah kegiatan menjadi lebih ekonomis. Contoh sebuah perusahaan terdapat sebuah komputer *server* yang terhubung ke semua komputer lain sebagai kliennya, maka sebuah data dapat dibagikan ke sesama klien dalam jaringan perusahaan tersebut (Aliya, 2018).

### 2.12 *Hypertext Preprocessor* (PHP)

*PHP* adalah bahasa komputer atau bahasa pemrograman yang digunakan untuk mengolah data dari server untuk ditampilkan di *website*. PHP di gunakan untuk membuat *website* dinamis. Dalam penggunaan murninya, kode-kode PHP di sisipkan diantara kode HTML.File yang berisi script PHP harus berformat.php (Kristanto, 2010).

Adapun sejarah dari php ituawalnya, PHP merupakan singkatan dari *Personal Home Page* yang digunakan untuk membuat situs pribadi. Namun seiring perkembangannya, akronim PHP diperbaharui. PHP sendiri bermula ketika Rasmus Lerdorf, seorang pemrogram di Denmark/GreenLand pada 1994 membuat script dengan bahasa Perl di *web* pribadinya. Untuk meningkatkan performa, Lerdorf membuat ulang *script* tersebut dalam bahasa C. Script itu memiliki kemampuan untuk memproses form HTML agar dapat berkomunikasi dengan database. Ia memberikan nama dengan sebutan PHP/FI (*Personal Home Page Forum Interpreted)* yang terdiri dari sekumpulan *script* untuk mengolah data formulir dari *web*.

Dengan sebutan PHP/FI yang bersifat *open source* membuat banyak pemrogram yang ikut serta dalam pengembangan PHP. *Script* tersebut dirilis ke publik dengan sebutan PHP Tools version 1.0 pada 8 Juni 1995 melalui sebuah grup diskusi Usenet di alamat *comp.infosystems.www.authoring.cgi*. Pada versi 1.0, dikatakan bahwa PHP merupakan sebuah *framework* bahasa C yang digunakan dalam pengembangan *web*. Pada April 1996, Lerdorf mengumumkan PHP/FI versi 2.0 saat sedang mengerjakan proyek di Universitas Toronto. Proyek tersebut membutuhkan pengolahan data dan desain web yang rumit.

Dalam versi 2.0 ini terjadi penambahan fitur baru seperti fitur logika “*if”* dan *“else”.* Istilah *scripting language* mulai digunakan ketika itu. Pada Pertengahan 1997, Zeev Suraski dan Andi Gutmans yang merupakan pemrograman pendatang baru ikut mengambil bagian untuk membuat ulang interpreter PHP agar lebih stabil. Perilisan PHP versi 3.0 ditandai dengan melakukan perubahan akronim PHP menjadi *Hypertext Preprocessor*. Adapun fungsi dari PHP adalah sebagai berikut:

1. Mempersingkat Tatanan HTML dan CSS

Untuk membangun sebuah halaman web yang dinamis, PHP dapat berfungsi untuk mempersingkat penggunaan tatanan HTML dan CSS. Sebagai contoh, Dalam suatu [sistem](https://www.nesabamedia.com/pengertian-sistem-komputer/) karyawan memiliki jumlah baris 100. Jika menggunakan HTML dan CSS maka barisan tersebut menjadi sangat panjang. Sedangkan jika ditambah dengan menggunakan PHP, maka Anda bisa mengatur beberapa baris yang dibutuhkan atau ditampilkan.

1. Input Data

Dengan menggunakan bahasa pemrograman PHP, Anda dapat menginput data dan menyimpannya dalam sistem *Database*, seperti [MySQL.](https://www.nesabamedia.com/pengertian-mysql/)

1. Manajemen *Cookie* dan *Session*

Dalam PHP, *Cookie* dan *Session* digunakan untuk menyimpan informasi pengguna. *Fungsi session\_start()* untuk memulai *session* dan *cookie* dengan fungsi *setcookie(*). Sebagai contoh proses *cookie*, menyimpan *username* dan *password* pengguna di *browser* sehingga tidak harus mengisinya ulang ketika membuka situs yang sama. *Session* contohnya menyimpan informasi *login* yang hanya berlaku dalam satu sesi saja.

