

BAB II

TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Sebagai tinjauan pustaka berikut beberapa referensi penelitian yang sudah di lakukan oleh para peneliti yang dapat di digunakan sebagai acuan dan pengetahuan.

Dalam penelitian yang berjudul “Analisis dan Implementasi Sistem *Monitoring* Koneksi *Internet* Menggunakan *The Dude* Di STIKOM Al Khairiyah” Bahwa dengan adanya *monitoring server* ini. mudah sekali untuk mengawasi keseluruhan jaringan di *server* jika ada *maintenance* pada jaringan tersebut bisa mengetahui dalam sistem *monitoring the dude* sehingga bisa mengetahui informasi melalui notifikasi ponsel via *E-mail*. (Sutarti & Alfiyansyah, 2017).

Penelitian yang berjudul “Aplikasi *Monitoring* Perangkat dan Aktivitas Pengguna pada Jaringan Menggunakan Protocol *SNMP* dan *Squid Proxy*”. Dengan banyaknya perangkat jaringan yang dikelola, admin akan mengalami kesulitan jika proses *monitoring* perangkat jaringan dilakukan secara manual yaitu hanya mengandalkan laporan dari *client*. Dengan digabungkannya *Protocol SNMP* dan *Squid Proxy* maka admin langsung menerima notifikasi melalui *Email* tanpa harus mengontrol manual atau lewat pengaduan *client*. (Wijayanto & Waspada, 2016).

Penelitian yang berjudul ”Aplikasi *Monitoring* Keamanan Jaringan Dengan Menggunakan *IDS* Dan *Router* Mikrotik”. bahwa Penggabungan metode *IDS* dan *IPTables* mikrotik merupakan sistem pencegahan penyusup. dirancang akan memberikan *blocking* pada alamat *IP* yang diketahui mengirimkan paket penyusup. sistem mampu memperoleh data *output* dari mikrotik serta dapat mengenali segala aktifitas yang dilakukan *intruder* dalam usaha untuk menyusup kedalam sistem dengan menggunakan *Port scanner, ssh, ftp*. (Wiyanto, Hamzah, & Sholeh, 2015).

Dalam Penelitian yang berjudul “Perancangan dan Implementasi *Network Monitoring* Sistem Menggunakan Nagios dengan *Email* dan *SMS Alert*”. membahas tentang *monitoring host* yang meliputi perancangan, implementasi dan pengujian. sehingga diperoleh beberapa kesimpulan seperti *monitoring* untuk melihat kondisi *Up* atau *Down* dari sebuah *host*. Dan sistem monitoring dapat menggunakan *Email* dan *SMS alert* untuk mempermudah admin agar mendapatkan informasi kondisi *host* dimana saja. (Amnur, Defni, Prayama, & Agustin, 2014).

2.2 Landasan Teori

2.2.1 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya (*printer, CPU*), berkomunikasi (surel, pesan instan), dan dapat mengakses informasi (peramban *web*). Tujuan dari jaringan komputer adalah agar dapat mencapai tujuannya, setiap bagian dari jaringan komputer dapat meminta dan memberikan layanan (*service*). Pihak yang meminta/menerima layanan disebut klien (*client*) dan yang memberikan/mengirim layanan disebut peladen (*server*). Desain ini disebut dengan sistem client-server, dan digunakan pada hampir seluruh aplikasi jaringan komputer. (Yudianto, 2007).

Jaringan komputer merupakan sekelompok komputer otonom yang saling berhubungan satu sama lain, dengan menggunakan satu *protocol* komunikasi sehingga seluruh komputer yang saling terhubung tersebut dapat berbagi informasi, program, sumber daya dan juga dapat saling menggunakan perangkat keras lainnya secara bersamaan, seperti *printer, harddisk* dan lain sebagainya. (Kristanto, 2003).

2.2.2 Jenis-Jenis Jaringan Komputer

2.2.2.1 Berdasarkan Luas Area

Berdasarkan kondisi geografis dan luas area yang dicakupnya, jaringan komputer terbagi menjadi 3 jenis, yaitu :

a. *Local Area Network (LAN)*

LAN merupakan kependekan dari *Local Area Network*. Dari namanya saja sudah mendeskripsikan bahwa jaringan LAN ini merupakan tipe jaringan paling sederhana dan juga paling kecil ruang lingkungnya. Biasanya jaringan LAN hanya digunakan dalam ruang lingkup kecil, seperti dalam ruangan, dalam rumah, dalam sekolah, ataupun warnet. Dengan menggunakan model jaringan LAN, maka seluruh komputer dalam satu ruangan tersebut dapat terkoneksi satu sama lain. LAN ini merupakan jaringan yang kasat mata yang hanya berjalan pada radius beberapa meter saja, oleh sebab itu jaringan ini jaringan terkecil bila di dibandingkan dengan lingkup jaringan lainnya. Meski jaringan komputer LAN ini memiliki lingkup yang kecil namun *speed* yang dimilikinya tidak kalah dengan jaringan lainnya, jaringan LAN ini cukup stabil dengan penggunaan yang standar dalam satu wilayah. Jaringan ini juga lebih memudahkan setiap pengguna dalam membagikan *file* dengan cara sharing yang lebih ringkas dan cepat. Kelebihan lainnya dari jaringan LAN adalah biaya operasional yang relatif kecil karena lebih sedikit menggunakan kabel yaitu hanya satu ruangan saja.

