# BAB II
# TINJAUAN PUSTAKA

## 2.1. Penelitian Terdahulu

Rujukan penelitian yang pertama yaitu jurnal mahasiswa program studi Teknik Informatika Politeknik TEDC Bandung (Syani dan Ropi, 2018) dengan judul Analisis Dan Implementasi *Network Security System* Menggunakan Teknik *Host-Based Intrusion Detection System* (HIDS) Berbasis *Cloud Computing*. Dalam penelitiannya, peniliti bermaksud untuk menggunakan *Cloud Computing* sebagai perantara untuk menganalisis dan mengimplementasikan sistem keamanan jaringan menggunakan teknik *Host-Based Intrusion Detection System* dari IDS dengan *software* OSSEC sebagai *tools* keamanan jaringannya.

Rujukan penelitian yang kedua yaitu jurnal mahasiswa jurusan Sistem Komputer Universitas Komputer Indonesia (Rakhman dan Lestariningati, 2015) dengan judul Perancangan IDS Dengan Teknik HIDS (*Host Based Intrusion Detection System*) Menggunakan *Software* OSSEC. Dalam penilitiannya, peniliti merancang sistem keamanan jaringan menggunakan teknik HIDS pada *server* dengan sistem operasi Ubuntu.

## 2.2. Personal Computer (PC)

Personal Komputer adalah komputer yang merujuk pada komputer yang dapat digunakan dan diperoleh oleh orang-orang dengan mudah. PC ini juga merujuk kepada mikrokomputer 1 yang sesuai dengan spesifikasi Komputer IBM. Komputer pribadi pertama kali didistribusi dan dikeluarkan oleh perusahaan IBM dan secara tidak langsung mencetuskan penggunaan istila PC. (Tedjamaja, 2019).

**Gambar 2.1** Personal Komputer

## 2.3. Jaringan Komputer

Jaringan komputer adalah “interkoneksi” antara 2 komputer autonomous atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (wireless). Autonomous adalah apabila sebuah komputer tidak melakukan kontrol terhadap komptuer lain dengan akses penuh, sehingga dapat membuat komputer lain, restart, shutdown, kehilangan file atau kerusakan sistem. (Wongkar, 2015)

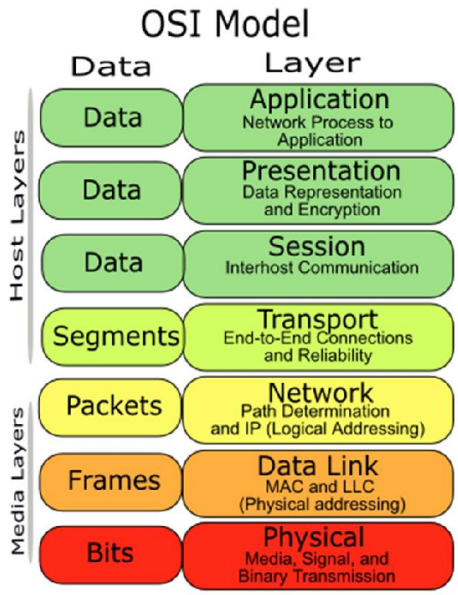
## 2.4. Keamanan Jaringan Komputer

Keamanan jaringan adalah data-data yang berada pada perangkat keras dan perangkat lunak dalam sistem jaringan dilindungi dari tindakan-tindakan yang bersifat jahat atau merusak, modifikasi dan hal-hal yang bersifat membocorkan data ke pihak lain, untuk memastikan sistem akan berjalan secara konsisten dan handal tanpa adanya gangguan pada sistem tersebut.(Fauzi and Suartana 2018). Keamanan jaringan adalah komponen yang paling vital dalam keamanan informasi karena bertanggung jawab untuk mengamankan semua informasi melewati komputer berjejaring. Keamanan Jaringan mengacu pada semua fungsi perangkat keras dan perangkat lunak, karakteristik, fitur, prosedur operasional, akuntabilitas, tindakan, kontrol akses, dan administrasi dan manajemen kebijakan yang diperlukan untuk memberikan tingkat perlindungan yang dapat diterima untuk perangkat keras dan perangkat lunak, dan informasi dalam jaringan.

