BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Rujukan penelitian yang pertama yaitu jurnal Md Rifat Bin Emdad dan Md Shahun Khan mahasiswa program studi Ilmu Komputer dan Teknik *Jahangirnagar University* tahun 2019 dengan judul *A Stardard Data Security model Using AES Algorithm in Cloud Computing.* Dalam penelitiannya peneliti menganalisa keamanan data melalui *Cloud Computing.*

Rujukan penelitian yang kedua yaitu jurnal Agus Tedyyana, Supria Teknik Informatika Politeknik Negeri Bengkalis pada tahun 2018 dengan judul Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway. Dalam Penelitiannya peneliti menggunakan Mikrotik dengan metode melalui *SMS Gateway*.

Rujukan penelitian yang ketiga yaitu jurnal Amarudin Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia pada tahun 2018 dengan judul Analisis dan Implementasi Keamanan Jaringan Pada Mikrotik Router OS Mengguakan Metode Port Knocking.

Sedangkan penelitian yang akan dilakukan oleh peneliti tidak jauh berbeda dengan penelitian sebelumnya yaitu untuk melakukan pencegahan serangan Malware yang dapat mengakibatkan kerusakan data yang terdapat di Jurusan Teknik Komputer agar semua *user* yang terhubung ke dalam jaringan terbebas dari seangan *Malware*.

Untuk lebih jelas dan detail terhadap penelitian terdahulu dapat dilihat pada tabel berikut:

No	Penelitian	Persamaan	Perbedaan
1.	Md Rifat Bin Emdad dan Md Shahun Khan. 2019. *A Stardard Data*	- Kemanan data dan jaringan	- Membuat sitem kemanan data dari serangan Malware

	Security model Using AES Algorithm in Cloud Computing		dengan menggunakan metode Port Knocking pada Filter Firewal pada Mikrotik
2.	Agus Tedyyana, Supria. 2018. Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway.	- Membahas Malware Security - Menggukaan Media (Mikrotik)	- Metode dalam implementasi menggunakan metode Port Blocking
3	Amirudin. 2018. Analisis dan Implementasi Keamanan Jaringan Pada Mikrotik Router OS Mengguakan Metode Port Knocking.	- Menggunakan metode Port Knocking	- Membuat Malware Security dengan metode Port Blocking

Dari penelitian diatas masih terdapat beberapa kekurangan dari sisi kemanan dan penulis berusaha mengembangkan hal tersebut dengan melakukan konfigurasi filter firewall untuk kemanana jaringan dari serangan malware.

2.2 Mikrotik

Mikrotik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan computer menjadi router yang handal mencakup berbagai fitur yang dibuat untuk IP network dan jaringan wireless, cocok digunakan oleh ISP, provider hotspot, dan warnet. Fitur-fitur tersebut diantaranya : Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, dan masih banyak lagi fitur lainnya. Mikrotik dapat digunakan dalam 2 tipe, yaitu dalam bentuk perangkat keras dan perangkat lunak. Dalam bentuk

perangkat keras, Mikrotik biasanya sudah diinstalasi pada suatu board tertentu, sedangkan dalam bentuk perangkat lunak, Mikrotik merupakan satu distro Linux yang memang dikhususkan untuk fungsi router(Yohanes,2013).

2.2.1 Mikrotik OS

MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai. Mikrotik sekarang ini banyak digunakan oleh ISP, provider hotspot, ataupun oleh pemilik warnet. Mikrotik OS menjadikan komputer menjadi router network yang handal yang dilengkapi dengan berbagai fitur dan tool, baik untuk jaringan kabel maupun wireless (Handriyanto,2019).

2.2.2 Akses Mikrotik:

a. via console

Mikrotik router board ataupun PC dapat diakses langsung via console/ shell maupun remote akses menggunakan putty (www.putty.nl).

b. via winbox

Mikrotik bisa juga diakses/remote menggunakan software tool Winbox.

c. via web

Mikrotik juga dapat diakses via web/port 80 dengan menggunakan browser.

2.3 Jaringan Komputer

Jaringan komputer adalah sebuah sistem yang terdiri atas komputer-komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi, dan dapat mengakses informasi. 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 dan yang memberikan/mengirim layanan disebut peladen (*server*) Desain ini disebut dengan sistem *client - server*, dan digunakan pada hampir seluruh aplikasi jaringan komputer (Ridwan,2019).