b. *Metropolitan Area Network (MAN)*

Metropolitan Area Network, merupakan kumpulan dari beberapa jaringan LAN yang menjadi satu, sehingga bisa tersambung dalam ruang lingkup yang lebih besar dari satu ruangan saja. Biasanya, MAN diaplikasikan untuk menghubungkan komputer melalui jaringan, pada satu kota tertentu. Namun di Indonesia, penggunaan MAN tidak berkembang dan jarang sekali digunakan. Jaringan komputer MAN ini lebih efisien untuk cakupan yang lebih luas, dengan menggunakan tipe jaringan MAN ini para pengguna akan lebih mudah mengakses data dari pengguna lainnya meski lokasi berjauhan. Jaringan ini lebih sering di gunakan oleh gedung-gedung yang memiliki keterkaitan satu sama lain, seperti gedung perkantoran. Tentunya manfaat jaringan komputer ini sangat berguna oleh beberapa instansi yang memang menggunakan jaringan MAN dalam kegiatan pekerjaan mereka. Selain lebih memudahkan

dalam pengiriman *file* dari satu tempat ke tempat lainnya, penggunaan jaringan MAN ini lebih efektif untuk di gunakan secara bersamaan.

c. *Wide Area Network* (WAN)

Wide Area Network merupakan jaringan yang jauh lebih luas ruang lingkungannya, seperti satu negara, satu benua, bahkan satu dunia. *Internet* yang biasa kita gunakan termasuk ke dalam jaringan WAN atau *Wide Area Network*, karena dapat menghubungkan komputer kita dengan jaringan seluruh dunia. Teknologi jaringan WAN ini menggunakan kabel yang terletak di dalam tanah maupun di dasar laut, dengan begitu jaringan yang tercakup lebih luas bahkan antar benua dan banyak negara. Terdapat jenis-jenis kabel jaringan komputer yang biasa di gunakan, dan kabel yang di gunakan untuk jaringan WAN ini menggunakan kabel *fiber optic* yang cukup kuat sehingga rentan akan kerusakan meski tertanam di dalam tanah maupun di lautan. Kelebihan dari jaringan ini memiliki *speed* yang cukup baik dan stabil, pertukaran informasi yang di lakukanpun lebih aman dan terarah. Karena menyangkut hubungan antar negara maka jaringan ini cukup baik di bandingkan jaringan LAN dan jaringan MAN. Namun terdapat kekurangan juga dari jaringan WAN ini, yaitu biaya operasional yang cukup tinggi sebab harus menyediakan kabel yang lebih banyak dan biaya *maintenance* untuk jaringan agar lebih aman.

2.2.2.2 Berdasarkan Media Transmisi

Berdasarkan media transisi atau komunikasinya, maka kita dapat membagi jaringan menjadi 2 jenis, yaitu:

a. Jaringan Kabel (*Wired Network*)

Jaringan komputer ini dibentuk dengan menggunakan koneksi kabel antar komputer. Biasanya, koneksi dari jaringan kabel ini menggunakan *port*, dimana kabel LAN akan dicolokkan ke dalam *port LAN Card*, untuk kemudian dihubungkan ke komputer. Penggunaan jaringan kabel ini seringkali digunakan untuk membentuk jaringan dalam skala kecil seperti warnet

ataupun dalam rumah. Contoh konkrit dari jaringan kabel adalah telepon rumah yang biasa kita gunakan sehari-hari.

b. Jaringan Tanpa Kabel (*Wireless Network*)

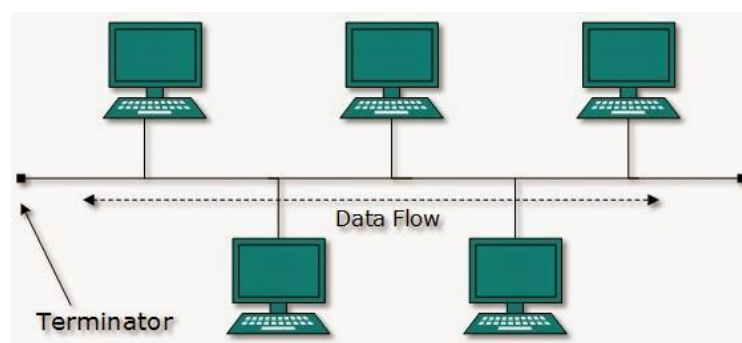
Jaringan tanpa kabel atau *wireless network* merupakan salah satu pengembangan jaringan yang saat ini sudah banyak digunakan. Jaringan *wireless* membutuhkan satu buah menara atau *tower* pengirim sinyal, dan juga penempatan *chip* penangkap sinyal pada komputer, Jaringan *wireless* ini lebih banyak di gunakan karena lebih efisien dan praktis selain itu tidak perlu mengeluarkan biaya operasional untuk kabel dalam penyambungannya ke beberapa perangkat untuk terhubung ke *internet*.