Masalah keamanan jaringan dapat dibagi secara kasar menjadi empat bidang yang saling terkait: kerahasiaan, otentikasi, nonrepudiation, dan integrity control. Kerahasiaan berkaitan dengan menjaga informasi dari tangan dari pengguna yang tidak berhak. Inilah yang biasanya terlintas dalam pikiran ketika orang memikirkan keamanan jaringan. Otentikasi berhubungan dengan menentukan siapa yang Anda ajak bicara sebelum mengungkapkan informasi sensitif atau memasuki kesepakatan bisnis. Nonrepudiasi berurusan dengan tanda tangan Integritas Pesan: Sekalipun pengirim dan penerima saling mengotentikasi, mereka juga ingin memastikan bahwa isi komunikasi mereka tidak berubah.

## 2.5. OSI Layer

OSI Layer adalah model referensi yang membantu terjadinya transfer data antar host yang berbeda. Layer OSI (Open System Interconnection) tercipta pada akhir tahun 1970 oleh International Organization for Standarization. Layer OSI terdiri atas tujuh lapisan yaitu Layer Application, Layer Presentation, Layer Session, Layer Transport, Layer *Network*, Layer Data Link, Layer Physical. (Sirait dan Putra, 2018). OSI Layer merupakan model referensi yang digunakan untuk memahami jaringan komputer secara umum. Secara *de facto*, OSI layer telah dijadikan sebagai acuan saat mempelajari *network* yang dibangun menggunakan perangkat Cisco. OSI Reference Model atau model referensi OSI terdiri atas lapisan berjumlah 7 buah (layer).




**Gambar 2.2** Model OSI Layer

**Layer 7 : Application Layer**

Merupakan layer dimana terjadi interaksi antarmuka end user dengan aplikasi yang bekerja menggunakan fungsionalitas jaringan, melakukan pengaturan bagaimana aplikasi bekerja menggunakan resource jaringan, untuk kemudian memberika pesan ketika terjadi kesalahan. Beberapa service dan protokol yang berada di layer ini misalnya HTTP, FTP, SMTP, dll.

**Layer 6 : Presentation Layer**

Layer ini bekerja dengan mentranslasikan format data yang hendak ditransmisikan oleh aplikasi melalui jaringan, ke dalam format yang bisa ditransmisikan oleh jaringan. Pada layer ini juga data akan di-enkripsi atau di-deskripsi.

**Layer 5 : Session Layer**

Session layer akan mendefinisikan bagaimana koneksi dapat dibuat, dipelihara, atau dihancurkan. Di layer ini ada protocol Name Recognition,NFS & SMB.

**Layer 4 : Transport Layer**

Layer ini akan melakukan pemecahan data ke dalam paket-paket data serta memberikan nomor urut pada paket-paket data tersebut sehingga dapat disusun kembali ketika sudah sampai pada sisi tujuan. Selain itu, pada layer ini, akan menentukan protokol yang akan digunakan untuk mentransmisi data, misalkan protokol TCP. Protokol ini akan mengirimkan paket data, sekaligus akan memastikan bahwa paket diterima dengan sukses (acknowledgement), dan mentransmisikan ulang terhadap paket-paket yang hilang atau rusak di tengah jalan.

**Layer 3 : *Network* Layer**

*Network* layer akan membuat header untuk paket-paket yang berisi informasi IP, baik IP pengirim data maupun IP tujuan data. Pada kondisi tertentu, layer ini juga akan melakukan routing melalui inter*network*ing dengan menggunakan router dan switch layer-3.

**Layer 2 : Data-link Layer**

Befungsi untuk menentukan bagaimana bit-bit data dikelompokkan menjadi format yang disebut sebagai frame. Selain itu, pada level ini terjadi koreksi kesalahan, flow control, pengalamatan perangkat keras (seperti halnya Media Access Control Address (MAC Address)), dan menetukan bagaimana perangkat-perangkat jaringan seperti hub, bridge, repeater, dan switch layer 2 beroperasi.

