1. *Unauthorized Access to Computer System and Service*

   Kejahatan ini dengan motif menyusup/memasuki ke dalam suatu system jaringan komputer secara illegal, tidak sah, tanpa ijin dari pemilik jaringan komputer yang dimasukinya. Adapun yang dilakukannya bermacam-macam contohnya pencurian data, sabotase, dan lain sebagainya.

2. *Illegal Contents*

   Kejahatan ini dilakukan dengan cara memasukan informasi maupun data ke jaringan public tentang suatu hal yang belum tentu benar, tidak sesuai dengan hokum dan menganggu ketertiban umum. Contohnya yaitu tindakan pornografi, pemuatan berita bohong, dan berbagi informasi yang melawan kebenaran.

3. *Data Forgery*

   Kejahatan ini dilakukan dengan teknik memalsukan data pada dokumen atau informasi penting yang tersimpan melalui internet.

4. *Carding*

   Kejahatan ini dilakukan untuk mengambil nomor kartu kredit milik orang lain dengan cara melanggar hukum yang berlaku lalu digunakan dalam bertransaksi dunia perdagangan digital.

5. *Hacking dan Cracker*

   Hacker merupakan sebutan bagi individu atau kelompok yang melakukan *hacking*. *Hacker* merupakan pihak yang punya minat dan

keinginan besar untuk mempelajari sistem komputer dengan cara rinci dan bagaimana menambah kapabilitasnya. Serta *cracker* sebutan bagi pihak yang melakukan *cracking.* Lalu *cracker* merupakan pihak yang melakukan kegiatan dalam perusakan arsitektur fisik maupun digital pada jaringan komputer. Dari pengertian diatas dapat diartikan seorang *cracker* juga seorang *hacker* namun memanfaatkan pengetahuan dan keterampilannya dalam dunia jaringan komputer untuk hal yang negatif.

6. *Hijacking*

   Kejahatan ini dilakukan dalam rangka pembajakan hasil karya orang lain untuk kepentingan pribadi. Kejahatan ini sering dijumpai pada *Software Privacy* (Pembajakan pada perangkat lunak).

2.2.8 Solusi dari Ancaman Jaringan Komputer

Berdasarkan uraian sebelumnya, telah dijelaskan bahwa banyak sekali ancaman dari jaringan komputer karena seiring dengan perkembangan zaman dan kebutuhan informasi yang begitu pesat, namun pakar IT pada saat ini melakukan usaha untuk mencari solusi dari masalah keamanan tersebut dengan cara :

1. Filtering Firewall

   Pada suatu komputer yang terhubung dengan jaringan baik itu jaringan lokal maupun public atau jaringan internet, seharusnya mempunyai firewall dan menjalankannya, karena tanpa firewall komputer tersebut akan berpeluang untuk diakses oleh siapapun di

jaringan yang saling terhubung. *Firewall* bisa diartikan sebagai "pos pemeriksa" yang menganalisa setiap aliran data dan trafik-trafik yang keluar dan masuk diantara jaringan lokal dan jaringan publik, setiap kali trafik yang lewat akan diperiksa jika terdapat hal yang mencurigakan akan di tolak namun jika trafik tersebut dianggap normal maka akan diteruskan. Fungsi *traffic filtering* dirancang dengan *policy-policy* keamanan (Suci et al., 2018).

2. Antivirus dan Antispyware

Antivirus merupakan aplikasi komputer yang terprogram untuk mencegah, mendeteksi, melumpuhkan (mematikan aktifitas virus) serta melakukan penanganan terhadap dokumen atau file yang terinfeksi oleh virus komputer dan program yang mengancam keamanan komputer (Akbar, Widiartha, Pada, & Ips, 2015).

Antivirus dapat dikelompokan menjadi 3 jenis, yaitu :

1. *Fix*, yaitu sebuah aplikasi yang mampu mendeteksi dan menghapus hanya satu macam virus.
2. *Antidot*, yaitu sebuah aplikasi yang mampu mendeteksi dan menghapus beberapa macam virus.
3. *Antivirus*, yaitu sebuah aplikasi yang mampu mendeteksi, memindai, mencegah, melumpuhkan dan menghapus banyak macam virus, dimana karakteristik umumnya ketika komputer dihidupkan otomatis aplikasi *antivirus* akan berjalan.

