# BAB 2

# Tinjauan Pustaka

## 2.1 Landasan Teori

### 2.1.1 Jaringan Komputer

Menurut Abdul Kadir (2003:348) "Jaringan komputer adalah hubungan dua buah simpul (umumnya berupa komputer) atau lebih yang tujuan utamanya adalah untuk melakukan pertukaran data". Berbagi sumber daya (printer, CPU), berkomunikasi (pesan instan), dan dapat mengakses informasi (peramban web).

Menurut Melwin Syafrizal (2005:241) "Jaringan komputer adalah himpunan interkoneksi antara 2(dua) komputer *autonomous* atau lebih yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). Bila sebuah komputer dapat membuat komputer lainnya *restart*, *shutdown*, atau melakukan kontrol lainnya, maka komputer-komputer tersebut bukan *autonomous* (tidak melakukan terhadap komputer lain dengan akses penuh). 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. Jaringan komputer dapat dikatakan sebagai sebuah sistem yang terdiri dari berbagai komputer beserta *resource*-nya yang didesain agar dapat menggunakan sumber daya yang ada, sehingga dapat mengakses informasi yang diperlukan. Tujuan dibangunnya suatu jaringan komputer adalah untuk mengirim data atau informasi dari pengirim kepada penerima secara cepat dan akurat.

Jaringan komputer dibagi atas lima jenis, yaitu : (Supriyadi & Gartina, 2007)

1. *Local Area Network* (LAN), merupakan jaringan internal di dalam sebuah gedung atau kampus. LAN seringkali digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor suatu organisasi, perusahaan atau pabrik-pabrik untuk memakai bersama sumberdaya (misalnya printer, media penyimpanan/storage) dan saling bertukar informasi.

2. *Metropolitan Area Network* (MAN), merupakan versi LAN yang dengan area yang lebih luas dan biasanya menggunakan teknologi yang sama dengan LAN. MAN dapat mencakup kantor-kantor perusahaan yang letaknya berdekatan atau juga sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum. MAN mampu menunjang data dan suara, bahkan dapat berhubungan dengan jaringan televisi kabel.
3. *Wide Area Network* (WAN), jangkauannya mencakup daerah geografis yang luas, seringkali mencakup sebuah negara bahkan benua. WAN terdiri dari kumpulan mesin-mesin yang bertujuan untuk menjalankan program-program (aplikasi) pemakai.
4. *Internet*. Orang yang terhubung ke jaringan sering berharap untuk bisa berkomunikasi dengan orang lain yang terhubung ke jaringan lainnya. Keinginan seperti ini memerlukan hubungan antar jaringan yang seringkali tidak kompatibel dan berbeda. Kumpulan jaringan yang saling terhubung (terinterkoneksi) inilah yang disebut dengan internet.
5. *Jaringan Tanpa Kabel*, atau lebih dikenal dengan wireless merupakan suatu solusi terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Jaringan

Local Area Network (LAN) merupakan jaringan milik pribadi di dalam sebuah gedung atau kampus yang berukuran sampai beberapa kilometer dengan tujuan memakai bersama sumberdaya dan saling bertukar informasi. LAN diciptakan untuk menghemat biaya dalam penggunaan alat secara bersama-sama, tetapi lama kelamaan fungsinya makin bertambah. Sebuah saluran komunikasi dapat digunakan secara bersama oleh banyak komputer yang terhubung satu dengan yang lain. Penggunaan bersama saluran komunikasi menjadi kunci utama dalam pengefisienan jaringan komputer menjadi sebuah jaringan yang sangat besar seperti Internet.


Gambar 2. 1 Contoh Jaringan Komputer

Berdasarkan jenis jaringannya, teknologi LAN dapat dibedakan menjadi tiga karakteristik yakni: ukuran, teknologi transmisi, dan topologinya. LAN mempunyai ukuran yang terbatas, yang berarti waktu transmisi dalam keadaan terburuknya terbatas dan dapat diketahui sebelumnya. LAN seringkali menggunakan teknologi transmisi kabel. LAN tradisional beroperasi pada kecepatan 10 sampai dengan 100 Mbps dan mempunyai faktor kesalahan yang kecil. LAN modern dapat beroperasi pada kecepatan yang lebih tinggi, sampai ratusan megabit/detik.

*Transmission Control Protocol/Internet Protocol* (TCP/IP) merupakan protokol untuk mengirim data antar komputer pada jaringan. Protokol ini merupakan protokol yang digunakan untuk akses Internet dan digunakan untuk komunikasi global. TCP/IP terdiri atas dua protokol yang terpisah. TCP/IP terdiri dari lima layer, yaitu : (Muslim, 2007)

a. *Layer Application*, di dalam layer ini aplikasi seperti FTP, Telnet, SMTP, dan NFS dilaksanakan.
b. *Layer Transport*, di dalam layer ini TCP dan UDP menambahkan data transport ke paket dan melewatkannya ke layer Internet.
c. *Layer Internet*, layer ini mengambil paket dari layer transport dan menambahkan informasi alamat sebelum mengirimkannya ke layer *network interface*.
d. *Layer Network Interface*, di dalam layer ini data dikirim ke layer physical melalui device jaringan.
e. *Layer Physical*, layer ini merupakan sistem kabel yang digunakan untuk proses mengirim dan menerima data.

TCP/IP dikirimkan ke setiap jaringan lokal sebagai subnet yang masing-masing subnet telah diberi alamat. IP yang menggunakan pengalamatan disebut dengan IP Address. IP Address ini digunakan untuk mengidentifikasi subnet dan hOSt secara logik di dalam TCP/IP. (Riadi, 2011)

IP Address terdiri dari 2 bagian yaitu : (Supriyadi & Gartina, 2007)

1) Network Id (Identitas Jaringan)
2) HOSt Id (Identitas Komputer)

Prosesan IP Address terbagi atas 4 angka, yang masing-masing mempunyai nilai maksimum 255 (maksimum dari 8 bit) : IP Address : 255.255.255.255.