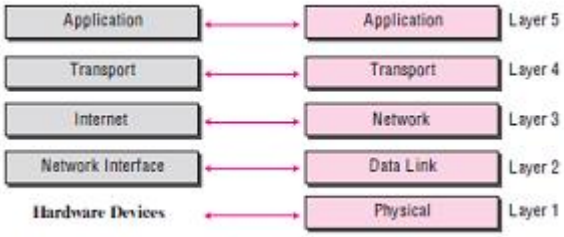
Spesifikasi IEEE 802, membagi level ini menjadi dua level anak, yaitu lapisan Logical Link Control (LLC) dan lapisan Media Access Control (MAC).

**Layer 1 : Physical Layer**

Layer Physcal berkerja dengan mendefinisikan media transmisi jaringan, metode pensinyalan, sinkronisasi bit, arsitektur jaringan (seperti halnya Ethernet atau Token Ring), topologi jaringan dan pengabelan. Selain itu, level ini juga mendefinisikan bagaimana *Network* Interface Card (NIC) dapat berinteraksi dengan media kabel atau radio.

### 2.5.1. TCP/IP *Protocol Suite*

Protokol TCP/IP yang original didefinisikan sebagai empat lapisan perangkat lunak yang dibangung diatas perangkat kerass. Tapi saat ini TCP/IP dianggap sebagai model dengan lima layer dengan lapisan yang bernama dengan yang ada di model OSI.




**Gambar 2.3** Protokol TCP/IP

Berikut ini adalah lapisan-lapisan dari protokol TCP/IP yang digunakan sebagai standar saat ini:

1. Physicial Layer,
2. Data Link Layer,
3. Network Layer,
4. Transport Layer, dan
5. Application Layer.

## 2.6. Topologi Jaringan

Topologi adalah pola aturan untuk menghungkan komputer dan komponen jaringan satu sama lain secara fisik dan pola hubungan antar komponen yang berkomunikasi di dalam jaringan. Ada dua jenis topologi yaitu topologi fisik dan topologi logika. Topologi fisik terdiri dari topologi *Bus, Star, Ring* dan *Mesh*. Sedangkan topologi logika terdiri dari *Shared Media* dan *Token Based*.

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

*Intrusion Detection System* (IDS) merupakan sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan pada sebuah sistem atau jaringan.(Gondohanindijo 2011). IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan aktivitas yang mencurigakan pada *traffic* jaringan maka IDS akan memberikan sebuah peringatan terhadap sistem atau administrator jaringan dan melakukan analisis dan mencari bukti dari percobaan penyusupan. Ada dua teknik IDS yaitu *Network based* IDS (NIDS) dan *Host based* IDS (HIDS).

### 2.7.1. Tujuan Penggunaan IDS

IDS (*Intrutrusion Detection System*) merupakan adalah sebuah sistem yang melakukan pengawasan terhadap *traffic* jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. (Fauzi dan Suartana, 2018). IDS merupakan software atau hardware yang melakukan otomasi proses monitoring kejadian yang muncul di sistem komputer atau jaringan dan menganalisanya untuk menemukan permasalahan keamanan. IDS adalah pemberi sinyal pertama jika seorang penyusup mencoba membobol sistem keamanan komputer. Secara umum penyusupan dapat berarti serangan atau ancaman terhadap keamanan dan integritas data, serta tindakan atau percobaan untuk melewati sebuah sistem keamanan yang dilakukan oleh seseorang dari internet atau dari dalam sistem.

IDS dibuat bukan untuk menggantikan fungsi *firewall* karena kegunaannya berbeda. Sebuah sistem *firewall* tidak dapat mengetahui apakah sebuah serangan sedang terjadi atau tidak, tapi IDS dapat mengetahuinya. Dengan meningkatnya

jumlah serangan pada jaringan, IDS merupakan sesuatu yang diperlukan pada infrastruktur keamanan di kebanyakan organisasi. Secara singkat, fungsi IDS adalah pemberi peringatan kepada administrator atas serangan yang terjadi pada sistem

### 2.7.2. Jenis - Jenis IDS

**1. *Network*-based Intrusion Detection System (NIDS)**

Tugas NIDS ialah memonitor dan menganalisis *traffic* pada keseluruhan subnet *network*, dimana NIDS ini akan meng-*capture* semua *traffic* seperti sebuah sniffer. Untuk mengumpulkan semua *traffic* pada *network*, implementasinya bisa menggunakan *network tap* atau *port mirror*, dimana intinya adalah mengirimkan *copy* dari semua *traffic* pada *network* ke IDS. NIDS bekerja dengan mengkombinasikan *signature analysis*, *anomaly analysis*, dan *application/protocol analysis*.