2.2.2.3 Berdasarkan Topologi

Menurut Syahfrizal (2005), Topologi jaringan merupakan hal yang menjelaskan hubungan geometris antara unsur-unsur dasar penyusun jaringan, yaitu *node*, *link*, dan *station*. Topologi jaringan dapat dibagi menjadi 6 kategori utama. Yaitu:

a. Topologi *Bus*

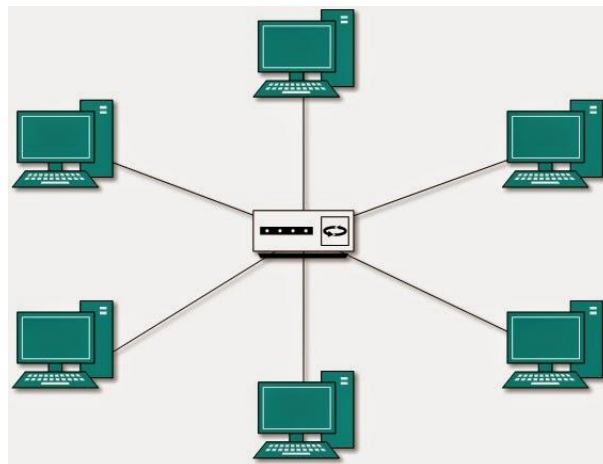
Topologi *bus* adalah jaringan yang hanya memakai satu kabel (*coaxial*) untuk media transmisi dan kabel tersebut sebagai pusat bagi seluruh *server* yang terhubung. Masing-masing komputer dihubungkan ke kabel utama dengan menggunakan konektor *Bayonet Neill–Concelman* (BNC), lalu diakhiri dengan terminator, apabila Konektor BNC sudah terhubung dengan kabel *Coaxial*. Seperti pada Gambar 2.1.



Gambar 2. 1 Topologi *Bus* (www.puruhitas.blog.uns.ac.id)

b. Topologi *Star*

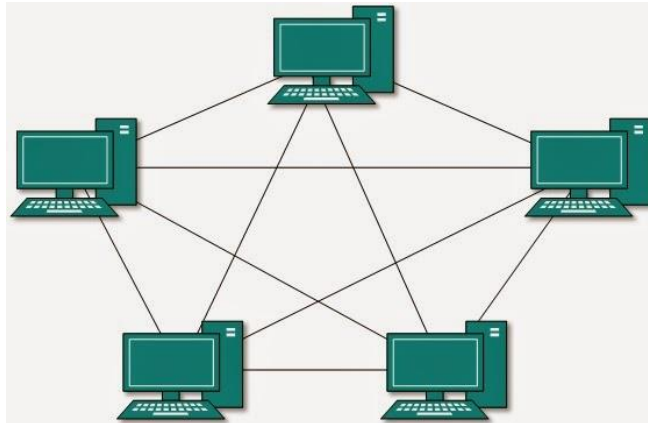
Topologi star merupakan bentuk jaringan yang mana terdapat satu penghubung (*Hub/Switch*) sebagai pusat dan setiap komputer terhubung ke penghubung tersebut. *Hub/Switch* ini posisinya ada di tengah dan berfungsi untuk menghubungkan satu komputer ke setiap komputer yang terhubung dan juga menghubungkan komputer ke *File Server*. Cara kerjanya yaitu apabila komputer berkirim data antara satu dengan yang lainnya maka data tersebut harus mengalir ke *Hub/Switch* terlebih dahulu baru kemudian menuju ke komputer yang dituju. Seperti pada Gambar 2.2.



Gambar 2. 2 Topologi *Star* (www.puruhitas.blog.uns.ac.id)

c. Topologi *Mesh*

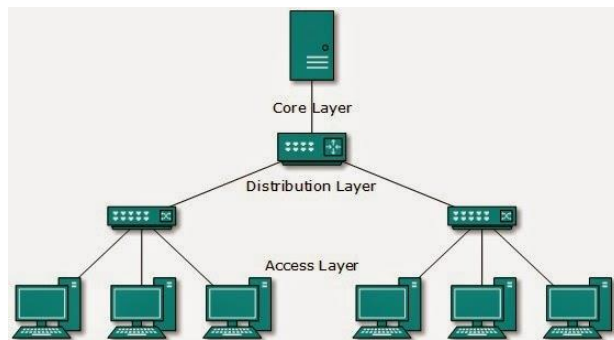
Topologi *Mesh* atau mudahnya dinamai topologi jala adalah bentuk topologi jaringan yang mana semua *Workstation* bisa terhubung satu sama lain secara acak atau tidak teratur. Karena *Workstation* langsung terhubung dengan *Workstation* yang dituju maka arus data bisa dilakukan dengan cepat tanpa harus melalui *workstation* lain. Masing-masing *Workstation* setidaknya memiliki 2 jenis sambungan yaitu pertama kabel yang terhubung dengan workstation lain dan terakhir terhubung dengan *File Server*. Topologi jaringan jala cocoknya digunakan pada jaringan komputer yang kecil bukan yang besar. Alasannya adalah selain karena sambungan antar *workstation* yang berlebihan tetapi juga sangat sulit untuk mengendalikannya. Seperti pada Gambar 2.3.