1. Kompress Teks dalam PHP, Anda bisa mengkompres teks yang panjang menjadi lebih pendek dengan fungsi *gzcompress()* dan mengembalikannya dengan fungsi *gzuncompress().*

### 2.13 *Basic Security and Analysis Engine* (BASE)

Menurut Endorf dkk (2004) BASE adalah sistem manajemen basis data berbasis web yang dapat digunakan untuk *query* dan menganalisis *alert* yang berasal dari sistem IDS *snort*. Program ini dapat melakukan analisis dari data *intrusion* yang telah lebih dahulu dideteksi oleh *snort*.

BASE adalah sistem manajemen basis data berbasis desktop yang lengkap, didesain untuk memenuhi kebutuhan yang luas dari pengguna, BASE menawarkan panduan untuk membantu pengguna yang baru terhadap desain basis data (baru terhadap BASE) untuk membuat tabel, *query*, *form*, dan *report*, bersama dengan sekumpulan definisi tabel yang sudah didefinisikan untuk melacak *asset*, konsumen, *invoice*, dan banyak lagi.

Di dalam program BASE ini administrator dapat memutuskan jenis dan banyaknya informasi yang dapat dilihat oleh setiap *user*. BASE memiliki *user interface* yang mudah dipahami, dan di dalam *user interface* tersebut *user* dapat melakukan perubahan terhadap file tertentu.

### 2.14 *Linux Ubuntu*

*Linux* adalah suatu sistem operasi komputer bertipe *unix* yang bersifat *open source*. Karena sifatnya *open source*, maka kode sumber *linux* dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh siapapun. Linux pada awalnya dibuat oleh seorang mahasiswa Finlandia yang bernama Linus Torvalds. Dulunya *linux* merupakan proyek hobi yang diinspirasikan dari Minix, yaitu sistem *unix* kecil yang dikembangkan oleh Andrew Tanenbaum.Linux versi 0.01 dikerjakan sekitar bulan Agustus 1991. Kemudian pada tanggal 5 Oktober 1991, Linus mengumumkan versi resmi *linux*, yaitu versi 0.02 yang hanya dapat menjalankan shell bash (GNU Bourne AgainShell) dan gcc (GNU C Compiler) (Megawati, 2012).

Saat ini *linux* adalah sistem *unix* yang sangat lengkap, bisa digunakan untuk jaringan, pengembangan software dan bahkan untuk pekerjaan sehari-hari. Linux sekarang merupakan alternatif sistem operasi yang jauh lebih murah jika dibandingkan dengan sistem operasi komersial (misalnya Windows 9.x/NT/2000/ME). *Linux* mempunyai perkembangan yang sangat cepat. Hal ini dapat dimungkinkan karena *linux* dikembangkan oleh beragam kelompok orang. Keragaman ini termasuk tingkat pengetahuan, pengalaman serta geografis (Megawati, 2012).

*Linux* bisa didapatkan dalam berbagai distribusi (sering disebut Distro). Distro adalah bundel dari kernel *linux*, beserta sistem dasar linux, program instalasi, tools basic, dan program-program lain yang bermanfaat sesuai dengantujuan pembuatan distro. Ada banyak sekali distro *linux*, diantaranya : Ubuntu, RedHat, Debian, Slackware, SuSE, Fedora, Kali Linux dan lain-lain.

Ubuntu merupakan salah satu distribusi *linux* yang berbasiskan [Debian](https://id.wikipedia.org/wiki/Debian) dan didistribusikan sebagai [perangkat lunak bebas.](https://id.wikipedia.org/wiki/Perangkat_lunak_bebas) Nama Ubuntu berasal dari filosofi dari [Afrika Selatan](https://id.wikipedia.org/wiki/Afrika_Selatan) yang berarti kemanusiaan kepada sesama. Ubuntu dirancang untuk kepentingan penggunaan pribadi, namun versi *server* Ubuntu juga tersedia, dan telah dipakai secara luas (Megawati, 2012).