Gambar 2.1 Jaringan Komputer

(Sumber: Ridwan, 2019)

2.3.1 Jenis - Jenis Jaringan

Dalam jaringan komputer, terdapatjenis-jenis jaringan yang berbeda. diantaranya :

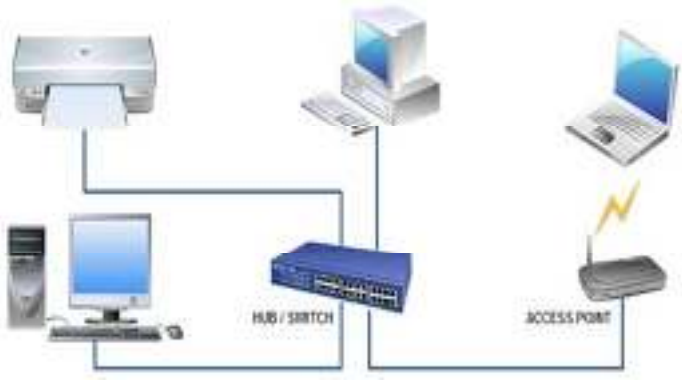
1. PAN (Personal Area Network)

PAN adalah singkatan dari personal area network. Jenis jaringan komputer PAN adalah hubungan antara dua atau lebih sistem komputer yang berjarak tidak terlalu jauh. Biasanya Jenis jaringan yang satu ini hanya berjarak 4 sampai 6 meter saja. Jenis jaringan ini sangat sering kita gunakan. Contohnya menghubungkan hp dengan komputer seperti pada Gambar 2.1 (Wongkar, 2015).

Gambar 2.2 PAN (*Personal Area Network*)
(Sumber: Wongkar, 2015)

2. LAN (Local Area Network)

LAN adalah singkatan dari local area network. Jenis jaringan LAN ini sangat sering kita temui di warnet-warnet, kampus, sekolah ataupun perkantoran yang membutuhkan hubungan atau koneksi antara dua komputer atau lebih dalam suatu ruangan seperti Gambar 2.1 (Wongkar, 2015).

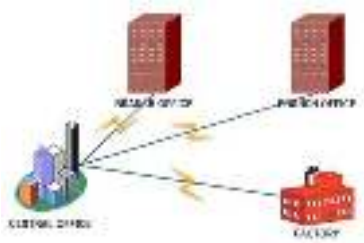


Gambar 2.3 LAN (*Local Area Network*)
(Sumber: Wongkar, 2015)

3. MAN (Metropolitan Area Network)

MAN singkatan dari metropolitan area network. Jenis jaringan komputer MAN ini adalah suatujaringan komputer dalam suatu kota dengantransfer data berkecepatan tinggi yang menghubungkan suatu lokasi seperti sekolah, kampus, perkantoran dan pemerintahan. Sebenarnya jaringan MAN ini adalah gabungan

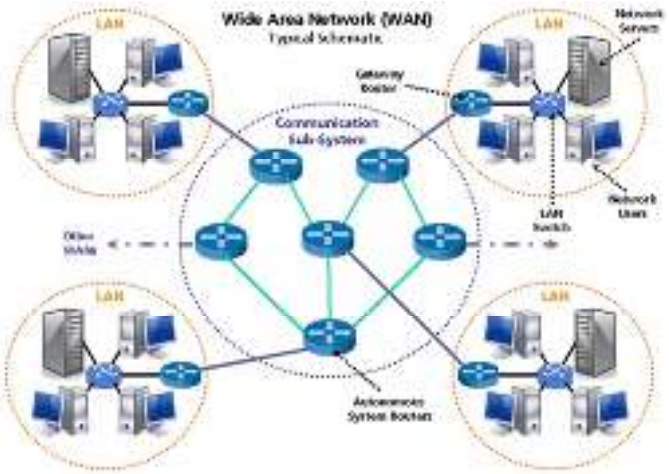
dari beberapa jaringan LAN. Jangkauan dari jaringan MAN ini bisa mencapai 10 - 50 kilo meter seperti pada Gambar 2.4 (Wongkar, 2015).



Gambar 2.4 MAN (*Metropolitan Area Network*)
(Sumber: Wongkar, 2015)

4. WAN (Wide Area Network)

WAN singkatan dari wide area network. WAN adalah jenis jaringan komputer yang mencakup area yang cukup besar. Contohnya adalah jaringan yang menghubugkan suatu wilayah atau suatu negara dengan negara lainnya. Kita dapat melihat contoh WAN pada Gambar 2.5 (Wongkar, 2015).