Gambar 2. 3 Topologi *Mesh* (www.puruhitas.blog.uns.ac.id)

d. Topologi *Tree*

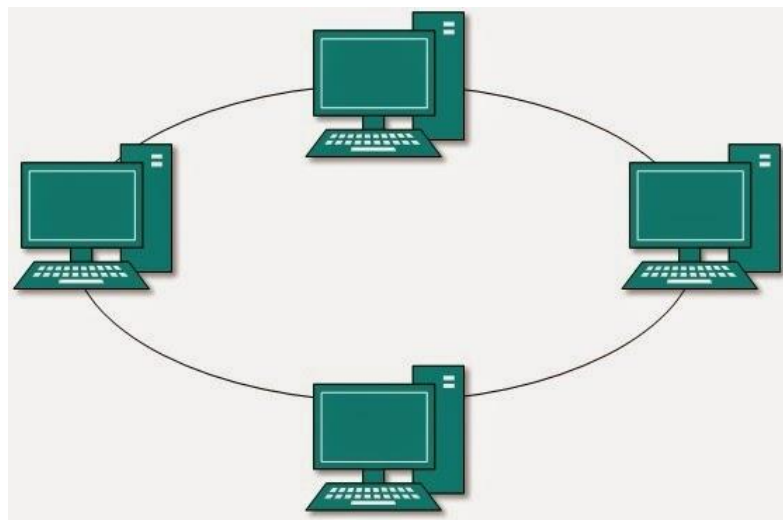
Topologi jaringan *tree* atau pohon merupakan topologi jaringan yang bertingkat dan hierarki yang mana antar koneksi menggunakan *Hub/Switch* dan masing-masing *Hub* terhubung dengan *file server*. Topologi *tree* sebenarnya adalah kombinasi dari topologi *star* dan topologi *bus* namun yang membedakannya adalah topologi *tree* ini terdapat banyak *Hub* di dalam jaringannya dan sistemnya yang hierarki. Seperti pada Gambar 2.4.



Gambar 2. 4 Topologi *Tree* (www.puruhitas.blog.uns.ac.id)

e. Topologi *Ring*

Topologi ring atau topologi cincin adalah Topologi jaringan yang rangkaianannya berupa titik yang mana masing-masing titik bagian kanan dan kirinya terhubung ke dua titik lainnya sampai ke komputer yang pertama dan akhirnya membentuk cincin atau lingkaran. Titik yang ada pada topologi cincin tersebut berfungsi memperkuat sinyal di setiap rangkaianannya atau sebagai repeater. Dengan metode ini, sinyal dan aliran data tetap akan stabil. Arah aliran datanya bisa searah jarum jam atau berlawanan dengan jarum jam, tergantung dengan kebutuhan. Seperti pada Gambar 2.5.



Gambar 2. 5 Topologi *Ring* (www.puruhitas.blog.uns.ac.id)

f. Topologi *Peer To Peer*

Topologi *peer to peer* merupakan topologi yang sangat sederhana dikarenakan hanya menggunakan 2 buah komputer untuk saling terhubung. Pada topologi ini biasanya menggunakan satu kabel yang menghubungkan antar komputer untuk proses pertukaran data. Seperti pada Gambar 2.6.



Gambar 2. 6 Topologi *Mesh* (www.puruhitas.blog.uns.ac.id)

2.2.3 Mikrotik

MikroTik RouterOS, merupakan sistem operasi berbasis Linux yang diperuntukkan sebagai router jaringan. Didesain untuk memberikan kemudahan bagi penggunaannya. Administrasinya bisa dilakukan melalui *Windows Application* (WinBox). Selain itu instalasi dapat dilakukan pada Standar komputer PC (*Personal Computer*). Seperti pada Gambar 2.7.



Gambar 2. 7 Mikrotik Routerboard (www.mikrotik.id)

PC yang akan dijadikan router mikrotik pun tidak memerlukan *resource* yang cukup besar untuk penggunaan standar, misalnya hanya sebagai *gateway*. Untuk keperluan beban yang besar (jaringan yang kompleks, *routing* yang rumit) disarankan untuk mempertimbangkan pemilihan *resource PC* yang memadai.

2.2.3.1 Fungsi Mikrotik

Router Mikrotik tak hanya dapat digunakan sebagai penghubung jaringan saja. Namun ada banyak manfaat lain yang ada di dalam *router* Mikrotik. Beberapa diantaranya adalah sebagai berikut.

a. Sebagai internet *Gateway* bagi *LAN*

Router Mikrotik juga dapat digunakan sebagai *gateway* jaringan lokal sehingga dapat menghubungkan beragam jaringan lokal tersebut yang nantinya dihubungkan ke *internet* secara lebih luas. *Router* Mikrotik nantinya akan dapat mengatur ruang gerak dan lintasan data pada jaringan *internet* yang masuk maupun yang keluar. Bahkan *router* Mikrotik juga sangat efektif berfungsi sebagai pengatur konten yang dapat atau tidak dapat diakses oleh

client. Konfigurasi *LAN* dapat dijalankan hanya dengan memanfaatkan *PC* Mikrotik *Router OS* dan dengan kebutuhan perangkat keras yang cukup rendah yang berfungsi untuk memudahkan prosesnya.