Proyek Ubuntu resmi disponsori oleh [Canonical Ltd.](https://id.wikipedia.org/wiki/Canonical_Ltd.) yang merupakan sebuah perusahaan yang dimiliki oleh pengusaha [Afrika Selatan](https://id.wikipedia.org/wiki/Afrika_Selatan) Mark Shuttleworth. Tujuan dari distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam filosofi Ubuntu ke dalam dunia perangkat lunak. Ubuntu adalah [sistem operasi](https://id.wikipedia.org/wiki/Sistem_operasi) lengkap berbasis *linux*, tersedia secara bebas, dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli profesional.

### 2.15 *Snort*

*Snort* merupakan IDS yang gratis dan berbasis *open source* yang diciptakan oleh Martin Roesch pada tahun 1998. Snort dikembangkan oleh *Sourcefire* dengan Roesch sebagai pendiri sekaligus CTO dari Sourcefire. *Snort* sebagai IDS berbasis jaringan *open source* memiliki kemampuan untuk menganalisa lalu lintas jaringan secara *real time* dan pendataan paket pada IP jaringan (Pradana, 2016).

*Snort* bekerja dengan melakukan analisa protokol, pencarian dan pencocokan konten, dan digunakan secara aktif untuk mendeteksi suatu serangan. *Snort* memiliki beberapa komponen yang setiap komponennya mempunyai tugas masing-masing. Pada saat paket jaringan yang melewati *Ethernet* dimana snort dipasang, maka ada beberapa hal yang dilalui:

## 1. *Packet capture library (libpcap)*

*Libpcap* akan melakukan pemisahan paket data yang melalui *Ethernet card* untuk selanjutnya digunakan oleh snort.

## 2. *Packet decoder*

*Packet decoder* mengambil data yang dikirim dari proses 1. Kemudian snort akan memisahkan data link seperti Ethernet, tokenRing, 802.11, kemudian protokol IP, dan selanjutnya paket TCP dan UDP. Setelah pemisahan data selesai, snort telah mempunyai informasi protokol yang dapat diproses lebih lanjut.

## 3. *Preprocessor*

*Preprocessor* yaitu tahap analisis atau manipulasi terhadap paket sebelum dikirim ke *detection engine.* Manipulasi paket berupa penandaan dan pengelompokan.

## 4. *Detection Engine*

Paket dari *packet decoder* akan ditest dan dibandingkan dengan *rules* yang telah ditetapkan sebelumnya. *Rules* berisi tanda-tanda (*Signature*) yang termasuk serangan.

## 5. *Output*

*Output* berupa *report* dan *alert* yang dapat berupa *text, syslog, tcpdump, binary format,* atau *database.*

### 2.16 IPTables

IPTables adalah *Intrusion Prevention System* (IPS) dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalu lintas data dalam komputer, baik yang masuk ke komputer, keluar dari komputer, maupun sekedar melewati komputer. Secara sederhana digambarkan sebagai pengatur lalu lintas data.

*Iptables* merupakan *Firewall*, yang default diinstall hampir semua distribusi Linux, seperti, Ubuntu, Kubuntu, Xubuntu, Fedora Core, dan lain-lain. Iptables sudah terinstall, tapi defaultnya mengizinkan semua trafik untuk lewat (Purbo, 2006).

Firewall adalah potongan perangkat lunak yang mengatur komunikasi antar jaringan tak aman (*insecure*), seperti internet dan jaringan aman (*secure*), seperti LAN perusahaan. Komunikasi ini di atur oleh aturan-aturan akses. Firewall merupakan benteng keamanan dalam internet yang berfungsi melindungi jaringan kecil dari jaringan internet yang lua.

### 2.17 *Port*

*Port*adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. *Port* dapat dikenali dengan angka 16-Bit (dua *byte*) yang disebut dengan *Port Number* dan diklasifikasikan dengan jenis protokol transport apa yang digunakan, ke dalam *Port* TCPdan *Port* UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah *port* untuk setiap protokol *transport* yang digunakan adalah 65536 buah (Beaver, 2004).