Gambar 2.5 WAN (*Wide Area Network*)
(Sumber: Wongkar, 2015)

5. WLAN (Wireless LAN)

Pengertian Wireless LAN atau kadang disingkat dengan WLAN adalah sebuah sistem komunikasi data yang fleksibel yang dapat diaplikasikan sebagai ekstensi ataupun sebagai alternatif pengganti untuk jaringan LAN kabel. Wireless

LAN menggunakan teknologi frekuensi radio, mengirim dan menerima data melalui media udara, dengan meminimalisasi kebutuhan akan sambungan kabel. Dengan begitu, wireless LAN telah dapat mengkombinasikan antara konektivitas data dengan mobilitas user. Wireless LAN adalah sebuah alternatif dimana untuk alternatif LAN kabel sulit atau tidak mungkin dibangun. Tempat-tempat seperti bangunan tua yang dilindungi atau ruang ruang kelas (Wongkar, 2015).

2.3.2 Topologi Jaringan

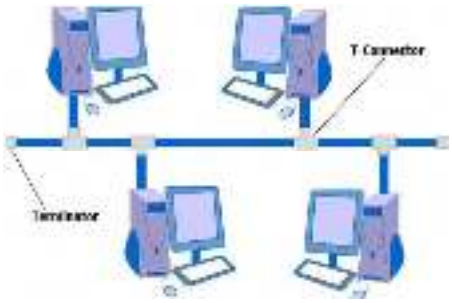
Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk suatu jaringan. Topologi jaringan komputer atau arsiterktur jaringan komputer adalah merupakan pola hubungan antar terminal dalam suatu sistem jaringan komputer yang dapat mempengaruhi tingkat efektivitas kinerja jaringan.

Dari beberapa pengertian diatas dapat disimpulkan bahwa topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk pola hubungan antar terminal dalam suatu sistem jaringan yang dapat mempengaruhi tingkat efektivitas kinerja jaringan. Ada beberapa jenis topologi yang dapat diimplementasikan dalam jaringan komputer yaitu topologi Bus, topologi Ring, topologi Star, topologi Mesh (Ginta, 2013).

2.3.3 Jenis - Jenis Topologi Jaringan

1. Topologi Bus

Topologi *Bus* adalah merupakan topologi yang menghubungkan semua terminal ke satu jalur komunikasi yang kedua ujungnya ditutup dengan terminator. Terminator adalah perangkat yang menyediakan resistansi listrik untuk menyerap sinyak pada akhir transmisi sambungan agar sinya tidak terlontar kembali dan diterima oleh stasiun jaringan. Contoh topologi bus dapat dilihat pada Gambar 2.6 dibawah ini (Ginta, 2013).



Gambar 2.6 Topologi *Bus*
(Sumber: Ginta, 2015)

Kareteristik Topologi *Bus*:

a. Node-node dihubungkan secara serial sepanjang kabel
b. Sangat sederhana dalam instalasi
c. Sangat ekonomis dalam biaya
d. Paket-paket data saling bersimpangan pada suatu kabel
e. Tidak diperlukan *Hub*, yang banyak diperlukan adalah *Tconnector*

Keuntungan Topologi *Bus* :

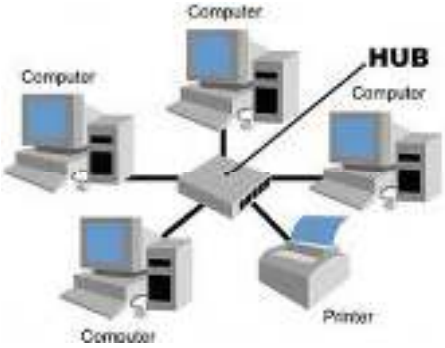
a. Topologi yang sederhana
b. Kabel yang digunakan sedikit untuk menghubungkan komputer-komputer atau peralatan yang lain
c. Biayanya lebih murah dibandingkan dengan susunan pengkabelan yang lain
d. Cukup mudah apabila ingin memperluas jaringan pada topologi bus

Kekurangan Topologi *Bus* :

a. *Traffic* (lalu lintas) yang padat akan memperlambat jalur bus
b. Seluruh jaringan mati jika terjadi kerusakan pada kabel utama
c. Membutuhkan terminator pada kedua sisi kabel utamanya
d. Sangat sulit mengidentifikasikan permasalahan jika jaringan mati
e. Paling lambat jika dibandingkan dengan topologi jaringan yang lain

2. Topologi Star

Topologi star didesain dimana setiap node (file server, workstation, dan perangkat lainnya) terkoneksi ke jaringan melewati sebuah Hub atau Concentrator (Ginta, 2013).