Karena setiap angka mempresentasikan 8 bit, maka jumlah total IP Address adalah 32 bit ditulis sebagai berikut :

00000000 00000000 00000000 00000000

11111111 11111111 11111111 11111111

IP Address dirancang untuk mempunyai class yang didefinisikan dalam Tabel 2.1 berikut :

Tabel 2. 1 Class IP Address

| Class | Antara | Jumlah Jaringan | Jumlah HOSt per Jaringan |
|---|---|---|---|
| A | 1-126 | 126 | 16.777.214 |
| B | 128-191 | 16.384 | 65.536 |
| C | 192-223 | 2.097.152 | 254 |

Dengan demikian, untuk menentukan Class A, B atau C cukup dilihat dari angka 8 bit pertama :

97.123.7.12 → Class A

134.23.28.14 → Class B

202.159.1.168 → Class C

### 2.1.2 Router

Router adalah peralatan yang bekerja pada layer 3 OSI dan sering digunakan menyambungkan jaringan luas (Wide Area Networking-WAN) atau untuk melakukan segmentasi layer 3 di LAN. WAN seperti halnya dengan LAN juga beroperasi di layer 1, 2 dan 3 OSI, sehingga router yang digunakan untuk menyambungkan LAN dan WAN harus mampu saling mendukung. Pada layer ini juga sudah dikenal pengalamatan jaringan menggunakan IP Address, serta router ini juga berperan penting sebagai penghubung atau penerus paket data antara dua segmen jaringan/lebih.

Selain itu Router juga bisa digunakan untuk menyediakan koneksi ke banyak jaringan kecil pada jaringan yang memiliki ukuran lebih besar, jaringan ini disebut *internetwork*. Bisa juga berarti perangkat yang bisa membagi jaringan besar menjadi beberapa *subnetwork* untuk memperbaiki dan menyederhanakan sistem jaringan. Terkadang perangkat pemiliknya juga digunakan untuk menghubungkan 2 buah jaringan dengan menggunakan media yang berbeda

seperti *Ethernet to Token Ring*. Secara umum, perangkat router ini dikategorikan menjadi dua jenis, yaitu *router statis* dan *dynamic routers.*

Menurut Kurniawan (2007:54) router adalah "perangkat yang dapat digunakan untuk menghubungkan dua jaringan lokal yang mempunyai protokol sama pada lapisan jaringan OSI". Kegunaan alat ini untuk melewatkan paket IP dari suatu host ke host lain yang berbeda. Lebih jelasnya alat untuk menyelaraskan IP yang berbeda jaringan sehingga dapat berkomunikasi dengan yang lainnya. Dapat digunakan untuk membentuk sebuah internetwork, dengan menggunakan router sebuah jaringan yang besar yang memiliki jumlah host yang sangat banyak dapat dipecah menjadi dua atau lebih jaringan. Dengan memecah jaringan yang lebih kecil, lalu lintas data dapat diatur dengan baik sehingga kinerja jaringan meningkat.

Router merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru secara virtual. Hampir sama seperti aplikasi VMware atau VirtualPC pada Windows. Router bisa kita gunakan untuk menjalankan Operating System didalam OS MikroTik yang sedang berjalan. Dengan menggunakan Router, client seolah - olah memiliki router sendiri. Dan kita sebagai admin, kita tetap bisa memanagement router fisik. Sebelum membagun sebuah virtual machine, kita perlu tentukan terlebih dahulu besar RAM dan Hardisk yang akan dialokasikan untuk virtual router. Dengan Operating System MikroTik, minimal RAM yang disarankan adalah 24 MB. Untuk ukuran Hardisk bisa disesuaikan dengan kebutuhan. Jika parameter tadi sudah ditentukan maka saatnya kita jalankan virtualisasi di router MikroTik dengan fitur Router. Router adalah yang paling mudah digunakan, meskipun hanya bisa menjalankan virtualisasi topologi jaringan, RouterOS dan OpenWRT.

Jenis Tipe Router berdasarkan mekanisme, yaitu :

**a. Router Statis**

Router statis atau router statis adalah router yang memiliki tabel routing statis dengan pengaturan manual di sisi administrator jaringan.

Kelebihan menggunakan Router Statis :

Kelebihan penggunaan router statis adalah adanya administrator, dimana administrator bisa memilih router yang bisa dilalui dan tidak bisa dilewati. Hal ini membuat proses routing dieksekusi oleh administrator. Proses perutean bisa

dilakukan dengan cepat dan mudah, maka bisa dilakukan kapan saja, tanpa kondisi tertentu. Menggunakan tabel routing pada *router statis* membuat administrator mudah dalam perutean. Pengguna atau pengguna dapat meminta atau meminta akses ke perutean dari administrator, sehingga tidak bergantung pada proses perutean.

Kekurangan menggunakan Router Statis :

Administrator harus memahami sistem dan juga perintah/perintah terhadap tabel routing harus menjadi pakar jaringan yang sudah memiliki banyak pengalaman di bidang routing sehingga static routing bisa bekerja maksimal. Kemampuan administrator untuk membuat tabel routing baru diperlukan, terutama bila harus menghapus atau menambahkan jalur routing. Tidak ada dukungan dalam jaringan yang sibuk, luas dan banyak digunakan oleh pengguna.

**b. Router Dinamis**

Router dinamis atau router dinamis adalah router yang memiliki tabel routing dinamis yang dilakukan dengan membaca lalu lintas jaringan dan dapat saling berhubungan dengan beberapa router lainnya.

Kelebihan Router Dinamis :

- Hanya mengenalkan alamat network yang terhubung langsung dengan routernya
- Tidak perlu mengetahui semua alamat network yang ada
- Bila terjadi penambahan suatu network baru tidak perlu semua router mengkonfigurasi.

Kekurangan Routing Dinamis :

- Beban kerja router lebih berat karena selalu memperbarui ip table pada tiap waktu tertentu
- Kecepatan pengenalan network terbilang lama karena router membroadcast ke semua router hingga ada yang cocok
- Setelah konfigurasi harus menunggu beberapa saat agar setiap router mendapat semua Alamat IP yang ada
- Susah melacak permasalahan pada suatu topologi jaringan lingkup besar

**c. Router Nirkabel**

Router Wireless tidak berjalan berdasarkan router statis atau router dinamis. Router nirkabel berjalan tanpa kabel dan bergantung pada koneksi nirkabel yang menggunakan antena udara. Penerapan wireless router di zaman modern sangat banyak karena memberikan kemudahan penggunaan.

Kelebihan menggunakan Wireless Router :

Ini bisa berjalan sangat baik seperti router statis dan juga router dinamis tidak memerlukan kabel, jadi instalasi mudah. Bisa dibuat Access Point, sehingga lebih mudah terhubung dengan laptop, notebook, smartphone dan perangkat komputer atau perangkat lain yang memiliki fitur wifi. Bisa dipasang dimana saja

Cukup 1 modem untuk beberapa pengguna komputer.