*Port* yang memiliki akses paling banyak dalam sebuah jaringan adalah *port* ICMP (*Internet Message Control Protocol*) , FTP (*File Transfer Protocol*), SSH (*Secure Shell*), Telnet (Telecommunication network) dan HTTP (Hypertext Transfer Protocol).

1. ICMP (*Internet Message Control Protocol*)

Internet Control Message Protocol (ICMP : 138) adalah salah satu protokol inti dari keluarga protko[l internet.](https://id.wikipedia.org/w/index.php?title=Keluarga_protokol_internet&action=edit&redlink=1) ICMP utamanya digunakan oleh [sistem operasi](https://id.wikipedia.org/wiki/Sistem_operasi) [komputer](https://id.wikipedia.org/wiki/Komputer) jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau (Beaver, 2004).

1. FTP (*File Transfer Protocol*)

*File Transfer Protocol* (FTP : 21) adalah sebuah [protokol *Internet*](https://id.wikipedia.org/wiki/Protokol_Internet) yang dapat berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman  [berkas](https://id.wikipedia.org/wiki/Berkas_komputer)  (*file*)  [komputer](https://id.wikipedia.org/wiki/Komputer)  antar mesin-mesin dalam sebuah [antar jaringan.](https://id.wikipedia.org/wiki/Antarjaringan) FTP merupakan salah satu protokol *Internet* yang paling awal dikembangkan, dan masih digunakan hingga saat ini untuk melakukan [pengunduhan](https://id.wikipedia.org/wiki/Download)

[(*download*)](https://id.wikipedia.org/wiki/Download)  dan [penggugahan (*upload*)](https://id.wikipedia.org/wiki/Upload) berkas-berkas komputer antara klien FTP dan *server* FTP (Beaver, 2004).

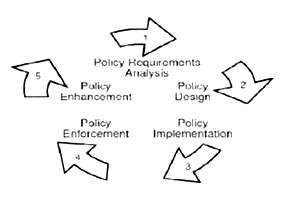
1. SSH (*Secure Shell*)

*Secure Shell* (SSH: 22) menggunakan kriptografi kunci publik untuk mengotentikasi komputer *remote*  dan biarkan computer *remote*  untuk mengotentikasi pengguna, jika perlu. Ada beberapa cara untuk menggunakan SSH, salah satunya adalah dengan menggunakan secara otomatis pasangan *public-privat key* untuk mengenkripsi koneksi jaringan, dan kemudian menggunakan otentikasi *password* untuk *login* (Beaver, 2004).4. Telnet (*Telecommunication Network*)

*Telecommunications Network Protocol* (*Telnet*: 23) adalah perangkat lunak yang digunakan untuk melakukan kontrol jarak jauh pada sistem komputer. Pengertian dari *Telnet* bisa dijabarkan sebagai *remote* *login* yang yang terjadi pada jaringan komputer yang memungkinkan penggunanya dapat melakukan *login* dan bekerja dari jarak yang jauh melalui jaringan *internet*. Pengguna dapat mengakses dan menjalankan komputer dari jarak yang jauh melalui *service* dari protokol *telnet* (Beaver, 2004).

### 2.18 *Security Policy Development Life Cycle* (SPDLC)

*Security Policy Development Life Cycle* (SPDLC) adalah suatu pendekatan proses dalam komunikasi data yang menggambarkan siklus yang tiada awal dan akhirnya. Dalam membangun sebuah jaringan komputer mencakup lima tahap, yaitu *analysis, design, implementation, enforcement dan enhancement* (Wahsheh dan Jim, 2008).



**Gambar 2.7 *Security Policy Development Life Cycle* (SPDLC)**

## (Wahsheh dan Jim, 2008) 1. *Analysis*

*Analysis* adalah sebuah proses yang dilakukan untuk pemecahan sebuah permasalahan.

## 2. *Design*

*Design* adalah proses penggambaran pemecahan masalah dengan solusi yang ditawarkan.

## 3. *Implementation*

*Implementation* adalah proses untuk mewujudkan sebuah sistem baru kedalam sistem yang sebenarnya.