Gambar 2.7 Topologi Star
(Sumber: Ginta, 2013)

Karakteristik Topologi *Star* :

a. Setiap node berkomunikasi langsung dengan *hu*b
b. Bila setiap paket data yang masuk ke *consentrator* (*Hub*) kemudian di broadcast keseluruh node yang terhubung sangat banyak (misalnya memakai *hu*b 32 *port*), maka kinerja jaringan akan semakin turun
c. Jika salah satu *ethernet card* rusak, atau salah satu kabel pada terminal putus, maka keseluruhhan jaringan masih tetap bisa berkomunikasi atau tidak terjadi *down* pada jaringan keseluruhan tersebut

Keuntungan Topologi *Star* :

a. Mudah dipasang dan pengkabelan
b. Tidak mengakibatkan gangguan bila terjadi perbaikan
c. Mudah untuk mendeteksi kesalahan dan memindahkan perangkat lain

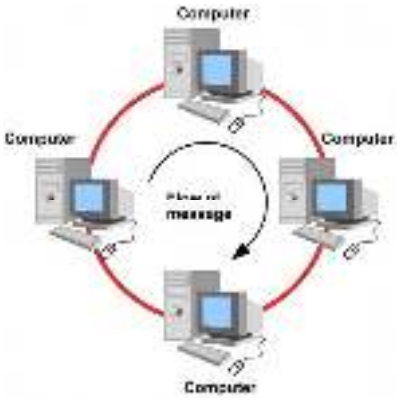
Kekurangan Topologi *Star* :

a. Memiliki satu titik kesalahan, terletak pada *hub*. Jika *hub* pusat mengalami kegagalan, maka seluruh jaringan akan gagal untuk beroperasi

b. Membutuhkan lebih banyak kabel karena semua kabel jaringan harus ditarik .ke satu *central point*, jadi lebih banyak membutuhkan lebih banyak kabel daripada topologi jaringan yang lain
c. Jumlah terminal terbatas, tergantung dari *port* yang ada pada *hub*

3. Topologi *Ring*

Di dalam topologi *Ring* semua *work station* dan *server* dihubungkan sehingga terbentuk suatu pola lingkaran atau cincin. Tiap *workstation* ataupun *server* akan menerima dan melewatkan informasi dari satu komputer ke komputer lain, bila alamat-alamat yang dimaksud sesuai maka informasi diterima dan bila tidak informasi akan dilewatkan (Ginta, 2013).



Gambar 2.8 Topologi *Ring*
(Sumber: Ginta, 2013)

Karakteristik Topologi *Ring* :

a. Node-node dihubungkan secara serial di sepanjang kabel, dengan bentuk jaringan seperti lingkaran
b. Paket-paket data dapat mengalir dalam satu arah (kekiri atau kekanan) sehingga *collision* dapat dihindarkan
c. Problem yang dihadapi sama dengan topologi *bus*, yaitu: jika salah satu node rusak maka seluruh node tidak bisa berkomunikasi dalam jaringan tersebut

Keuntungan Topologi *Ring* :

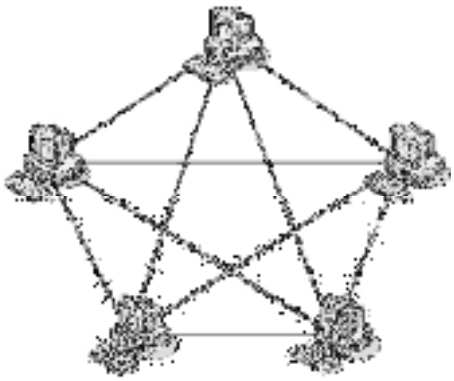
a. Data mengalir dalam satu arah sehingga terjadinya *collision* dapat dihindarkan
b. Aliran data mengalir lebih cepat karena dapat melayani data dari kiri atau kanan dari *server*
c. Dapat melayani aliran lalulintas data yang padat, karena data dapat bergerak kekiri atau kekanan

Kekurangan Topolgi *Ring* :

a. Apabila ada satu komputer dalam *ring* yang gagal berfungsi, maka akan mempengaruhi keseluruhan jaringan
b. Menambah atau mengurangi komputer akan mengacaukan jaringan
c. Sulit untuk melakukan konfigurasi ulang

4. Topologi *Mesh*

Topologi mesh memiliki hubungan yang berlebihan antara peralatan-peralatan yang ada. Susunan dalam suatu jaringan saling berhubungan dengan peralatan yang lainnya.