3. Instrusion Prevention System (IPS)

Instrusion Prevention System (IPS) adalah metode yang selalu digunakan sistem keamanan komputer, IPS terdiri dari kombinasi antara teknik *firewall* dan metode IDS *(Instrusion Detection System)* dengan semestinya. Teknologi ini berfungsi untuk mencegah serangan yang datang dari jaringan luar (publik) dengan menganalisa dan mencatat seluruh paket serta membaca paket dengan sensor, ketika ancaman telah terdeteksi, IPS akan membatalkan akses *(block)* lalu mendokumentasikan *(log)* semua paket data yang terdeteksi tersebut. IPS berperan seperti layaknya *firewall* yang akan menerapkan *allow* dan *block* yang berpadu dengan metode IDS yang mampu mendeteksi aliran paket secara rinci. IPS memanfaatkan *signatures* untuk mendeteksi aktivitas trafik di jaringan komputer dan terminal, dimana dalam mendeteksi paket yang keluar dan masuk dapat dicegah secepat mungkin sebelum mengganggu atau diberi akses masuk kedalam jaringan lokal (Simamora, Hendrarini, Lya, & Sitepu, 2011).

4. Access Control List (ACL)

ACL merupakan daftar *device* yang memuat MAC *Address* yang diberi hak untuk terhubung ke sebuah jaringan. Daftar ini akan menginformasikan *router* terhadap aliran paket data mana yang dapat diterima atau ditolak. ACL memberi keputusan menurut sumber data, alamat tujuan, protokol, dan nomor *port.* ACL sungguh membantu dalam pengelolaan lalu lintas data dalam akses jaringan komputer. Secara dasar, cara kerja ACL yaitu menyortir paket yang tidak

dibutuhkan saat komunikasi data bekerja sehingga mengatasi permintaan akses meskipun lalu lintas paket data yang mencurigakan dalam sistem keamanan jaringan komputer (Agnia & Larasati, 2015). Adapun fungsi dari *Access Control List* (ACL) yakni:

a. Melakukan pembatasan trafik jaringan dan meningkatkan kinerja jaringan. Contohnya, dengan membatalkan trafik video, yang berdampak mengurangi beban jaringan sehingga meningkatkan kinerja jaringan.
b. Dapat membagikan pondasi keamanan dalam akses ke jaringan. Misalnya saat *user* A tidak diizinkan untuk terhubung ke jaringan lokal institusi, namun *user* B diizinkan.
c. Dapat memberikan ketetapan terhadap jenis trafik apa yang akan diteruskan atau dibatalkan melalui *router*. Contohnya trafik *google.com* dapat diakses namun trafik *youtube.com* tidak diberi akses dalam waktu yang ditentukan.
d. Memilah *user-user* yang diberi akses atau yang tidak diberi akses ke jaringan komputer. Contohnya, ACL membolehkan atau membatalkan akses HTTP atau FTP.

5. Virtual Private Network

Pengguna yang memanfaatkan fasilitas jaringan komputer yang mempunyai mobilitas tinggi dalam menemukan informasi yang dibutuhkan, dimana pengguna yang cenderung tidak memperhatikan keamananya dalam mengakses fasilitas tersebut akan rentan terhadap

keamanan data pribadinya. Oleh sebab itu, dalam jaringan komputer membutuhkan jalur komunikasi pribadi untuk mengakses data maupun informasi penting di jaringan lokal instansi atau perusahaan dimanapun mereka berada. Maka dibuatlah mekanisme *Remote Desktop* melalui teknologi *Virtual Private Network (VPN)* yang mendasari *IPSec* yang merupakan solusi yang akurat untuk menyelesaikan permasalahan tersebut. VPN adalah sebuah jaringan *virtual* yang bersifat pribadi berada di jaringan publik. Untuk membantu dan menyediakan keamanan dalam transmisi data maka ditambahkan *IPSec* merupakan protokol yang handal dalam mengamankan transmisi data dalam *internetwork* yang berdasarkan dari model *TCP/IP* (Yunanri, Riadi, & Yudhana, 2016).

VPN merupakan suatu jaringan virtual yang dapat memberi mekanisme koneksi aman untuk aliran data dan informasi IP yang saling berhubungan antar jaringan. VPN mampu dikembangkan dalam jaringan tunggal untuk mengamankan komunikasi yang rentan terpengaruh dari pihak lain dalam jaringan yang sama. Protokol yang sering digunakan dalam implementasi dari jaringan VPN, yaitu :

a. Ipsec (Ip Security Protocol)
b. Layer-2 Forwarding
c. Layer-2 Tunneling Protocol (L2TP)
d. Point to point Tunneling Protocol