## 4. *Enforcement*

*Enforcement* adalah proses pengujian sistem dan penyelesaian dari kasus tersebut.

**5. *Enhancement***

*Enhancement* adalah peningkatan pada sistem untuk kebijakan selanjutnya.

**BAB III**

**METODOLOGI PENELITIAN**

## 3.1 Metode Pengumpulan Data

Untuk pengumpulan sejumlah data yang diperlukan dalam penyusunan tugas akhir ini, penulis menggunakan Studi literatur. Pengumpulan data, gambaran dan keterangan yang lebih lengkap peneliti menggunakan studi literatur dengan cara mengumpulkan dan mempelajari literatur yang berkaitan dengan perangkat lunak yang dibuat dan membantu memperjelas teori-teori yang ada. Sumber literatur berupa buku teks,jurnal*,* karya ilmiah dan situs-situs penunjang.

## 3.2 Metode Pengembangan Sistem

Metode pengembangan sistem yang gunakan yaitu *Security Policy Development Life Cycle* (*SPDLC)*, dalam pengembangan sistem SPDLC memiliki lima tahapan yaitu *Analysis, Design, Implementation, Enforcment, Enhancement.*

# Tabel 3.1 Fase pengembangan *system*

|  |  |
| --- | --- |
| **Fase SPDLC** | **Proses yang dilakukan** |
| *Analysis* | Menganalisa spesifik sistem yang akan dibangun seperti perangkat lunak (software) dan perangkat keras (hardware) yang dibutuhkan untuk sistem IDS dan IPS. |
| *Design* | Merancang topologi jaringan serta *flowchart* sistem untuk simulasi sistem IDS dan IPS dan sebagai gambaran umum sistem. |
| *Implementation* | Instalasi dan Konfigurasi sistem IDS dan IPS (*Snort*, *IPTables* dan *BASE*) dan media notifikasi *(telegram dan whatsapp)* serta email *(google mail)* |
| *Enforcment* | Pada tahap ini meliputi pengoperasian, pengamatan, pengujian sistem dan pengiriman notifikasi pada |