- Pada signature analysis digunakan semacam rule untuk mengidentifikasi suatu log atau packet jaringan yang ter-capture. Masing-masing aktifitas memiliki ciri (*signature*) tersendiri, ciri tersebut kemudian dijadikan rule untuk menghasilkan alert.
- Pada anomaly analysis, IDS menggunakan data yang telah disediakan oleh vendor aplikasi/protocol maupun sumber lainnya tentang aktifitas apa saja yang normal dan yang tidak (diluar kondisi biasanya) pada aplikasi/*protocol* tersebut, untuk kemudian dijadikan rule untuk menghasilkan *alert*.
- Pada application/protocol analysis bekerja dengan mengidentifikasi secara detail kerja dari aplikasi/protocol tersebut, yang mana dapat digunakan untuk mengidentifikasi adanya serangan seperti DoS, *buffer overflow*, dan lainnya.

**2. *Host-based Intrusion Detection System* (HIDS)**

Tugas HIDS ialah memonitor dan menganalisis *traffic network* yang berasal dan keluar dari sebuah *host* dimana perangkat HIDS tersebut diimplementasi. Perbedaannya dengan NIDS, HIDS hanya memonitor spesifik *host* saja, sedangkan

NIDS memonitor seluruh *subnet*. Karena memonitor spesifik *host*, maka HIDS lebih dapat 'melihat banyak' aktifitas yang ada pada suatu host, seperti dapat melihat apakah pada suatu host tersebut terdapat aktifitas *port scan*, *malware* ataupun adanya *vulnerability* pada *host* tersebut, dengan cara memonitor log yang dikirimkan oleh host tersebut. HIDS juga melakukan semacam *snap shot* terhadap sistem host tersebut dan akan mencocokkan dengan *snap shot* sebelumnya. Apabila sistem mengalami perubahan atau penghapusan, *alert* akan dikirimkan untuk selanjutnya diinvestigasi oleh *security analyst*.

### 2.7.3. Cara Kerja IDS

Berdasarkan cara kerja IDS dalam menganalisis apakah paket data dianggap sebagai penyusupan atau bukan, IDS dibagi 2 yaitu:

1. *Knowledge-based* atau *misuse detection*
   Cara kerjanya adalah menyadap paket data kemudian membandingkannya dengan database rule IDS (berisi signature-signature paket serangan). Jika paket data mempunyai pola dengan salah satu pola di database rule IDS, maka data tersebut dianggap sebagai serangan.
2. *Behavior-based* atau *anomaly based*
   Cara kerjanya adalah dengan mengamati adanya kejanggalan-kejanggalan pada sistem, sebagai contoh adanya penggunaan memori yang meningkat secara terus- menerus atau ada koneksi paralel dari 1 IP dalam jumlah banyak dan dalam waktu yang bersamaan.

Berdasarkan kemampuan mendeteksi penyusupan pada jaringan, IDS dibagi 2 yaitu:

1. *Host based Intrusion Detection System*, hanya mampu mendeteksi penyusupan pada host tempat implementasi IDS.
2. *Network based Intrusion Detection System* mampu mendeteksi seluruh host yang berada satu jaringan dengan host implementasi IDS tersebut

## 2.8. *Firewall*

*Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, *firewall* diterapkan dalam sebuah mesin yang terdedikasi, yang berjalan pada *gateway* antara jaringan lokal dan jaringan lainnya. *Firewall* umumnya digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan lokal dari pihak luar. (Suparsin and Mariaty 2011). Saat ini, istilah *firewall* menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Secara fundamental , *firewall* dapat berfungsi sebagai berikut:

1. Mengatur dan mengontrol lalu lintas jaringan.
2. Melakukan autentikasi terhadap akses.
3. Melindungi sumber daya dalam jaringan lokal.