Gambar 2.9 Topologi *Mesh*
(Sumber: Ginta, 2013)

Karakteristik Topologi *Mesh* :

a. Jika jumlah peralatan yang terhubung sangat banyak, tentunya ini akan sangat sulit sekali untuk dikendalikan dibandingkan hanya sedikit peralatan saja yang terhubung

b. Susunannya pada setiap peralatan yang ada didalam jaringan saling terhubung satu sama lain.
c. Topologi mesh memiliki hubungan yang berlebihan antara peralatan-peralatan yang ada

Keuntungan Topologi *Mesh* :

a. Keuntungan utama dari penggunaan topologi mesh adalah *fault tolerance*
b. Terjaminnya kapasitas channel komunikasi, karena memiliki hubungan yang berlebih
c. Relatif lebih mudah untuk dilakukan *troubleshoot*

Kekurangan Topologi *Mesh* :

a. Sulitnya pada saat melakukan instalasi dan melakukan konfigurasi ulang saat jumlah komputer dan peralatan-peralatan yang terhubung semakin meningkat jumlahnya
b. Biaya yang besar untuk memelihara hubungan yang berlebih

2.4 TCP (Transport Control Protocol) :

TCP merupakan protokol yang terdapat pada lapisan transport TCP/IP. Dalam pengiriman data TCP bersifat byte stream, connection- oriented, dan dapat diandalkan. Komunikasi byte stream berarti data dinyatakan dalam urutan-urutan byte. Connection-oriented berarti sebelum terjadi pertukaran data, harus terlebih dahulu terjadi sebuah hubungan.

TCP andal dalam pengiriman data. Unit data dipecah-pecah dan diberi nomor urut (sequence number) sebelum dikirimkan dari lapisan aplikasi ke lapisan berikutnya. TCP selalu meminta konfirmasi setiap kali data yang dikirim selesai. TCP menggunakan sebuah checksum untuk memastikan kerusakan data. Jika data sampai ke tujuan dengan selamat, TCP akan mengirimkan data urutan selanjutnya. Jika tidak, urutan data yang hilang atau rusak tersebut akan dikirim ulang oleh TCP.

Model komunikasi dua arah pada client dan server sebelum terjadi pengiriman data disebut handshake. TCP menggunakan three-way handshake yang bertujuan untuk pembentukan koneksi, sinkronisasi segmen, dan pemberitahuan besar data yang bisa diterima pada suatu saat antara client dan server.

2.5 Malware

Malware (singkatan dari istilah Bahasa Inggris 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 (Erick, 2016).

Default Port dan Protocol pada Malware :

31/tcp	Agent 31, Hackers Paradise, Masters Paradise
1170/tcp	Psyber Stream
1234/tcp	Ultors Trojan
1243/tcp	SubSeven server (default for V1.0- 2.0)
1981/tcp	ShockRave
2001/tcp	Trojan Cow
2023/tcp	Ripper Pro
2140/udp	Deep Throat, Invasor
2989/tcp	Rat backdoor
3024/tcp	WinCrash
3150/tcp	Deep Throat, Invasor
3700/tcp	Portal of Doom
4950/tcp	ICQ Trojan
6346/tcp	Gnutella
6400/tcp	The Thing

6667/tcp	Trinity intruder-to-master and master-To-daemon SubSeven server (default for V2.1 Icqfix and beyond)
6670/tcp	Deep Throat
12345/tcp	NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill
12346/tcp	NetBus 1.x
16660/tcp	Stacheldraht intruder-to-master
18753/udp	Shaft master-to-daemon
20034/tcp	NetBus 2 Pro
20432/tcp	Shaft intruder-to-master
20433/udp	Shaft daemon-to-master
27374/tcp	SubSeven server (default for V2.1- Defcon)
27444/udp	Trinoo master-to-daemon
27665/tcp	Trinoo intruder-to-master
30100/tcp	NetSphere
31335/udp	Trinoo daemon-to-master
31337/tcp	Back Orifice, Baron Night, Bo Facil
33270/tcp	Trinity master-to-daemon
33567/tcp	Backdoor rootshell via inetd (from Lion worm)
33568/tcp	Trojaned version of SSH (from Lion worm)
40421/tcp	Masters Paradise Trojan horse
60008/tcp	Backdoor rootshel via inetd (from Lion worm)
65000/tcp	Stacheldraht master-to-daemon
1080	MyDoom.B,MyDoom.F, MyDoom.G, MyDoom.H
2283	Dumaru.Y
2535	Beagle.W, Beagle.X, other Beagle/Bagle variants
2745	Beagle.C through Beagle.K
3127	MyDoom.A