Terlepas dari mekanismenya, jenis router terbagi menjadi 3 lapisan lainnya, berdasarkan aplikasinya, yaitu :

**a. PC Router**

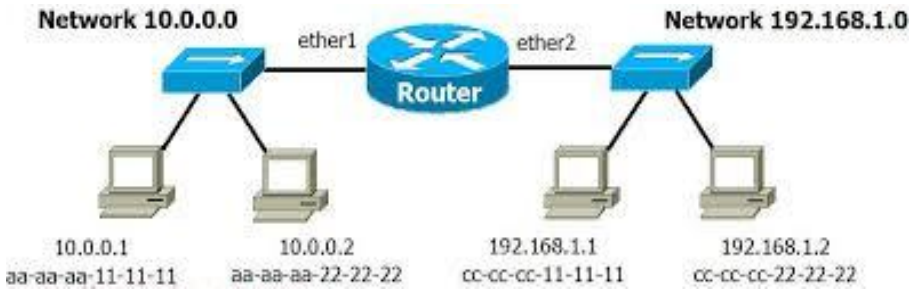
Router PC adalah Sistem Operasi yang memiliki fasilitas share yang bisa membagi IP Address. Router PC adalah sejenis router yang berasal dari komputer tempat komputer dibuat sedemikian rupa sehingga bisa berfungsi sebagai router. Dalam pembuatannya, komputer tidak harus memiliki spesifikasi yang tinggi. Spesifikasi komputer minimum untuk router PC ini adalah pentium II dengan harddisk 10 GB dan 64 RAM. Spesifikasi seperti ini sudah bisa digunakan sebagai router melalui proses instalasi sistem operasi khusus. Jenis router PC ini sering digunakan pada operasi MikroTik.

**b. Router Hardware**

Hardware Router adalah sistem perangkat yang bisa digunakan serta menggunakan router asli, dimana hardware atau hardware sedang melakukan hal yang sama seperti router seperti *sharing, transmitting,* dan sharing IP Address.

**c. Router Aplikasi**

Application Router adalah jenis jenis router yang terdapat pada aplikasi yang bisa dipasang di Sistem Operasi sehingga Sistem Operasi akan memiliki kemampuan seperti router, termasuk SpyGate WinProxy, WinRoute, dan WinGate.




Gambar 2. 2 Jaringan Router

Pada gambar 2.2 terdapat dua buah network yang terhubung dengan sebuah router. Network sebelah kiri yang terhubung ke ether1 router mempunyai alamat network 10.0.0.0 dan network sebelah kanan terhubung ke ether2 dari router dengan network address 192.168.1.0. Komputer dengan IP 10.0.0.1 mengirim data ke komputer IP 10.0.0.1, maka router tidak akan meneruskan data tersebut ke network lain. Begitu pula ketika komputer dengan IP 192.168.1.1 mengirim data ke komputer IP 192.168.1.2, router tidak akan meneruskan paket data ke network lain. Barulah ketika komputer dengan IP 192.168.1.0 mengirimkan data ke komputer IP 10.0.0.2, maka router akan menruskan paket data tersebut ke komputer dengan IP 10.0.0.2.

MikroTik adalah sistem operasi komputer dan perangkat lunak komputer yang digunakan untuk menjadikan komputer biasa menjadi router, MikroTik dibedakan menjadi dua yaitu operation sistem MikroTik bisa dikenakan MikroTik OS dan MikroTik board, untuk MikroTik board tidak memerlukan komputer dalam menjalankannya cukup menggunakan board yang sudah include dengan MikroTik OS. MikroTik OS mencakup fitur yang dibuat khusus untuk ip network dan jaringan wireless. Sistem operasi MikroTik, adalah sistem operasi Linux base yang digunakan sebagai network router. dibuat untuk memberikan kemudahan dan kebebasan bagi penggunanya. Pengaturan Administrasinya dapat dilakukan menggunakan Windows Application (WinBox).

### 2.1.3 Miktorik RouterOS

MikroTik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless, cocok digunakan oleh ISP dan provider hostspot. MikroTik RouterOS dapat digunakan menggunakan peralatan *embedded* (minimum sistem) maupun menggunakan PC (personal komputer) serta kompatibel dengan IBM PC X86. MikroTik RouterOS

dapat berfungsi sebagai access konsentrator dengan berbagai pilihan protokol. (Muslim, 2007)

MikroTik RouterOS mampu menggunakan protokol tunneling seperti IP security (IPsec), Point-To-Point Tunneling Protocol (PPTP), Layer 2 Forwarding Protocol (L2TP) dan Point-to-point over Ethernet (Ppoe). MikroTik juga mampu melakukan access ke data Microsoft Active Directory dengan menggunakan Microsoft Windows yaitu Internet Autentication Service. MikroTik RouterOS adalah sistem operasi perangkat keras MikroTik Routerboard.

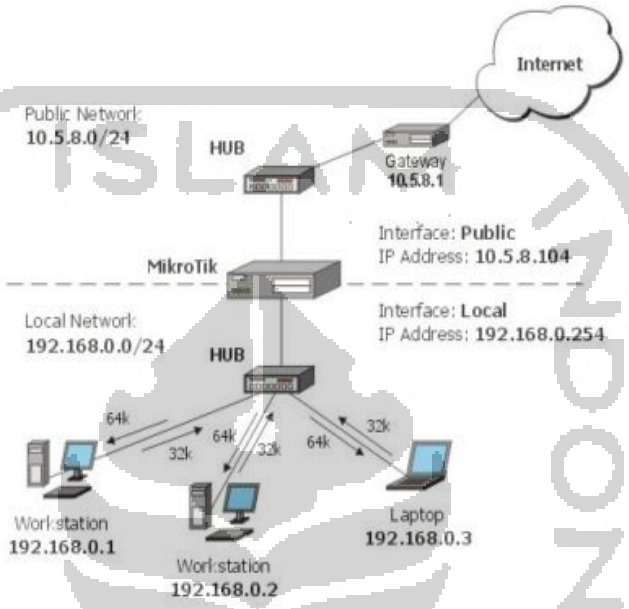
Fitur-fitur Mikrotik RouterOS, diantaranya : (Doni, Studi, & Informatika, 2014)

a. Address List : Pengelompokan IP Address berdasarkan nama.
b. DHCP (Dynamic Host Configuration Protocol), Mendukung DHCP tiap antarmuka, diantaranya :
    a. DHCP Relay
    b. DHCP Client
    c. Multiple network DHCP
    d. static and dynamic DHCP leases.
c. Firewall dan NAT (Network Address Translation): Mendukung proses filtering koneksi peer to peer, source NAT dan destination NAT. Mampu melakukan proses filtering berdasarkan MAC address (Media Access Control Address), IP address, range port, protokol IP, pemilihan opsi protokol seperti ICMP (Internet Control Message Protocol), TCP Flags dan MSS.
d. Hotspot : Hotspot gateway dengan otentikasi RADIUS. Mendukung limit data rate, SSL, HTTPS.
e. Proxy : memiliki fitur Cache untuk FTP dan HTTP proxy server, HTTPS proxy meliputi transparent proxy, untuk DNS dan HTTP mendukung protokol SOCKS, mendukung parent proxy, dan static DNS.
f. Tool : Ping, Traceroute, bandwidth test, ping flood, telnet, SSH, packet sniffer, Dinamik DNS update.
g. WinBox : Aplikasi mode GUI untuk meremote dan mengkonfigurasi MikroTik RouterOS.