### 2.8.1. Jenis-Jenis *Firewall*

*Firewall* terbagi menjadi dua jenis, yaitu sebagai berikut:

1. Personal *Firewall*

Didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. *Firewall* jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total dengan ditambahkannya beberapa fitur pengaman tambahan seperti perangkat proteksi terhadap virus, anti-spyware, anti-spam,dll. Bahkan beberapa produk *firewall* lainnya dilengkai dengan fungsi pendeteksian gangguan keamanan jaringan (Intrusion Detection System). Contoh *firewall* dari jenis ini adalah Microsoft Windows *Firewall*. Personal *firewall* secara umum hanya memiliki dua fitur utama, yaitu Packet Filter *Firewall* dan Stateful *Firewall*.

2. *Network Firewall*

Didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Ada dua bentuk yaitu sebuah perangkat yang terdedikasi atau sebuah perangkat lunak yang diinstalasikan dalam sebuah *server*. *Network Firewall* secara

umum mempunyai beberapa fitur utama yaitu Packet Filter *Firewall*, Stateful *Firewall*, Circuit Level Gateway, Application Level Gateway, dan NAT *Firewall*. *Network Firewall* umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang dizinkan, dan paket mana yang ditolak.

## 2.9. Jenis Serangan

### 2.9.1. *Denial of Service*

*Denial of service* merupakan jenis serangan terhadap sebuah komputer atau *server* dengan cara menghabiskan resources (sumber) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain mendapatkan layanan dari *server*/komputer yang diserang tersebut. (Suparsin and Mariaty, 2011). Beberapa cara yang dilakukan oleh penyerang dalam melakukan *Denial of Service*, yakni sebagai berikut:

1. *Traffic flooding* merupakan teknik yang digunakan dengan membanjiri *traffic network* dengan data sehingga *traffic network* yang datang dari pengguna yang terdaftar, tidak dapat masuk ke dalam sistem jaringan.
2. *Request flooding* dilakukan dengan membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga request yang datang dari pengguna yang terdaftar tidak dapat dilayani oleh layanan tersebut.
3. Mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan *server* yang dapat mengganggu komunikasi antara host dengan kliennya.

### 2.9.2. *Scanning*

*Scanning* merupakan aktivitas yang dilakukan untuk mendapatkan informasi target. Adapun informasi yang ditemukan oleh penyerang antara lain IP address, sistem operasi, arsitektur sistem, service running di tiap komputer. (Suparsin and Mariaty, 2011).

*Scanning* dapat dibagi menjadi tiga jenis yaitu:

1. Port Scanning merupakan scanning yang bertujuan untuk menemukan port-port yang terbuka dari suatu host.
2. *Network* Scanning merupakan scanning yang bertujuan untuk menemukan host atau komputer yang aktif pada suatu jaringan.
3. Vulnerability Scanning merupakan scanning yang bertujuan menemukan kelemahan dari suatu sistem.

Tujuan dari *scanning* antara lain:

1. Untuk mendeteksi live sistem yang berjalan di jaringan.
2. Untuk menemukan port yang aktif/running.
3. Untuk menemukan sistem operasi yang berjalan di sistem target.
4. Untuk menemukan service yang berjalan.
5. Untuk menemukan IP address sistem target.

## 2.10. CentOS

CentOS kependekan dari *Community Enterprise Operating System* adalah sistem operasi bebas yang didasarkan pada Red Hat Enterprise Linux (RHEL) yang merupakan salah satu keluarga dari Linux. (Susanto dan H, 2009). CentOS adalah Distro Linux yang cocok dipakai dalam skala *Enterprise* atau skala perusahaan yang bebas biaya atau Gratis. CentOS sendiri di *code* dari *source code Red Hat Enterprise* (RHEL) yang dikembangkan dalam sebuah komunitas yang disebut CentOS *Project*. CentOS sangat cocok dan kompatibel dengan *Red Hat*, yang merupakan sistem operasi yang sangat handal untuk perusahaan bersekala *enterprise* dan *Red Hat* merupakan sistem operasi yang didukung resmi oleh *CPanel Driver*.