b. Sebagai *Routing*

Router Mikrotik ini mempunyai kemampuan *routing*nya yang dapat menghubungkan perangkat dengan lebih dari satu jaringan serta dapat memilih jalur yang paling optimal menuju ke perangkat komputer atau perangkat tujuan lainnya. Dengan hal inilah menjadi salah satu alasan banyak orang untuk menjadikan Mikrotik sebagai *Router* mereka.

c. Sebagai *Access Point*

Selain digunakan sebagai dalam proses *routing* yang menghasilkan kinerja maksimal, *Router* Mikrotik juga berfungsi sebagai *access point* yang handal dan mumpuni pada jaringan *Wi-Fi*. Hal ini disebabkan *Router* Mikrotik dibekali dengan *interface wireless* yang memiliki cakupan sangat luas.

2.2.3.2 Fitur- Fitur Pada Mikrotik

Berikut ini adalah beberapa fitur yang terdapat pada *Router* Mikrotik, diantaranya :

- a. *Firewall* dan *NAT*
- b. *Routing*
- c. *Data Rate Management*
- d. *Hotspot*
- e. *Point-to-point tunneling protocols*
- f. *Simple tunnels*
- g. *IPSec*
- h. *Web Proxy*
- i. *DHCP*
- j. *NTP*
- k. *SNMP*
- l. *Monitoring*

2.2.4 Wi-fi

Wi-Fi, adalah singkatan dari *wireless fidelity*, merupakan pengembangan dari istilah *Hi-Fi*, sebuah teknologi jaringan nirkabel yang digunakan di seluruh dunia. *Wi-Fi* mengacu pada sistem yang menggunakan standar 802.11, yang dikembangkan oleh *Institute of Electrical and Electronics Engineers* (IEEE) dan dirilis pada tahun 1997. Awalnya *Wi-Fi* ditujukan untuk penggunaan perangkat nirkabel dan Jaringan Area Lokal (*LAN*), namun saat ini lebih banyak digunakan untuk mengakses *internet*. Cara kerja *Wi-Fi* sama halnya dengan ponsel, jaringan *Wi-Fi* juga menggunakan gelombang radio untuk mengirimkan informasi melalui jaringan. komputer harus termasuk adaptor nirkabel yang akan menerjemahkan data yang dikirim menjadi sinyal radio. Sinyal yang sama ini akan dikirim melalui antena untuk *decoder* dikenal sebagai *router*. Setelah diterjemahkan, data akan dikirim ke *Internet* melalui koneksi Ethernet kabel.

Wi-Fi dirancang berdasarkan spesifikasi IEEE 802.11. Sekarang ini ada empat variasi dari 802.11, dapat dilihat pada Tabel 2.1. berikut.

Tabel 2. 1 Tabel Spesifikasi Wi-Fi

Spesifikasi	Kecepatan	Frekuensi Band	Seri Kompatibilitas
802.11b	11 Mb/s	2,4 GHz	B
802.11a	54 Mb/s	5 GHz	A
802.11g	54 Mb/s	2,4 GHz	b,g
802.11n	100 Mb/s	2,4 GHz	b,g,n

2.2.5 Hotspot Area

Hotspot adalah lokasi fisik dimana orang dapat mendapatkan akses Internet, biasanya menggunakan teknologi *Wi-Fi*, melalui jaringan area lokal nirkabel (WLAN) menggunakan *router* yang terhubung ke penyedia layanan *internet* (ISP).

Konsep *Hotspot* pertama kali dikemukakan tahun 1993 oleh Bret Stewart, saat konferensi *Networld* dan *Interop*, di San Fransisco. Dengan pemanfaatan

teknologi ini, setiap orang dapat mengakses jaringan *internet* melalui komputer, laptop, atau ponsel yang mereka miliki di lokasi-lokasi area bersinyal ini tersedia.

2.2.6 Internet Protocol Address (IP Address)

IP Address (*Internet Protocol Address*) merupakan deretan angka biner antara 32 bit sampai dengan 128 bit yang digunakan sebagai alamat identifikasi untuk tiap komputer *host* dalam jaringan internet. Angka 32 bit digunakan untuk alamat IP Address versi IPv4 dan angka 128 bit digunakan untuk *IP Address* versi IPv6 untuk menunjukkan alamat dari komputer pada jaringan internet berbasis *TCP/IP*.

2.2.6.1 Jenis IP Address

Berdasarkan jenis, *Internet Protocol Address* (IP Address) terbagi menjadi 2 jenis, yaitu:

1. IPv4

Internet protocol version 4 atau IPv4 adalah sebuah jenis pengalaman jaringan yang digunakan di dalam protokol jaringan TCP/IP yang menggunakan protokol IP versi 4. Panjang totalnya adalah 32-bit, dan dapat mengalami hingga 4 miliar lebih *host* komputer di seluruh dunia, jumlah *host* tersebut didapatkan dari 8 *bit* dipangkat 4 sehingga nilai maksimal dari alamat *IP* versi 4 tersebut adalah 255.255.255.255.