33

34

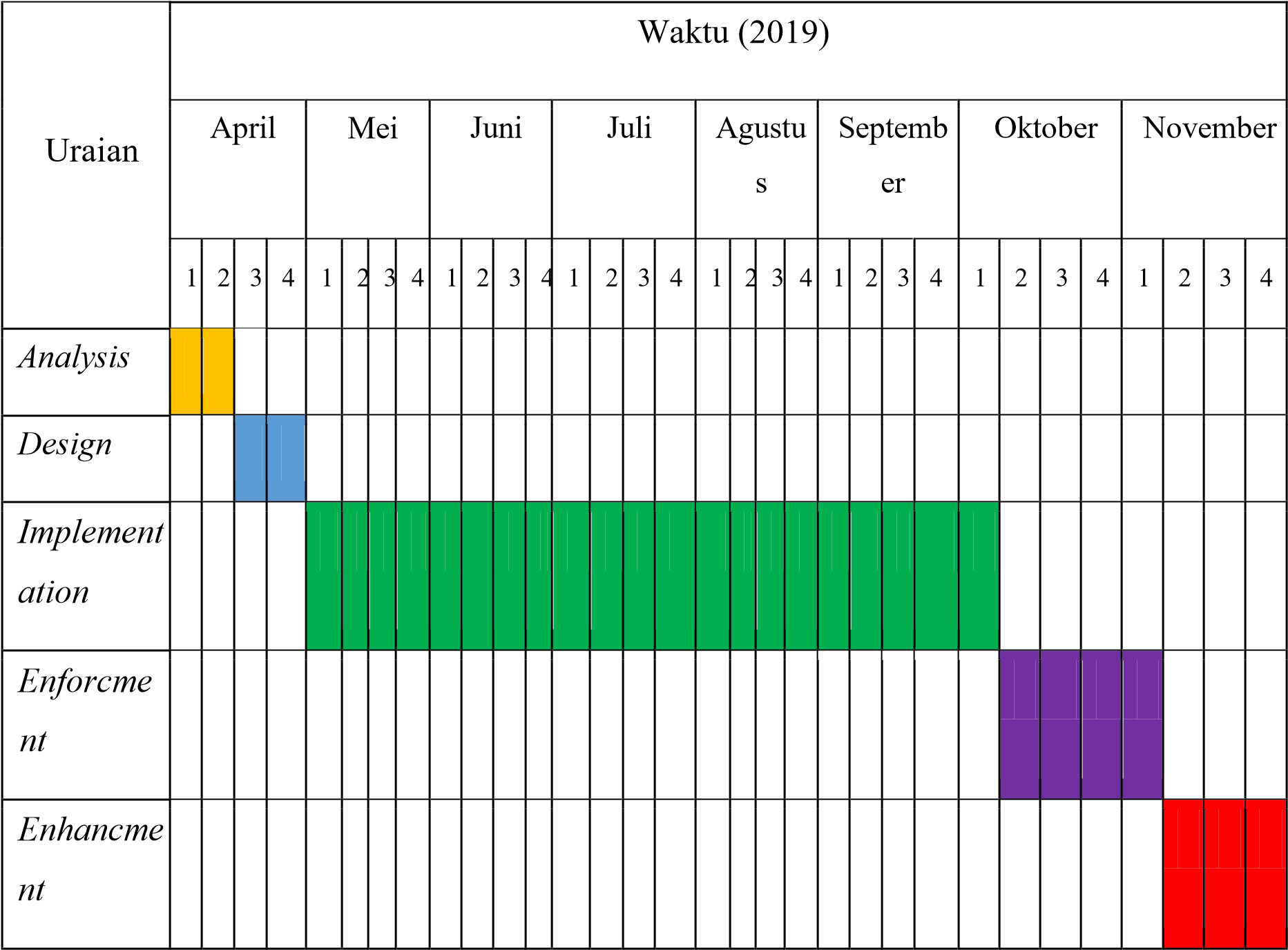
|  |  |
| --- | --- |
|  | sistem IDS dan IPS *Server* pada jaringan *wireless* di Lab Multimedia dan AI. |
| *Enhancment* | Memperbaiki masalah-masalah yang muncul saat pembuatan dan setelah pengujian sistem. |

### 3.3 Waktu dan Tempat Penelitian

**3.3.1 Waktu Penelitian**

Waktu yang diperlukan dalam penelitian ini dapat dilihat pada Tabel 3.2.

# Tabel 3.2 Tabel waktu kegiatan



### 3.3.2 Tempat Penelitian

Penelitian tugas akhir bertempat di Laboratorium Multimedia dan AI, Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kota Kendari, Sulawesi Tenggara.

## DAFTAR PUSTAKA

Aliya, Nadira. 2018, Pengertian Server, Fungsi Server Beserta Cara Kerja dan Jenisjenis Server, [https://www.nesabamedia.com/pengertian-server-dan-fungsiserver/,](https://www.nesabamedia.com/pengertian-server-dan-fungsi-server/) diakses 10 Mei 2018, jam 02.51

Ariyus, D., 2007, *Intrusion Detection System*, Yogyakarta: ANDI Yogyakarta

Arsin, F., 2017, Implementasi *Security System* Menggunakan Metode IDPS (*Intrusion Detection & Prevention System*) Dengan *Real Time Notification, Skripsi,* Universitas Halu Oleo, Kendari

Beaver, Kevin, 2004, Hacking for Dummies. Willey Publishing, Indianapolis, Indiana

C. Endorf, E. Schultz and J. Mellander, 2014, *Intrusion Detection & Prevention*, Boston: McGraw-Hill

Deris S, A. Hanan dan M. Yazid, 2010, “The Measurement Internet Services”,

International Conferences on Green Computing

E. Carter, et al., 2006, “Intrusion Prevention Fundamentals: an introduction to network attack mitigation with IPS”,Cisco press

Fathoni, W., dkk, 2016, Deteksi Penyusupan Pada Jaringan Komputer Menggunakan IDS *Snort, Skripsi,* Universitas Telkom, Bandung