**Gambar 2.4** Logo CentOS

## 2.11. OSSEC

OSSEC merupakan aplikasi HIDS yang bersifat *open source*. Aplikasi ini dapat melakukan analisis log, memeriksa integritas file, pemantauan lalu lintas jaringan, deteksi rootkit dan *active response*. (Suparsin and Mariaty, 2011). OSSEC memberikan fungsi yang sama seperti SIEM (*Security Information and Event Management*) dan STRM (*Security Threat Response Management*). Komunikasi antara keduanya menggunakan protokol UDP dengan port 1514 dan dienkripsi menggunakan algoritma symmetric key Blowfish.


**Gambar 2.5** Logo OSSEC

## 2.12. Metasploit

Metasploit adalah sebuah proyek keamanan komputer yang dapat menyediakan informasi tentang kerentanan keamanan dan membantu dalam pengujian penetrasi dan pengembangan signature IDS. Metasploit memiliki beberapa sub proyek. Metasloit merupakan software security yang sering digunakan untuk menguji coba tahanan suatu sistem dengan cara mengeksploitasi kelemahan software suatu sistem. (Vonny, 2019).

*The Metasploit Project* adalah proyek yang dikembangkan oleh Rapid7, proyek ini mengembangkan sistem yang menyediakan informasi kerentanan pada suatu kemanan komputer dan mengembangkan source code yang memungkinkan suatu jaringan masuk ke jaringan sendiri untuk mengidentifikasi resiko keamanan pada jaringan tersebut. Metasploit ini juga kadang bisa menjadi software penyerang

ke sistem komputer yang mencari kelemahan dalam keamanannya, dan agar dapat memperoleh akses ke data dan fitir-fitur dari komputer tersebut.

Beberapa jenis metasploit sebagai berikut:

a. Metasploit Framework

   Merupakan sebuah penetration tool yang cukup powerfull untuk melakukan penetrasi kedalam sebuah system. Metasploit framework bisa juga dikatakan sebagai sebuah platfrom pengembangan untuk membuat tool security dan exploit.

b. Metasploit Payload

   Payload merupakan bagian dari perangkat lunak yang memungkinkan untuk mengendalikan sistem komputer setelah sudah dieksploitasi. Payload ini biasanya melekat dan disampaikan oleh mengeksloitasi. Payload metasploit yang paling populer disebut meterpreter yang memingkinkan anada untuk melakukan segala macam hal-hal yang funky pada sistem target.

## 2.13. *Web Server* Apache

Apache adalah *Web Server* yang dapat dijalankan pada banyak sistem operasi (Unix, BSD, Linux, dan Microsoft Windows) yang berguna untuk melayani dan memfungsikan situs web. Protokol yang digunakan untuk melayani fasilitas ini adalah HTTP. (Rakhman dan Lestariningati, 2015)

Apache memiliki fitur-fitur canggih seperti pesan kesalahan yang dapat dikonfigurasi, autentikasi berbasis basis data dan lain-lain. Apache juga didukung oleh sejumlah antarmuka pengguana berbasis grafik (GUI) yang memungkinkan penanganan *server* menjadi mudah. Apache merupakan perangkat lunak sumber terbuka dikembangkan oleh komunitas terbuka yang terdiri dari pengembang-pengembang dibawah naungan *Apache Software Foundation*.


**Gambar 2.6** Logo *Apache Software Foundation*

Meskipun disebut sebagai web server, Apache tidak hadir dalam bentuk server fisik, melainkan software yang menjalankan sebuah server. Fungsinya adalah membuat koneksi antara server dan browser milik *visitor website* (Firefox, Google Chrome, Safari, dan lain-lain) sembari mengirimkan file bolak-balik (antara *client-server*). Apache merupakan *software* lintas platform, dan karena itulah *server* ini dapat berfungsi baik di *server* Unix maupun *server* Windows.