MikroTik adalah salah satu vendor baik hardware dan software yang menyediakan fasilitas untuk membuat router. Salah satunya adalah MikroTik

Router OS, ini adalah Operating system yang khusus digunakan untuk membuat sebuah router dengan cara menginstallnya ke komputer. Fasilitas atau tools yang disediakan dalam MikroTik Router Os sangat lengkap untuk membangun sebuah router yang handal dan stabil. (Feby Puspitasari, 2007)

Adapun cara kerja MikroTik diasumsikan pada Gambar 2.3 berikut :




Gambar 2. 3 Cara Kerja MikroTik

Keunggulan Mikrotik RouterOS : (Doni et al., 2014)

1. Membuat PC yang murah menjadi sebuah router yang handal dan memiliki banyak fitur
2. Memiliki user interface yang mudah dan konsisten dan update versi software secara berkala dan konsisten
3. Instalasi yang mudah dan cepat dan banyak alternatif interface yang dapat digunakan
4. Ada banyak cara untuk mengontrol dan mengakses sistem, contohnya bisa melalui web browser, telnet, dan SSH.

## 2.2 Malware

*Malware* (*malicious software)*, yang berarti perangkat lunak yang mencurigakan adalah program komputer yang diciptakan dengan maksud dan tujuan tertentu dari penciptanya dan merupakan program yang mencari kelemahan dari software. Umumnya *malware* diciptakan untuk membobol atau merusak suatu *software* atau sistem operasi melalui *script* yang disisipkan secara

tersembunyi oleh pembuatnya. *Malware* merupakan program yang dirancang untuk disusupkan kedalam sebuah sistem dengan tujuan untuk melakukan beraneka ragam aktivitas yang bersifat merugikan pemiliknya. Merugikan dalam arti kata dampak negatif yang ditimbulkan dapat berkisar mulai dari sekedar memperlambat kinerja sistem hingga merusak bahkan menghancurkan data penting yang tersimpan dalam sistem dimaksud. Berikut ini berbagai jenis *malware* yang dinilai paling dominan menginfeksi komputer : (Adenansi & Novarina, 2017)

***a. Virus***

Sejak kemunculannya pertama kali pada pertengahan tahun 1980-an, virus komputer telah mengundang berbagai kontroversi akibat aksinya yang beraneka ragam. Seiring dengan perkembangan teknologi komputer, virus menemukan berbagai cara-cara baru untuk menyebarkan dirinya melalui berbagai modus operandi. Pada dasarnya, virus merupakan program komputer yang bersifat "*malicious*" (memiliki tujuan merugikan maupun bersifat mengganggu pengguna sistem) yang dapat menginfeksi satu atau lebih sistem komputer melalui berbagai cara penularan yang dipicu oleh otorasisasi atau keterlibatan "*user*" sebagai pengguna komputer. Fenomena yang mulai ditemukan pada awal tahun 1980-an ini memiliki beribu-ribu macam atau jenis sejalan dengan perkembangan teknologi komputer dewasa ini, terutama setelah dikembangkannya teknologi jaringan dan internet. Jenis kerusakan yang ditimbulkan virus pun menjadi bermacam-macam. Mulai dari yang sekedar mengganggu seperti menampilkan gambar-gambar yang tidak sepantasnya, hingga sampai yang bersifat mendatangkan kerugian ekonomis seperti memformat hard disk atau bahkan merusak file-file sistem operasi sehingga mengganggu komputer yang bersangkutan. Ditinjau dari cara kerjanya, virus dapat dikelompokkan menjadi :

1. *Overwriting Virus* merupakan penggalan program yang dibuat sedemikian rupa untuk menggantikan program utama (baca: host) dari sebuah program besar sehingga menjalankan perintah yang tidak semestinya;
2. *Prepending Virus* merupakan tambahan program yang disisipkan pada bagian awal dari program utama atau "host" sehingga pada saat dieksekusi,

program virus akan dijalankan terlebih (bereplikasi) dahulu sebelum program yang sebenarnya;

3. *Appending Virus* merupakan program tambahan yang disisipkan pada bagian akhir dari program host sehingga akan dijalankan setelah program sebenarnya tereksekusi;
4. *File Infector Virus* merupakan penggalan program yang mampu memiliki kemampuan untuk melekatkan diri (baca: attached) pada sebuah file lain, yang biasanya merupakan file "executable", sehingga sistem yang menjalankan file tersebut akan langsung terinfeksi;
5. *Boot Sector Virus* merupakan program yang bekerja memodifikasi program yang berada di dalam boot sector pada cakram penyimpan (baca: disc) atau disket yang telah diformat. Pada umumnya, sebuah boot sector virus akan terlebih dahulu mengeksekusi dirinya sendiri sebelum proses "boot-up" pada komputer terjadi, sehingga seluruh "floppy disk" yang digunakan pada komputer tersebut akan terjangkiti pula (perhatikan bahwa dewasa ini, modus operandi sejenis terjadi dengan memanfaatkan media penyimpan USB);
6. *Multipartite Virus* merupakan kombinasi dari Infector Virus dan Boot Sector Virus dalam arti kata ketika sebuah file yang terinfeksi oleh virus jenis ini dieksekusi, maka virus akan menjangkiti boot sector dari hard disk atau partition sector dari komputer tersebut, dan sebaliknya; dan
7. *Macro Virus* menjangkiti program "macro" dari sebuah file data atau dokumen (yang biasanya digunakan untuk "global setting" seperti pada template Microsoft Word) sehingga dokumen berikutnya yang diedit oleh program aplikasi tersebut akan terinfeksi pula oleh penggalan program macro yang telah terinfeksi sebelumnya.

Perlu diperhatikan bahwa virus hanya akan aktif menjangkiti atau menginfeksi sistem komputer lain apabila ada campur tangan manusia atau "user" sebagai pengguna. Campur tangan yang dimaksud misalnya dilakukan melalui: penekanan tombol pada keyboard, penekanan tombol pada mouse, "pemasukan" USB pada komputer, pengiriman file via email, dan lain sebagainya. Virus merupakan program komputer yang bersifat mengganggu dan merugikan pengguna komputer. Virus adalah *malware* pertama yang

dikenalkan sebagai program yang memiliki kemampuan untuk mengganggu kinerja sistem komputer. Hingga saat ini biasanya masyarakat lebih populer dengan kata virus komputer dibandingkan dengan istilah *malware* sendiri. Biasanya virus berbentuk file eksekusi (executable) yang baru akan beraktivitas bila user mengaktifkannya. Setelah diaktifkan virus akan menyerang file yang juga bertipe executable (.exe) atau juga tipe file lainnya sesuai dengan perintah yang dituliskan pembuatnya.