2. IPv6

Internet protocol version 6 atau IPv6 adalah IPv6 diciptakan untuk menjawab kekhawatiran akan kemampuan IPv4 yang hanya menggunakan 32 *bit* untuk menampung *IP Address* di seluruh dunia, semakin banyaknya pengguna jaringan *internet* dari hari ke hari di seluruh dunia IPv4 dinilai suatu saat akan mencapai batas maksimum yang dapat ditampungnya, untuk itulah IPv6 versi 128 *bit* diciptakan. Dengan kemampuannya yang jauh lebih besar dari IPv4 dinilai akan mampu menyediakan *IP Address* pada seluruh pengguna jaringan internet di seluruh dunia yang semakin hari semakin banyak.

2.2.6.2 Pembagian Kelas IP Address

IP Address dibagi menjadi beberapa kelas yaitu Kelas A, B, dan C dengan fungsi dan kegunaan masing-masing. Jarak alamat *IP address* dapat dilihat pada Tabel 2.2. dibawah ini.

Tabel 2. 2 Kelas *IP Address*

No	Default Subnet	Range	Jumlah Maksimum Network	Jumlah Max. Host
A	255.0.0.0	1-126	127	16777214
B	255.255.0.0	128-191	16384	65534
C	255.255.255.0	192-223	2097152	254

2.2.7 Keamanan Jaringan

Keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringan yang lebih banyak mempunyai ancaman keamanan dari pada komputer yang tidak terhubung ke mana – mana. Namun dengan adanya pengendalian maka resiko yang tidak diinginkan dapat dikurangi. (Purbo, 2010).

Macam-macam serangan pada jaringan komputer yaitu:

a. *Sniffer*

Sniffer adalah program yang membaca dan menganalisa setiap protokol yang melewati mesin di mana program tersebut diinstal. Secara *default*, sebuah komputer dalam jaringan (*workstation*) hanya mendengarkan dan merespon paket-paket yang dikirimkan kepada mereka. Namun demikian, kartu jaringan (*network card*) dapat diset oleh beberapa program tertentu, sehingga dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket tersebut dikirimkan. Aktifitasnya biasa disebut dengan *sniffing*. (Yusuf, 2017).

b. *Deface*

Deface adalah teknik mengganti atau menyisipkan *file* pada *server*, teknik ini dapat dilakukan karena terdapat lubang pada sistem keamanan yang

ada di dalam sebuah aplikasi. Hal ini bertujuan untuk melakukan perubahan tampilan pada *website* korban dengan tampilan yang dimiliki oleh si *defacer*. *Deface* merupakan sebuah serangan yang dilakukan untuk mengganti visual dari sebuah *website*. (Yusuf, 2017).

c. *Spoofing*

Spoofing adalah Teknik yang digunakan untuk memperoleh akses yang tidak sah ke suatu komputer atau informasi, dimana penyerang berhubungan dengan pengguna dengan berpura-pura memalsukan bahwa mereka adalah *host* yang dapat dipercaya. (Yusuf, 2017).

d. *Phising*

Phising adalah suatu metode untuk melakukan penipuan dengan mengelabui target dengan maksud untuk mencuri akun target. Istilah ini berasal dari kata *fishing* yaitu memancing korban untuk terperangkap dijebakannya. *Phising* bisa dikatakan mencuri informasi penting dengan mengambil alih akun korban untuk maksud tertentu. Hal ini bisa saja dengan maksud mencari celah untuk beberapa akun yang terhubung dengan akun yang telah didapat. (Yusuf, 2017).

e. *Scanning*

Scanning pada jaringan dilakukan seorang penyerang sebagai upaya untuk mengidentifikasi *host*, *port*, dan *service* yang tersedia pada jaringan. *Scanning* merupakan salah satu komponen *intelligence gathering* bagi seorang *attacker* untuk membuat profil di organisasi target. (Yusuf, 2017).

f. *Social Engineering*

Social engineering mengkonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Dan parahnya lagi, celah keamanan ini bersifat universal, tidak tergantung *platform*, sistem operasi, protokol, software ataupun hardware. Artinya, setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Setiap orang yang mempunyai akses kedalam sistem secara fisik adalah ancaman, bahkan jika orang tersebut tidak termasuk dalam kebijakan kemanan yang telah disusun. Seperti

metode *hacking* yang lain, *social engineering* juga memerlukan persiapan, bahkan sebagian besar pekerjaan meliputi persiapan itu sendiri. (Yusuf, 2017).

g. *Session Hijacking*

Session hijacking merupakan aksi pengambilan kendali *session* milik pengguna lain setelah sebelumnya penyerang berhasil memperoleh autentifikasi *ID session* yang biasanya tersimpan dalam *cookies*. *Session hijacking* menggunakan metode *Capture*, *Brute Forced* atau *Reverse Engineered* guna memperoleh *ID Session*, yang untuk selanjutnya pembajak memegang kendali atas *session* yang dimiliki oleh user lain tersebut selama *session* berlangsung. (Yusuf, 2017).

h. *Cross Site Scripting*

merupakan salah satu jenis serangan injeksi code. XSS dilakukan oleh penyerang dengan cara memasukkan kode *HTML* atau client *script code* lainnya ke suatu situs. Serangan ini akan seolah-olah datang dari situs tersebut. Akibat serangan ini antara lain penyerang dapat mem-bypass keamanan di sisi klien, mendapatkan informasi sensitif, atau menyimpan aplikasi berbahaya. (Yusuf, 2017).