Kimin, V. H., 2010, *Perancangan Sistem Keamanan Jaringan Komputer Berbasis Snort Intrusion Detection System* dan *IPTables Firewall*, Sumatera Utara: Universitas Sumatera Utara

Kristanto,A., 2010, *Kupas Tuntas PHP dan MySQL*, Klaten: Cable Book

Kurniawan, I. N., 2010, Sistem Deteksi dan Penanganan Intrusi Menggunakan Snort dan Base, *Skripsi*, IST AKPRIND, Yogyakarta

Megawati, C., 2012, Implementasi dan Analisa Unjuk Kerja Sistem Keamanan

Jaringan *Wireless* Berbasis Linux Platform dan DD-WRT *Firmware*, *Skripsi*,

Universitas Indonesia, Depok

Husain S.S., Muh. S., 2018, Implementasi Keamanan *Server* Pada Jaringan *Wireless* Menggunakan Metode *Intrusion Detection And Prevention System* (IDPS), *Skripsi,* Universitas Halu Oleo, Kendari

Nugroho, B., 2013, *Instalasi dan Konfigurasi topologi jaringan,* Yogyakarta: ANDI Yogyakarta

Nugroho, dkk, 2015, “Perancangan dan Implementasi IDSdi Jaringan Universitas Diponegoro”, *Skripsi*, Universitas Diponegoro, Semarang

Pradana, B. Y., 2016, Membandingkan Kemampuan Deteksi *Intrusion Detection System* (IDS) Snort dan Suricata Berbasis Aturan/Rules Standar Pengembang, *Skripsi*, Universitas Sanata Dharma, Yogyakarta

Purbo, Onno. W., 2006,*Buku Pegangan Internet, Wireless dan Hotspot*, Jakarta: Elex Media Komputindo

Putri, L., 2011, Implementasi *Intrusion Detection System* (IDS) menggunakan *Snort* pada Jaringan *Wireless*, *Skripsi*, UIN Syarif Hidayatullah, Jakarta

Rajab, M., 2010, *Analisa dan Perancangan Wireless LAN Security Menggunakan*

*WPA2-RADIUS*, *Skripsi*, Universitas Islam Negeri Syarif Hidayatullah, Jakarta

Rochim, H. N., 2016, Rancang Bangun Telegram Bot Pada Telegram *Messenger* Dengan Metode Long Polling Untuk Koperasi KOPMA, *Skripsi*, Universitas Gadjah Mada, Yogyakarta

Ratnaningsih, I., 2012, Sistem Keamanan Jaringan Komputer menggunakan *Intrusion Detection System* (IDS) pada *Linux*, *Skripsi*, IST AKPRIND, Yogyakarta

Sahid, A. B., dkk, 2014, Implementasi *Intrusion Detection System* (IDS) Menggunakan

Jejaring Sosial Sebagai Media Notifikasi, Teknik Informatika, IST AKPRIND, Yogyakarta

Saputra, A. R, 2013, Analisa Perbandingan Metode Load Balancing Peer Connection

Classifier (Pcc) Dengan nth Pada Router Mikrotik, *Skripsi,* Tekhnologi Informatika UIN, Bandung

Sofana, I., 2013, *Membangun Jaringan Komputer*, Bandung: Informatika Bandung Sopandi, D., 2008, *Instalasi dan Konfigurasi Jaringan Komputer*, Bandung: Informatika Bandung

Sugeng, W., 2010, *Jaringan Komputer dengan TCP/IP*, Bandung: Modula Community

Supratman, L. P., Wahyudin, A., 2017, Penggunaan Media Sosial oleh Digital Native International Journal of English Literature and Social Sciences, *2*(5): 51-58

Yuhefizar, 2008, *10 Jam Menguasai Internet Teknologi dan Aplikasinya*, Jakarta: PT. Elex Media Komputindo

Wahsheh, Luay A dan Foss, Jim Alves, 2008, *Security Policy Development:Towards a Life-Cycle and Logic-Based Verification Model* USA

Wu, Tzeyoung Max., 2009, *Information Assurance Tools Report – Intrusion* *Detection Systems Sixth Edition,* Herndon: IATAC