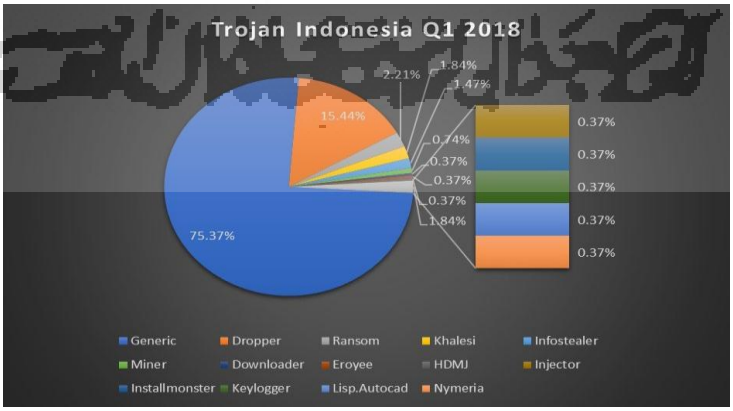
***b. Worm***

Istilah "*worm*" yang tepatnya diperkenalkan kurang lebih setahun setelah "virus" merupakan program *malicious* yang dirancang terutama untuk menginfeksi komputer- komputer yang berada dalam sebuah sistem jaringan. *Worm* yang berarti cacing merupakan *malware* yang cukup berbahaya. *Worm* mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Walaupun sama-sama sebagai sebuah penggalan program, perbedaan prinsip yang membedakan worm dengan pendahulunya virus yaitu yang bersangkutan tidak memerlukan campur tangan manusia atau pengguna dalam melakukan penularan atau penyebarannya. Worm merupakan program yang dibangun dengan algoritma tertentu sehingga yang bersangkutan mampu untuk mereplikasikan dirinya sendiri pada sebuah jaringan komputer tanpa melalui intervensi atau bantuan maupun keterlibatan pengguna. Pada mulanya worm diciptakan dengan tujuan tunggal yaitu untuk mematikan sebuah sistem atau jaringan komputer. Namun belakangan ini telah tercipta worm yang mampu menimbulkan kerusakan luar biasa pada sebuah sistem maupun jaringan komputer, seperti merusak file-file penting dalam sistem operasi, menghapus data pada hard disk, memacetkan aktivitas komputer (baca: hang), dan hal-hal destruktif lainnya.

Karena karakteristiknya yang tidak melibatkan manusia, maka jika sudah menyebar sangat sulit untuk mengontrol atau mengendalikannya. Usaha penanganan yang salah justru akan membuat pergerakan worms menjadi semakin liar tak terkendali dan "mewabah". Untuk itulah dipergunakan penanganan khusus dalam menghadapinya.

### c. *Trojan Horse*

Istilah "*Trojan Horse*" atau Kuda Troya diambil dari sebuah taktik perang yang digunakan untuk merebut kota Troy yang dikelilingi benteng nan kuat. Pihak penyerang membuat sebuah patung kuda raksasa yang di dalamnya memuat beberapa prajurit yang nantinya ketika sudah berada di dalam wilayah benteng akan keluar untuk melakukan penyerangan dari dalam. Adapun bentuk kuda dipilih sebagaimana layaknya sebuah hasil karya seni bagi sang Raja agar dapat dengan leluasa masuk ke dalam benteng yang dimaksud. Ide ini mengilhami sejumlah *hacker* dan *cracker* dalam membuat *virus* atau *worm* yang cara kerjanya mirip dengan fenomena taktik perang ini, mengingat pada waktu itu bermunculan Anti Virus Software yang dapat mendeteksi virus maupun worm dengan mudah untuk kemudian dilenyapkan. Dengan menggunakan prinsip ini, maka penggalan program *malicious* yang ada dimasukkan ke dalam sistem melalui sebuah program atau aktivitas yang legal, seperti : melalui proses instalasi perangkat lunak aplikasi, melalui proses "*upgrading*" versi software yang baru, melalui proses "download" program-program *freeware*, melalui file-file multimedia (seperti gambar, lagu, dan video), dan lain sebagainya. Pengertian *Trojan* dalam sistem komputer adalah sebuah program yang diinginkan dan disisipkan kedalam komputer/laptop dengan cara menumpangi sebuah program atau file lain untuk mengelabui user. Bila file tersebut dieksekusi oleh user, maka selain file tersebut berjalan seperti biasa nyatanya ada proses lain yang berjalan tanpa sepengetahuan user dan biasanya memberikan dampak yang merugikan bagi komputer/laptop yang telah terinfeksi oleh *Trojan*.




Gambar 2. 4 Statistik Perkembangan Trojan 2018

(*Sumber : Vaksin.com)*

Berdasarkan teknik dan metode yang digunakan, terdapat beberapa jenis *Trojan Horse*, antara lain: (Eko Indrajit, 2008)

a. *Remote Access Trojan (RAT)*, kerugian yang ditimbulkan adalah komputer korban dapat diakses secara *remote*;
b. *Password Sending Trojan*, kerugian yang ditimbulkan adalah *password* yang diketik oleh komputer korban akan dikirimkan melalui email tanpa sepengetahuan dari korban serangan;
c. *Keylogger*, kerugian yang ditimbulkan adalah ketikan atau input melalui keyboard akan dicatat dan dikirimkan via email kepada *hacker* yang memasang *keylogger*;
d. *Destructive Trojan*, kerugian yang ditimbulkan adalah file-file yang terhapus atau hard disk yang terformat;
e. *File Transfer Protocol (FTP) Trojan*, kerugian yang terjadi adalah dibukanya port 21 dalam sistem komputer tempat dilakukannya download dan upload file;
f. *Denial of Service (DoS) Trojan,* jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber *(resource)* yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.
g. *Software Detection Killer*, kerugiannya dapat program-program keamanan, seperti zone alarm, anti-virus, dan aplikasi kemanan lainnya; dan
h. *Proxy Trojan*, kerugian yang ditimbulkan adalah di- "settingnya" komputer korban menjadi "*proxy server*" agar digunakan untuk melakukan "*anonymous telnet*", sehingga dimungkinkan dilakukan aktivitas belanja online dengan kartu kredit curian dimana yang terlacak nantinya adalah komputer korban, bukan komputer pelaku kejahatan.