Berikut adalah kelebihan dari *web server* Apache, antara lain :

1. Open-source dan gratis, bahkan untuk tujuan komersial.
2. Software yang andal dan stabil.
3. Patch keamanan yang terus-menerus diperbarui.
4. Fleksibel karena memiliki struktur berbasis modul.
5. Kemudahan konfigurasi dan tidak sulit bagi pemula.
6. Lintas platform (dapat berfungsi baik di server Unix maupun Windows).
7. Pun dapat digunakan di situs WordPress.
8. Komunitasnya besar dan memudahkan pengguna jika menemukan masalah.

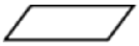
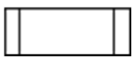
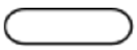
Terlebih banyak kelebihan, *web server* apache juga memiliki kekurangan, antara lain:

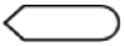
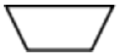
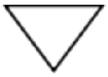
1. Terjadi gangguan pada performa jika suatu website menerima traffic dengan jumlah sangat tinggi.
2. Terlalu banyak opsi konfigurasi yang bisa mengarah ke rentannya keamanan.

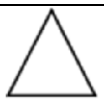
## 2.14. Flowchart

*Flowchart* merupakan sebuah diagram dengan simbol-simbol grafis yang menyatakan tipe operasi program yang berbeda. Sebagai *representasi* dari sebuah program, *flowchart* maupun algoritma dapat menjadi alat bantu untuk memudahkan perancangan alur urutan logika suatu program, memudahkan pelacakkan sumber kesalahan program, dan alat bantu untuk menerangkan logika program (Budiutomo, 2017). Simbol *Flowchart* dapat dilihat pada tabel 2.1.

**Tabel 2.1.** Simbol *Flowchart*

| No. | Simbol | Nama Simbol | Keterangan |
|---|---|---|---|
| 1. |  | *Alternate Process* | Menyatakan segala jenis operasi yang diproses dengan menggunakan mesin yang memiliki *keyboard.* |
| 2. |  | *Decision* | Suatu penyelesaian kondisi dalam program. |
| 3. |  | *Data* | Mewakili data *input* atau *output.* |
| 4. |  | *Predefined Process* | Suatu operasi yang rinciannya di tunjukkan di tempat lain. |
| 5. |  | *Document* | *Document input* dan *output* baik untuk proses manual, mekanik atau komputer. |
| 6. |  | *Terminator* | Untuk menunjukkan awal dan akhir dari suatu proses. |
| 7. |  | *Process* | Proses dari operasi program komputer. |
| 8. |  | *Manual Input* | *Input* yang menggunakan *online* keyboard. |

| | | | |
|---|---|---|---|
| 9. |  | *Conector* | Penghubung ke halaman yang masih sama . |
| 10. |  | *Off-Page Connector* | Penghubung ke halaman lain. |
| 11. |  | *Display* | *Output* yang ditampilkan di monitor. |
| 12. |  | *Delay* | Menunjukkan penundaan. |
| 13. |  | *Preparation* | Memberi nilai awal suatu besaran. |
| 14. |  | *Manual Operation* | Pekerjaan manual. |
| 15. |  | *Card* | *Input* atau *output* yang menggunakan kartu. |
| 16. |  | *Punch Tape* | *Input* atau *output* menggunakan pita kertas berlubang. |
| 17. |  | *Merge* | Penggabungan atau penyimpanan beberapa proses atau informasi sebagai salah satu. |
| 18. |  | *Dirrect Access Storage* | *Input* atau *output* menggunakan drum magnetik. |
| 19. |  | *Magnetic Disk* | *Input* atau *output* menggunakan *hard disk.* |
| 20. |  | *Sequential Access Storage* | *Input* atau *output* menggunakan pita magnetik. |
| 21. |  | *Sort* | Proses pengurutan data di luar komputer. |
| 22. |  | *Stored Data* | *Input* atau *output* menggunakan *diskette.* |

| | | | |
|---|---|---|---|
| 23. |  | *Extract* | Proses dalam jalur paralel. |
| 24. |  | *Arrow* | Menyatakan jalan atau arus suatu proses. |
| 25. |  | *Summing Junction* | Untuk berkumpul beberapa cabang sebagai proses tunggal. |
| 26. |  | *Or* | Proses menyimpang dalam dua proses. |