3128	MyDoom.B
3410	Backdoor.OptixPro.13 and variants
5554	Sasser through Sasser.C, Sasser.F
8866	Beagle.B
9898	Dabber.A and Dabber.B
10000	Dumaru.Y
10080	MyDoom.B
12345	NetBus
17300	Kuang2
27374	SubSeven
65506	various names: PhatBot, Agobot, Gaobot

2.5.1 Jenis – jenis *Malware*

Menurut (Agung, 2011) berikut ini berbagai jenis *Malware* yang dinilai paling dominan menginfeksi komputer :

1. **Virus**

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.

2. ***Worm***

Worm yang berarti cacing merupakan Malware yang cukup berbahaya. Worm mampu untuk menyebar melalui jaringan komputer tanpa harus tereksekusi sebelumnya. Setelah masuk ke dalam sistem komputer, Worm memiliki kemampuan untuk mereplikasi diri sehingga mampu memperbanyak jumlahnya di

dalam sistem komputer. Hal yang diakibatkan dari aktivitas Worm adalah merusak data dan memenuhi memory dengan Worm lainnya hasil dari penggandaan diri yang dilakukannya. Replikasi ini membuat memory akan menjadi penuh dan dapat menngakibatkan aktivitas komputer menjadi macet (hang). Kebiasaan komputer menjadi hang dapat menjadi gejala awal terdapatnya Worm pada komputer tersebut. Contoh Worm yang populer akhir-akhir ini adalah Conficker.

3. *Trojan Horse*

Teknik *Malware* ini terinspirasi dari kisah peperangan kerajaan Yunani kuno yang juga diangkat ke Hollywood dalam film berjudul 'Troy'. 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*.

4. *Spyware*

Spyware merupakan *Malware* yang dirancang khusus untuk mengumpulkan segala informasi dari komputer yang telah dijangkitinya. Kegiatan *Spyware* jelas sangat merugikan *user* karena segala aktivitasnya yang mungkin menyangkut privasi telah diketahui oleh orang lain tanpa mendapat izin sebelumnya. Aktivitas *Spyware* terasa sangat berbahaya karena rentan terhadap pencurian *password*. Dari kegiatan ini juga akhirnya lahir istilah *Adware* yang merupakan iklan yang mampu muncul secara tiba-tiba di komputer korban hasil dari mempelajari aktivitas korban dalam kegiatan berkomputer. *Spam* yang muncul secara tak

terduga di komputer juga merupakan salah satu dampak aktivitas *Spyware* yang dirasa sangat menjengkelkan.

5. *Backdoor*

Kerja dari *Backdoor* sangat berkaitan dengan aktivitas *hacking*. *Backdoor* merupakan metode yang digunakan untuk melewati *autentifikasi* normal (*login*) dan berusaha tidak terdeteksi. *Backdoor* sendiri sering kali disusupkan bersama dengan *Trojan* dan *Worm*. Dapat diartikan secara singkat *Backdoor* berarti masuk ke sistem komputer melalui jalur pintu belakang secara tidak sah. Dengan metode *Backdoor* maka akan sangat mudah untuk mengambil alih kendali dari komputer yang telah berhasil disusupi. Setelah berhasil masuk maka aktivitas yang dilakukan oleh *Backdoor* antara lain adalah mengacaukan lalu lintas jaringan, melakukan *brute force attack* untuk *mengcrack password* dan enkripsi dan mendistribusikan serangan *Distributed Denial of Service* (DDoS).