Modus dari *Trojan Horse* ini adalah menumpangi file biasa yang bila sudah dieksekusi akan menjalankan aktivitas lain yang merugikan sekalipun tidak menghilangkan fungsi utama file yang ditumpanginya. *Trojan Horse* merupakan *malware* berbahaya, lebih dari sekedar keberadaannya tidak diketahui oleh pengguna komputer. *Trojan* dapat melakukan aktivitas tak

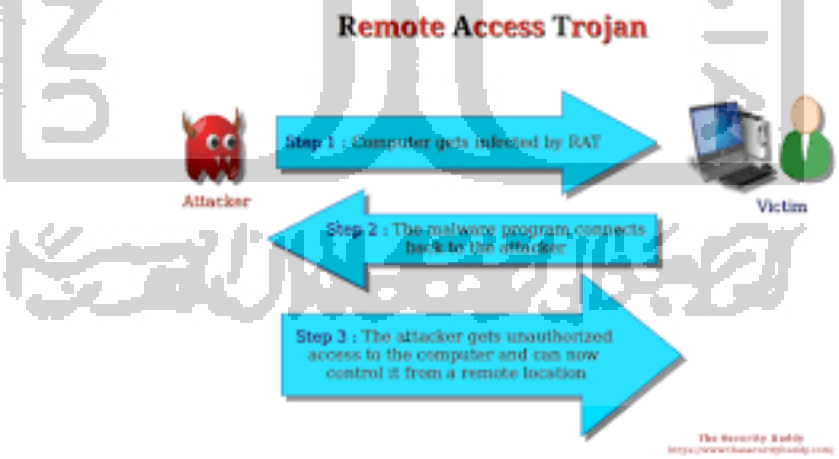
terbatas bila sudah masuk ke dalam sistem komputer. Kegiatan yang biasa dilakukan adalah merusak sistem dan file, mencuri data, melihat aktivitas *user* (*spyware*), mengetahui apa saja yang diketikkan oleh *user* termasuk *password* (*keylogger*) bahkan menguasai sepenuhnya komputer yang telah terinfeksi *Trojan Horse*.

### 2.2.1 *Remote Access Trojan* (RAT)

*Remote Access Trojan* (RAT) adalah sebuah *software* atau program yang digunakan hacker untuk mengendalikan komputer korban sepenuhnya. Hal ini dapat mengirim kepada komputer korban dalam bentuk gambar, video atau file lainnya. Beberapa jenis RAT tidak dapat di deteksi oleh anti virus apapun. Setelah RAT diinstal di Laptop korban oleh hacker, hacker dapat melakukan hampir semua hal dengan Laptop tersebut. (Septiani et al., 2017)

Beberapa fungsi berbahaya yang dapat dilakukan dengan RAT, yaitu :

- Menginfeksi file
- Menginstal Keylogger
- Mengontrol komputer jarak jauh termasuk webcam, suara, film, file dan lain-lain
- Menggunakan PC korban untuk menyerang website (DDoS)
- Melihat layar Laptop korban.




Gambar 2. 5 Cara Kerja RAT

Serangan *Remote Access Trojan (RAT)* sangat sulit dicegah, sebab memakan habis *bandwidth* yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para *script kiddies* yang pengetahuan hacking-

nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

### 2.2.2 Keamanan Data

Menurut Harol F. Tipton, keamanan data adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi. Ada empat aspek utama dalam keamanan data dan informasi yaitu: (Eko Indrajit, 2014)

a. *Privacy/Confidentiality* yaitu usaha menjaga data informasi yang bersifat pribadi dari orang yang tidak berhak mengakses.
b. *Integrity* yaitu usaha untuk menjaga data atau informasi tidak diubah oleh yang tidak berhak.
c. *Authentication* yaitu usaha atau metode untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar atau layanan dari *server* yang diberikan benar berasal dari *server* yang dimaksud.
d. *Availability* berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.

Keamanan data adalah keadaan catatan yang berisi kumpulan fakta-fakta yang berada dalam keadaan aman tanpa adanya gangguan yang membahayakannya. Seiring dengan berbagai tindak kejahatan yang terjadi dengan memanfaatkan kelemahan pada suatu jaringan. Juga berkembang beberapa teknik pengamanan yang bisa digunakan untuk meminimalisir resiko terjadinya kejahatan tersebut. Seperti yang dijelaskan dalam suatu penelitian, bahwa tidak ada suatu jaringan yang benar-benar aman, teknologi yang ada dibuat hanya untuk mengurangi resiko kejahatan yang bisa saja terjadi. Jadi, dengan meningkatkan sistem keamanan data pada jaringan komputer, kita dapat berupaya mempersulit para *hacker* atau *cracker* di saat mencoba membobol atau merusak sistem jaringan kita, sehingga mereka tidak bisa dengan mudahnya melakukan tindakan yang dapat merugikan.

Keamanan data dapat dibedakan menjadi dua kategori, yaitu keamanan fisik dan keamanan sistem. Keamanan fisik merupakan bentuk keamanan berupa fisik dari server, terminal/client router sampai dengan cabling. Sedangkan

keamanan sistem adalah keamanan pada sistem pengoperasiannya atau lebih khususnya pada lingkup perangkat lunak. Keamanan data adalah cara untuk memastikan data yang disimpan aman dari korupsi dan bahwa akses kesana adalah sesuai dikendalikan. Jadi keamanan data membantu untuk memastikan privasi, hal ini juga membantu dalam melindungi data pribadi.

Data-data yang dikirimkan melalui jaringan internet sebagian adalah data-data penting. Hal ini mengundang pihak lain untuk mencuri dan memanfaatkan data-data tersebut untuk kepentingan pribadinya. Tentu saja akan merugikan pemilik data. Pencurian dan pemanfaatan data-data oleh orang yang tidak berhak merupakan sebuah kejahatan. Internet sangat berperan penting dalam kehidupan manusia saat ini. Banyak aktivitas yang dilakukan dengan memanfaatkan internet. Data-data tersebut dikirim dari komputer user ke komputer server penyedia layanan yang digunakan. Sebelum sampai di komputer server penyedia jasa layanan, data-data yang dikirimkan akan melewati komputer-komputer yang ada di jaringan internet. Pada saat melewati jaringan internet, data-data yang dikirimkan rawan terhadap penyadapan. Selain penyadapan. Komputer yang digunakan bisa saja terjangkit oleh virus yang bekerja sebagai spyware. Dimana spyware dapat merekam semu aktivitas yang dilakukan. Karena terhubung dalam sebuah jaringan internet, maka sebuah komputer rawan terhadap penyusupan dari luar. Jika seseorang dapat menyusup ke sebuah komputer maka orang tersebut dapat mengambil data-data yang disimpan di komputer tersebut dan menggunakannya untuk keuntungan pribadi. Keamanan data menjadi hal penting dalam komunikasi data yang dilakukan. Bila data user ID dan password dari layanan yang kita gunakan jatuh ke tangan orang yang salah, bisa saja orang tersebut akan memanfaatkan untuk hal-hal yang tidak bertanggung jawab. (Kristono et al., 2018)