i. *Denial Of Service*

Denial of service adalah jenis serangan yang tujuannya adalah mencegah pengguna yang sesungguhnya menikmati layanan yang diberikan server. Server sesuai namanya adalah pelayan yang harus selalu siap melayani permintaan pengguna, yang umumnya beroperasi 24 jam tanpa henti. Contohnya adalah *web server* yang bertugas melayani pengunjung *web* menyediakan informasi dalam bentuk halaman *html*. Dalam kondisi normal, pengunjung dapat meminta resource dari *web server* untuk ditampilkan dalam *browser*nya, namun bila *web server* terkena serangan DoS maka pengunjung tidak bisa menikmati layanan *web server*. (Yusuf, 2017).

2.2.8 Bot

Bot Internet, juga dikenal sebagai robot *web*, adalah aplikasi perangkat lunak yang menjalankan tugas-tugas otomatis (skrip) melalui *Internet*. Biasanya, bot melakukan tugas-tugas yang sederhana dan berulang secara struktural, dengan tingkat yang jauh lebih tinggi daripada yang mungkin untuk manusia saja. Penggunaan *bot* terbesar adalah di *web spidering* (perayap web), di mana skrip otomatis menjemput, menganalisis, dan menyimpan informasi dari *server web* berkali-kali kecepatan manusia. Lebih dari separuh dari semua lalu lintas *web*. (Dwiartara, 2015).

2.2.9 API

API adalah singkatan dari *Application Programming Interface*, dan memungkinkan *developer* untuk mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan. *API* terdiri dari berbagai elemen seperti *function*, *protocols*, dan *tools* lainnya yang memungkinkan *developers* untuk membuat aplikasi. Tujuan penggunaan *API* adalah untuk mempercepat proses *development* dengan menyediakan fungsi secara terpisah sehingga *developer* tidak perlu membuat fitur yang serupa. Penerapan *API* akan sangat terasa jika fitur yang diinginkan sudah sangat kompleks, tentu membutuhkan waktu untuk membuat yang serupa dengannya. Terdapat berbagai jenis sistem *API* yang dapat digunakan, diantaranya :

a. Sistem Operasi

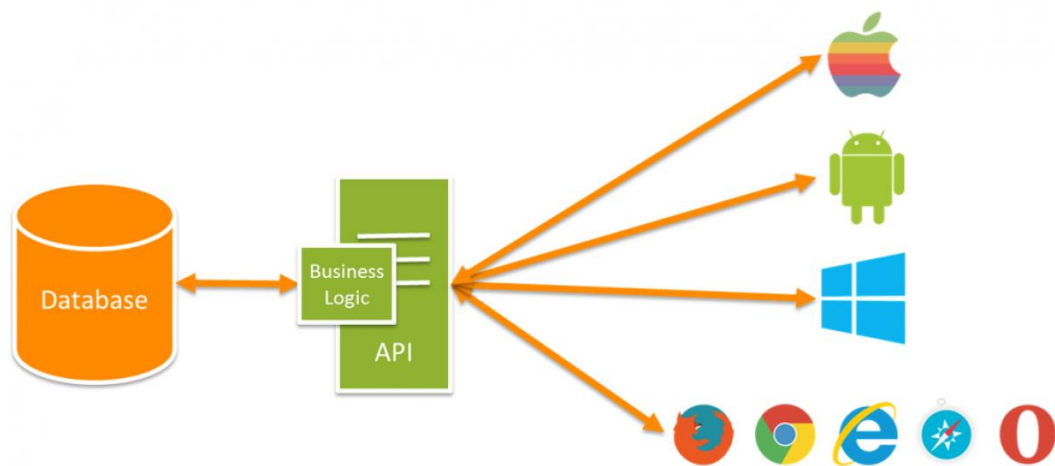
API yang bekerja pada tingkat sistem operasi membantu aplikasi berkomunikasi dengan *layer* dasar dan satu sama lain mengikuti serangkaian protokol dan spesifikasi. Contoh yang dapat menggambarkan spesifikasi tersebut adalah POSIX (*Portable Operating System Interface*). Dengan menggunakan standar POSIX, aplikasi yang di-*compile* untuk bekerja pada sistem operasi tertentu juga dapat bekerja pada sistem lain yang memiliki kriteria yang sama. *Software library* juga memiliki peran penting dalam menciptakan kecocokan antar sistem yang berbeda.

b. Library

Aplikasi yang berinteraksi dengan *library* harus mengikuti serangkaian aturan yang ditentukan oleh *API*. Pendekatan ini memudahkan *software developer* untuk membuat aplikasi yang berkomunikasi dengan berbagai *library* tanpa harus memikirkan kembali strategi yang digunakan selama semua *library* mengikut *API* yang sama. Kelebihan lain dari metode ini menunjukkan betapa mudahnya menggunakan *library* yang sama dengan bahasa pemrograman yang berbeda.

c. Web

Web API diakses melalui protokol *HTTP*, Kita bisa membuat *Web API* dengan menggunakan teknologi yang berbeda dan dengan menggunakan bahasa pemrograman yang berbeda seperti PHP, Java, dan lain sebagainya. Misalnya *Rest API* dari *Twitter* menyediakan akses baca dan tulis data dengan mengintegrasikan *Twitter* kedalam aplikasi kita sendiri. Dan *API* dari *Telegram* salah satunya digunakan untuk membuat *BOT*. Seperti pada Gambar 2.8.