6. *NjRAT*

NjRAT malware yang digunakan untuk *meremote* pc orang lain dengan jarak jauh. *RAT* digunakan untuk menghubungkan dan mengatur satu atau lebih komputer dengan berbagai kemampuan. Aspek utama dari *RAT* ini popularitasnya dengan sistem *Domain Name System* (*DNS*) layanan seperti *no-ip.com*. Sebuah layanan *DNS* dinamis adalah metode otomatis memperbarui *server* nama di *DNS*, sering secara *real time*, dengan konfigurasi *DNS* aktif *hostname* dikonfigurasi, alamat, atau informasi lainnya. Fitur ini memungkinkan penyerang tanpa IP statis khusus, seperti *DSL* atau koneksi *broadband*, untuk menggunakan nama *host* berbasis *DNS*.

2.6 Port

Port adalah tempat di mana informasi masuk dan keluar dari komputer, port scanning mengidentifikasi pintu terbuka ke komputer. Port memiliki penggunaan yang sah dalam mengelola jaringan, tetapi scanning port juga bisa berbahaya jika

seseorang sedang mencari titik akses yang lemah untuk masuk ke komputer anda(Sondakh,2014)..

2.7 Firewall

Firewall adalah sebuah sistem pengaman, jadi firewall bisa berupa apapun baik hardware maupun software. Firewall dapat digunakan untuk memfilter paket-paket dari luar dan dalam jaringan di mana ia berada. Jika pada kondisi normal semua orang dari luar jaringan anda dapat bermain-main ke komputer anda, dengan firewall semua itu dapat diatasi dengan mudah. Firewall yang sederhana biasanya tidak memiliki kemampuan melakukan filtering terhadap paket berdasarkan isi dari paket tersebut. Sebagai contoh, firewall tidak memiliki kemampuan melakukan filtering terhadap e- mail bervirus yang Anda download atau terhadap halaman web yang tidak pantas untuk dibuka. Yang bisa dilakukan firewall adalah melakukan blokir terhadap alamat IP dari mail server yang mengirimkan virus atau alamat halaman web yang dilarang untuk dibuka. Dengan kata lain, firewall merupakan sistem pertahanan yang paling depan untuk jaringan Anda (Sondakh,2014).

2.8 Router

Router merupakan perangkat keras jaringan komputer yang digunakan untuk menghubungkan beberapa jaringan yang sama atau berbeda. Router adalah sebuah alat untuk mengirimkan paket data melalui jaringan/ internet untuk dapat menuju tujuannya, proses itu disebut *routing*. Proses *routing* terjadi di lapisan 3 dari *stack protocol* tujuh-lapis OSI. Router terkadang untuk mengkoneksikan 2 jaringan dengan media berbeda, seperti dari Ethernet menuju ke Token Ring (Faizal : 2018).

2.9 Packet Filtering

Sistem pada paket filtering merupakan sistem yang digunakan untuk mengontrol keluar, masuknya paket dari antara host yang didalam dan host yang yang diluar tetapi sistem ini melakukannya secara selektif. Sistem ini dapat

memberikan jalan atau menghalangi paket yang dikirimkan, sistem ini sangat mengkitalkan arsitektur yang disebut dengan ‘Screened Router’. Router ini menjadi filter dengan menganalisa bagian kepala dari setiap paket yang dikirimkan (Sondakh,2014). Karena bagian kepala dari paket ini berisikan informasi penting

yaitu :

- IP source address.
- IP destination address.
- Protocol (dengan melihat apakah paket tersebut berbentuk TCP, UDP atau ICMP).
- Port sumber dari TCP atau UDP.
- Port tujuan dari TCP atau UDP.
- Tipe pesan dari ICMP.
- Ukuran dari paket.

Cara Kerja Sistem Packet Filtering ini adalah mengawasi secara individual dengan melihat melalui router, sedangkan router yang telah dimaksud adalah sebuah perangkat keras yang dapat berfungsi sebagai sebuah server karena alat ini harus membuat keputusan untuk me-rout seluruh paket yang diterima. Alat ini juga harus menentukan seperti apakah pengiriman paket yang telah didapat itu kepada tujuan yang sebenarnya. Dalam hal ini router tersebut saling berkomunikasi denganprotokol-protokol untuk me-rout. Protokol yang dimaksudkan adalah Routing Information Protocol (RIP) atau Open Shortest Path First (OSPF) yang menghasilkan sebuah table routing. Tabel routing itu menunjukkan kemana tujuan dari paket yang diterima. Router yang menjadi filter pada packet filtering dapat menyediakan sebuah choke point (sebuah channel yang sempit yang sering digunakan untuk dipakai oleh penyerang sistem dan tentu saja dapat dipantau juga dikontrol oleh kita) untuk semua pengguna yang memasuki dan meninggalkan network.