Berdasarkan hasil penelitian, tidak ada jaringan komputer yang benar-benar aman dari serangan hacker, cracker, spam, e-mail bomb, virus komputer dan sebagainya. Yang dapat dilakukan adalah menjaga jangan sampai jaringan tersebut mudah dijebol, sambil terus berusaha meningkatkan sistem keamanan data dan jaringan. Pada era global sekarang ini, keamanan sistem informasi berbasis internet menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada

saat data terkirim dari suatu komputer ke komputer lain di dalam internet, data itu akan melewati sejumlah komputer yang lain. Berarti akan memberi kesempatan pada user untuk mengambil alih suatu atau beberapa komputer. Kecuali suatu komputer terkunci alam suatu ruangan yang mempunyai akses terbatas ke luar dari ruangan itu, maka komputer tersebut akan aman. Pembobolan sistem keamanan di Internet terjadi hampir setiap hari diseluruh dunia. Kejahatan Cyber atau lebih dikenal Cyber Crime adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke Internet dan mengillustrasi komputer lain yang terhubung juga pada Internet. Adanya lubang-lubang pada system operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para hacker, cracker dan Script kiddies untuk menyusup ke dalam komputer tersebut. Kejahatan yang terjadi dapat berupa Pencurian terhadap data, Akses terhadap jaringan internal, Perubahan terhadap data-data penting Pencurian informasi dan berujung pada penjualan informasi.

Diantara teknik-teknik pengamanan data jaringan yang sering digunakan adalah sebagai berikut : (Widiasari & Chandra, 2008)

***a. Internet Firewall***

Jadi pengamanan jaringan bisa dengan menggunakan *internet Firewall*. Cara kerja sistem ini akan mengidentifikasi data-data dalam suatu jaringan agar tidak dapat diakses oleh pihak lain di luar dari yang terkoneksi pada jaringan tersebut. *Firewall* akan mengontrol, mengatur, mengendalikan siapa-siapa saja yang dapat mengakses di jaringan itu, sehingga data-data yang terdapat di jaringan ini terlindungi aman karena tidak sembarang orang bisa mengaksesnya. Tipe sistem pengamanan *Internet Firewall* ada 2, dengan menggunakan sistem *proxy* dan sistem *filtering*. Tipe sistem *proxy*, memberi kebebasan pada user yang terkoneksi dalam jaringan untuk saling bertukar data, mengakses data serta melakukan perintah lainnya, tetapi membatasi pengguna luar untuk bergabung dalam jaringan. Tipe *Proxy* membaca alamat IP masing-masing client yang sudah legal terhubung agar bisa berkoneksi, jika ada perangkat lain dengan IP yang belum terverifikasi maka akses tidak diberikan. Sedangkan Tipe *Filtering*, pengamanan tipe ini juga akan mengontrol keluar masuknya data yang beredar antar perangkat, baik yang di dalam ataupun yang di luar jaringan. Data yang terdapat pada jaringan di *filter*

terlebih dahulu keamanannya, mana tau ada unsur data yang tidak di kenal dan membahayakan sebagai virus. Jadi hanya data-data tertentu saja yang diizinkan untuk beredar pada jaringan dengan pengamanan tipe *filtering*.

**b. *Enkripsi***

Pengamanan dengan teknik ini memanfaatkan cara kerja sistem pengacakan. Jadi data yang masih dalam proses pengiriman, ditransformasikan, dibagi-bagi, diacak-acak menjadi semacam kode-kode yang tidak dapat di mengerti. Dengan begitu, jika terjadi pembobolan maka si hacker tadi tidak akan bisa mengerti (membaca) data-data yang di curi karena bentuknya sudah berupa kode-kode yang teracak tidak beraturan.

***c. Pretty Good Privacy***

Sistem pengamanan dengan menggabungkan metode enkripsi simetris, digest dan asimetris. Gabungan dari ketiga metode tersebut menghasilkan "*Private-Public-Key*" istilah pada sistem ini. Setiap user membuat key (kunci) sebagai kode agar bisa masuk ke dalam jaringan. Kode key yang dibuat secara otomatis terdiri atas 2 kode yang berbeda, *publik key* dan *secret key*. *Public key* merupakan kode yang bisa kita berikan pada perangkat lain agar bisa terhubung dengan kita, dan *secret key* adalah kode untuk kita bisa menerima pesan yang disampaikan perangkat lain yang sebelumnya telah kita berikan kode *publik key* tersebut. Jadi, meskipun ada perangkat lain tanpa sepengetahuan kita mengetahui kode *public key*, dia tidak dapat mengakses data pada jaringan komputer karena perangkat akan menolak sebuah perintah tanpa persetujuan pemberian *public key* secara legal. Dalam hal ini kita sebagai pengendali jaringannya.

**d. *Kriptografi***

Pengamanan data yang dilakukan untuk melindungi data dari gangguan pihak ketiga yang tidak dikenal. Sistem pengamanan ini mengutamakan pengolahan data menjadi bentuk yang rumit, dan hanya si pemilik yang mengetahui maksud dan tujuannya. *Kriptografi* dikenal juga dengan seni atau ilmu merahasiakan suatu informasi. Informasi diolah sedemikian rupa agar tidak terbaca oleh orang lain. Ada beberapa metode dalam *kriptografi* :

- *Substitution Ciphers*, metode mengganti data menjadi karakter atau simbol tertentu. Misalnya "Jatuh bangun" menjadi "Jwtxh bwngxn"

- *Transposition Ciphers*, metode mengacak huruf atau bagian kata agar menjadi lebih rumit. Misalnya “Jatuh bangun” menjadi “Tuhjah ngunba”
- *Steganography*, menyembunyikan pesan aslinya kemudian memodifikasi dengan data yang lain agar tidak diketahui pesan aslinya. Misalnya “Jatuh bangun” menjadi "Sangat jatuh sekali bangun”

***e. Sniffer Paket***

Atau disebut juga monitor jaringan. Merupakan aplikasi yang dapat melihat lalu lintas data atau kegiatan dalam suatu jaringan. Dapat menangkap informasi pada jaringan, guna mengontrol segala kegiatan yang terjadi. Dengan kemampuannya seperti itu aplikasi ini dapat dimanfaatkan untuk pengamanan jaringan :