Gambar 2. 8 Ilustrasi API (www.codepolitan.com)

2.2.10 Token API

Token API adalah sebuah pengenal unik atau kode unik untuk meminta akses ke suatu layanan. Layanan akan menghasilkan *Token API* untuk aplikasi yang mana kegunaannya adalah untuk meminta layanan. kode unik dihasilkan dari

kombinasi perangkat keras dan data alamat *IP*, dan waktu lain yang dihasilkan secara acak oleh server. *Token API* digunakan untuk autentikasi untuk pengguna.

2.2.11 Media Sosial

Media sosial adalah sebuah media *online*, dengan para penggunanya bisa dengan mudah berpartisipasi, berbagi, dan menciptakan isi meliputi blog, jejaring sosial, forum maupun dunia *virtual*. Blog, jejaring sosial dan wiki merupakan bentuk media sosial yang paling umum digunakan oleh masyarakat di seluruh dunia. Pendapat lain mengatakan bahwa media sosial adalah media online yang mendukung interaksi sosial dan media sosial menggunakan teknologi berbasis *web* yang mengubah komunikasi menjadi dialog interaktif. Seperti terlihat pada Gambar 2.9.



Gambar 2. 9 Media Sosial (www.google.com)

2.2.12 Telegram

Telegram adalah sebuah aplikasi layanan pengirim pesan instan multiplatform berbasis awan yang bersifat gratis. Klien Telegram tersedia untuk perangkat telepon seluler (*Android, iOS, Windows Phone, Ubuntu Touch*) dan sistem perangkat komputer (*Windows, OS X, Linux*) Para pengguna dapat mengirim pesan dan bertukar foto, *video*, stiker, *audio*, dan semua tipe *file* atau berkas. Telegram juga menyediakan pengiriman pesan ujung ke ujung terenkripsi opsional.



Gambar 2. 10 Logo *Telegram* (www.telegram.org)

2.2.13 OSI (*Open System Interconnection*)

OSI adalah sebuah model arsitektural jaringan yang dikembangkan oleh badan *International Organization for Standardization* (ISO) di Eropa pada tahun 1977. OSI sendiri merupakan singkatan dari *Open System Interconnection*. Model ini disebut juga dengan model Model tujuh lapis OSI. Tabel *layer* pada OSI dapat dilihat pada Tabel 2.3 berikut :

Tabel 2. 3 *Layer* OSI

No. Layer	Nama Lapisan	Keterangan
1	<i>Physical Layer</i>	<i>Physical layer</i> adalah layer pertama pada OSI layer ini, dan <i>physical layer</i> berhubungan dengan fisik karena sesuai dengan namanya yaitu <i>physical</i> dan berhubungan erat dengan fungsi sebuah sinyal dan <i>physical</i> ini merupakan layer yang paling dekat dengan <i>hardware</i>
2	<i>Data Link Layer</i>	<i>Data link layer</i> ini adalah salah satu <i>layer</i> yang sangat berperan penting karena mempunyai fungsi untuk mengkoreksi kesalahan pada tiap <i>layer</i> yang kita buat

No. Layer	Nama Lapisan	Keterangan
3	<i>Network Layer</i>	<i>Network layer</i> adalah <i>layer</i> yang mempunyai peran untuk membantu meendefinisikan suatu alamat <i>IP</i> atau suatu <i>internet protocol</i> , sehingga setiap komputer dapat saling berhubungan satu sama lain dengan satu jaringan
4	<i>Transport Layer</i>	<i>Transport layer</i> adalah <i>layer</i> yang berperan atau bertugas sebagai pengantar suatu data yang dikirimkan dari satu komputer ke komputer lain, dan <i>transport layer</i> ini memudahkan setiap data yang saling berjalan dari <i>server</i> menuju <i>client</i> tanpa ada gangguan sedikitpun.
5	<i>Session Layer</i>	<i>Session layer</i> adalah <i>layer</i> yang berperan utama untuk meendefinisikan bagaimana sebuah jaringan dapat dibuat atau dibangun, dan juga dapat berperan sebagai <i>management</i> dari sebuah koneksi sehingga dapat untuk menghancurkan atau menjaga sebuah koneksi.
6	<i>Prestation Layer</i>	<i>Prestation layer</i> adalah <i>layer</i> yang memiliki peran sebagai translate atau penterjemah suatu data yang akan ditransmisikan dari sebuah aplikasi atau untuk sebuah aplikasi.
7	<i>Application Layer</i>	<i>Application layer</i> adalah <i>layer</i> yang memiliki peran pertama pada saat data mulai ditransfer dari satu komputer ke komputer lain, dan juga merupakan lapisan akhir yang dilewati pada saat penerimaan data dari komputer <i>client</i> .