6. *Address List*

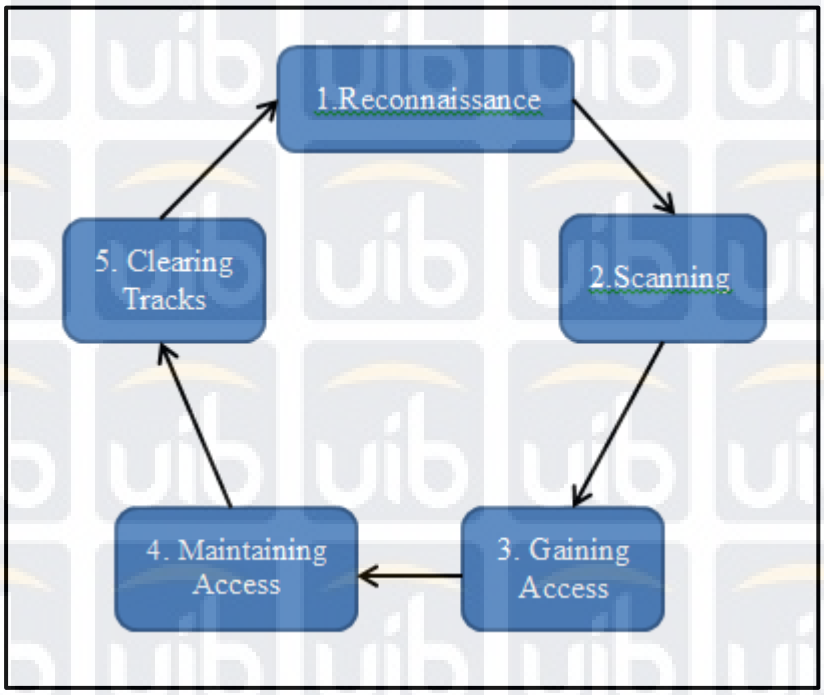
Address List adalah salah satu fasilitas dari mikrotik yang mempunyai tujuan untuk memudahkan admin jaringan dalam menandai alamat suatu konfigurasi. Dengan melakukan konfigurasi *address list*, dapat membuat daftar alamat *ip* yang ingin ditandai tanpa dipengaruhi konfigurasi pada fitur yang lainnya. Fasilitas *address list* bisa dijumpai pada aplikasi *winbox mikrotik* dengan mengarahkannya ke menu *ip* > *firewall* bagian *address list*.

Fungsi yang lain dari *address list* adalah sebagai pengambilan keputusan pada *firewall* saat admin melakukan konfigurasi *rule* sehingga *address list* dan *rule* saling berhubungan (Fitriastuti & Utomo, 2014).

2.2.9 Penetrasi *Testing*

Penentrasi *Testing* adalah mekanisme keamanan pada sistem komputer atau jaringan yang berguna untuk mengevaluasi keamanan yang telah dirancang serta mengidentifikasi kelemahan, kerentanan, dan celah keamanan dari jaringan atau sistem komputer. Dalam mengidentifikasi keamanan dapat dilakukan dalam jaringan lokal maupun jarak jauh *(remote)*. Tujuan dilakukan penetrasi *testing* yaitu menentukan dan mengetahui jenis-jenis serangan yang dapat terjadi pada sistem dampak dari serangan tersebut karena pada sistem komputer atau jaringan terdapat kelemahan sistem keamanan.

Kerentanan pada aplikasi perangkat jaringan komputer seperti *router* akan memberikan akses bagi peretas untuk melakukan eksploitasi terhadap sistem secara perlahan dan dapat memungkinkan sistem yang dieksploitasi dapat diambil alih seluruhnya. Untuk melakukan penetrasi *testing*, dibutuhkan batasan-batasan dalam melakukan ujicoba sistem atau jaringan komputer secara hati-hati untuk mencegah gangguan dan agar memberikan metode serangan dapat diterapkan atau tidak (Cahyadi, 2012).



Gambar 2.3 Mekanisme Penetrasi *Testing*

Untuk penerapan teknik penetrasi *testing* terdapat teknik atau pola yang bertahap dengan penjelasan sebagai berikut :

1. *Reconnaissance*, yaitu dimana peretas melakukan identifikasi korban melalui informasi baik itu secara internal maupun eksternal. Secara internal contohnya melacak informasi korban melalui perangkat

korban yang terhubung satu jaringan dengan peretas, atau dapat dengan melakukan metode *social engineering.*

2. *Scanning*, setelah informasi korban didapatkan kemudian dianalisa informasi korban yang telah didapatkan lalu melakukan pencarian celah dan kelemahan sistem menjadi target.
3. *Gaining Access*, merupakan metode untuk mencari teknik yang dapat dilakukan setelah mengetahui celah keamanan yang berada di komputer atau sistem korban,
4. *Maintaining Access*, melakukan eksploitasi oleh peretas untuk mendapatkan informasi yang dibutuhkan pada sistem korban, kemudian menanamkan *shell*(kode program), yang bertujuan untuk mendapatkan *backdoor*. *Shell* yang ditanam peretas bertujuan untuk memberi akses kepada sistem korban terhadap peretas jika sewaktu-waktu peretas ingin melakukan eksploitasi kembali.
5. *Clearing Tracks*, pada saat menyerang korban, peretas akan meninggalkan jejak, agar aktivitas peretas tidak terlacak oleh *IT Security* peretas menghapus jejak ketika melakukan serangan. Untuk penghapusan jejak peretas membutuhkan sumber daya yang banyak baik dari segi pengetahuan serta keahlian.