- Dapat mendeteksi jika adanya gangguan dalam jaringan, baik akibat gejala penyelundupan atau lainnya.
- Mengontrol penggunaan jaringan serta pertukaran data yang terjadi
- Kita memiliki akses terhadap pengguna luar yang tergabung dalam jaringan

### 2.2.3 Firewall

Firewall merupakan suatu perangkat keamanan jaringan yang memperkenalkan berbagai bagian ruas jaringan untuk melaksanakan komunikasi antara satu sama lainnya sesuai dengan definisi kebijakan keamanan *(Security Policy)* yang telah ditetapkan sebelumnya. Firewall bisa dikatakan sama fungsinya dengan Router, jika ditempatkan dalam konteks sebagai perangkat yang melaksanakan interkoneksi berbagai ragam ruas jaringan secara bersamaan. Perangkat lunak firewall berjalan pada sebuah *host* yang akan mengkoneksikan beragam jaringan yang memiliki berbagai tingkat keamanan. Sistem operasi di dalam host bertangggung jawab dalam pelaksanaan fungsi-fungsi *routing* yang kebanyakan sistem operasi memang memiliki kemampuan untuk itu.

Firewall berbeda dengan *router* dalam konteks kemampuan mereka menyediakan mekanisme keamanan dalam rangka memperkenankan atau menolak beragam trafik, seperti aktifitas autentikasi, enkripsi, keamanan isi atau muatan *(Content Security)* serta translasi alamat. Fungsi utama dari firewall adalah menyelenggarakan kebijakan keamanan terhadap suatu jaringan tertentu dan memang perangkat ini sengaja di desain untuk melaksanakan maksud-maksud ini. Firewall merupakan suatu sistem yang dirancang untu mencegah akses yang tak

diinginkan dari atau kedalam suatu jaringan internal. Firewall akan bertindak seperti sebuah pintu terkunci yang diletakkan di antara jaringan internal dengan eksternal dan cara paling efektif dalam rangka mengamankan suatu sistem jaringan. Firewall melacak dan mengendalikan jalannya data serta memutuskan aksi untuk melewatkan *(pass),* menjatuhkan (*drop),* menolak *(reject),* mengenkripsi atau melakukan *log* terhadap data. (Widiasari & Chandra, 2008)

Firewall menjamin agar data sesuai dengan aturan (*rules)* yang terdapat di dalam kebijakan keamanannya *(security policy),* yaitu seperangkat aturan yang telah didefinisikan di dalam keamanan jaringan internal.

### 2.2.4 Winbox

Winbox adalah sebuah software atau utility yang di gunakan untuk meremote sebuah server MikroTik kedalam mode GUI (*Graphical User Interface*) melalui operating system windows. Pengguna lebih banyak mengkonfigurasi MikroTik atau MikroTik routerboard menggunakan winbox di banding dengan yang mengkonfigurasi langsung lewat mode CLI (*Command Line Interface*). Itu di sebabkan, tidak lain karena pengerjaannya yang lebih simple & mudah dan dengan menggunakan software winbox ini penyettingan sebuah server dapat diselesaikan dengan cepat di banding dengan yang megunakan mode CLI yang harus menghapal dan mengetikan perintah-perintah console MikroTik. Untuk konfigurasi penggunaan Winbox harian Router MikroTik sebaiknya menggunakan IP-Address. Karena konfigurasi menggunakan IP-Address akan lebih stabil dengan menggunakan protocol TCP.

Untuk melakukan konfigurasi kadang sering tanpa sengaja atau karena mencoba suatu fitur sehingga dapat melakukan kesalahan setting yang mengakibatkan winbox putus dan Router tidak bisa diakses. Dengan kata lain konfigurasi yang kita tambahkan mengganggu kinerja router yang sedang berjalan. Dalam hal ini kita dapat meminimalkan kesalahan konfigurasi, mka kita dapat menggunakan tombol "Safe Mode". Selain itu Dashboard winbox dapat digunakan untuk menampilkan beberapa informasi yaitu Time, Date, CPU load, memory, dan Uptime. Dengan adanya informasi yang tertampil langsung di dashboard akan lebih memudahkan kita dalam mengontrol atau monitoring Router saat melakukan remote winbox.

Fungsi utama winbox adalah untuk setting yang ada pada MikroTik, berarti tugas utama windox adalah untuk menyetting atau mengatur MikroTik dengan GUI, atau tampilan desktop fungsi winbox lebih rinci adalah :

1. Setting MikroTik router
2. Setting Limit Bandwitch jaringan
3. Untuk setting blokir sebuah situs
4. Setting Login Hotspot
5. Setting pengaman jaringan dan
6. Masih banyak yg lainnya.

### 2.2.5 Wireshark

Wireshark adalah tool yang ditujukan untuk penganalisisan paket data jaringan. Wireshark melakukan pengawasan paket secara waktu nyata (*real time*) dan kemudian menangkap data dan menampilkannya selengkap mungkin. Wireshark bisa digunakan secara gratis karena aplikasi ini berbasis sumber terbuka. Aplikasi Wireshark dapat berjalan di banyak platform, seperti Linux, Windows dan Mac.

Ada banyak hal yang dapat kita lakukan dengan Wireshark, beberapa contoh skenario yang mungkin menggambarkan kapan kita perlu menggunakan Wireshark berikut :

1. Melakukan *troubleshoot* permasalahan jaringan
2. Melakukan pengujian masalah keamanan
3. Melakukan *debugging* implementasi protokol
4. Belajar protokol jaringan

Wireshark ini diibaratkan sebagai media tool sehingga pemakaiannya diserahkan kepada penggunanya, apakah untuk kebaikan atau kejahatan. Wireshark dapat digunakan untuk mencuri informasi sensitif yang berkeliaran pada jaringan, contohnya kata sandi, *cookie* dan sebagainya.

### 2.2.6 Disk Investigator

Disk Investigator adalah tool *software* yang mampu melihat dan melakukan *browsing* keseluruhan *file* yang ada pada sebuah *hard disk.* Tool ini bisa melihat *file* yang disembunyikan oleh *malware* masih ada atau tidak dan membaca informasi mengenai *drive.* Proses pembacaan tergantung dari seberapa besar kapasitas hard drive dan seberapa cepat komputer user, semakin besar

kapasitas hard disk, akan semakin lama pula proses pembacaannya. Tool ini menampilkan urutan angka *hexadecimal* yang mencerminkan urutan *cluster* pada *hard disk.* Tool ini juga bisa membantu ketika sebuah *malware* menyerang direktori yang tidak dapat diakses oleh pengguna melalui *System Volume Information* dan *Recycler.* Secara default pada sistem operasi windows, folder tersebut tidak ditampilkan file sistem.