Karena sistem ini beroperasi ditingkat Network Layer dan Transport Layer dari tingkatan protokol pada tingkatan pada Transmission Control Protocol

(TCP/IP). Bagian kepala dari network dan transport mengawasi informasi-informasi berikut:

• Protokol (IP header, pada network layer); didalamnya byte 9 mengidentifikasikan protocol dari paket.

• Source address (IP header, pada network layer); alamat sumber merupakan alamat IP 32 bit dari host yang menciptakan oleh paket.

• Destination address (IP header, pada network layer); alamat tujuan yang berukuran 32 bit dari host yang menjadi tujuan dari paket.

• Source port (TCP atau UDP header, pada transport layer); pada setiap akhir dari koneksi TCP atau UDP tersambung dengan sebuah port, Walaupun port-port TCP terpisah dan cukup jauh dari port-port user datagram protocol (UDP). Port-port yang mempunyai nomor dibawah 1024 diterbalikan karena nomor-nomor ini telah didefinisikan secar khusus, sedangkan untuk port-port yang bernomor diatas 1024 (inklusif) lebih dikenal dengan port ephermal. Konfigurasi dari nomor pengalamatan ini diberikan sesuai dengan pilihan dari vendor.

• Destination port (TCP atau UDP header, transport layer); nomor port dari tujuan mengindikasikan port yang dikirimi paket. Servis yang akan diberikan pada sebuah host dengan mendengarkan port. Adapun port yang difilter adalah 20/TCP dan 21/TCP untuk koneksi ftp atau data, 23/TCP untuk telnet, 80/TCP untuk http dan 53/TCP untuk zona transfer DNS.

• Connection status (TCP atau UDP header, transport layer); status dari koneksi memberitahukan apakah paket yang dikirim merupakan paket pertama dari sesi di network. Jika paket merupakan paket pertama maka pada TCP header diberlakukan ‘false’ atau 0 dan untuk mencegah sebuah host untuk mengadakan koneksi dengan menolak atau membuang paket yang mempunyai bit set ‘false’ atau 0.

TCP & UDP menggunakan port number ini untuk membedakan pengiriman paket data ke beberapa aplikasi berbeda yang terletak pada komputer yang sama (Stiawan, 2008). Pada saat paket data di alamatkan ke tujuan, komputer tujuan harus mengetahui yang harus dilakukan pada paket

tersebut, protocol TCP/IP menggunakan salah satu dari 65,536 pengelamatan penomeran port.

Port number inilah yang akan membedakan antara satu aplikasi dengan aplikasi lainnya atau satu protocol dengan protocol lainnya pada saat proses transmisi data antara sumber dan tujuan. Untuk dapat melewatkan paket data dari sumber ke tujuan pada router terdapat protocol pengelamatan atau routing protocol yang saling mengupdate antara satu dengan yang lainya agar dapat melewatkan data sesuai dengan tujuannya. Di peralatan router layer 3 diperlukan konfigurasi khusus agar paket data yang masuk dan keluar dapat diatur, Access Control List (ACL) adalah pengelompokan paket berdasarkan kategori yang mengatur lalu lintas network. Dengan menggunakan ACL ini kita bisa melakukan filtering dan blocking paket data yang yang masuk dan keluar dari network atau mengatur akses ke sumber daya di network (Sondakh,2014).

2.10 Aplikasi *Winbox*

Winbox adalah sebuah *utility* yang digunakan untuk melakukan *remote* ke *serve*r mikrotik dalam mode *GUI*. Mengkonfigurasi mikrotik melaui *winbox* ini lebih banyak digunakan karena selain penggunaannya yang mudah, juga tidak harus menghapal perintah-perintah *console* (Muhammad, 2017).

2.10.1 Fungsi *Winbox*

Fungsi utama *winbox* adalah untuk *setting* yang ada pada mikrotik, berarti tugas utama *winbox* adalah untuk men*setting* atau mengatur mikrotik dengan GUI, fungsi *winbox* lebih rinci adalah untuk melakukan setting mikrotik *router*, untuk setting *bandwidth* jaringan internet, dan untuk *setting* blokir sebuah situs (Muhammad, 2017).

Gambar 2.10 *Winbox*
(Sumber: Muhammad, 2017)