# BAB II

# LANDASAN TEORI

## Profil STMIK Bumigora Mataram

### Sejarah Singkat berdirinya STMIK Bumigora Mataram

Komputer adalah produk teknologi untuk membantu menyelesaikan proses dengan tingkat kecepatan, keakuratan, dan kecermatan tinggi. Teknologi informasi sebagai teknologi yang memanfaatkan komputer dalam segala bentuk sehingga meningkatkan kegiatan (aktifitas) dari suatu kegiatan disegala bidang. Ilmu komputer merupakan kebutuhan yang mendesak untuk segera dipelajari dan dikembangkan. Salah satu wujud realisasinya adalah melalui pendidikan formal.

Tantangan tersebut segera dijawab dengan didirikannya “Yayasan Pendidikan Eksekutip Komputer” Akte Notaris Nomor : 39 tanggal 26 September 1987 dihadapan Notaris Abdullah, SH. di Mataram, diikuti dengan berdirinya Perguruan Tinggi Komputer dengan nama Sekolah Tinggi Teknologi Komputer Bumigora (STTK Bumigora).

Gagasan untuk mendirikan Perguruan Tinggi tersebut sesungguhnya telah dirintis sejak tahun 1987, namun karena ada kebijaksanaan baru mengenai Pendidikan Perguruan Tinggi Swasta (PTS) oleh Dirjen Dikti No. 2834/D/T/1987, tanggal 26 September 1987 dan Nomor : 086a/D/T 88, tanggal 16 Januari 1988, rencana tersebut tertunda dan baru dapat diwujudkan dalam tahun akademik 1989/1990 atas dasar :

* Surat Petunjuk dari Kopertis Wilayah VIII, Nomor : 117/Kop.8/N/1989 tanggal 11 Mei 1989 perihal Pendirian PTS Baru
* Rekomendasi Gubernur Kepala daerah Tingkat I Propinsi NTB Nomor : 421.4/873/008 tanggal 15 Juni 1989
* Rekomendasi Bupati Kepala Daerah Tingkat II Lombok Barat Nomor : 425.12/563 tanggal 26 Juni 1989.

Keberadaan lembaga pendidikan STMIK Bumigora tersebut kemudian semakin dimantapkan lagi dengan dikeluarkannya surat keputusan menteri pendidikan dan kebudayaan melalui Koordinator Perguruan Tinggi Swasta (KOPERTIS) Wilayah VIII yang memberi status terdaftar untuk jenjang studi Strata 0 (S0) program studi Diploma tiga (D3) Manajemen Informatika, berdasar surat keputusan nomor 0390/O/1991 tertanggal 22 Juni 1991 sekaligus merubah nama Sekolah Tinggi Teknologi Komputer (STTK) menjadi Sekolah Tinggi Manajemen Informatika dan Komputer **(STMIK) Bumigora Mataram**. Beberapa waktu kemudian, yaitu tanggal 8 Januari 1992 dengan surat keputusan nomor 026/O/1992, program diploma tiga (D3) Teknik Informatika mendapat status Terdaftar.

Memperhatikan sistem pengelolaan kedua program studi tersebut dinilai cukup baik, STMIK Bumigora diperkenankan pula untuk menyelenggarakan jenjang studi Strata Satu (S1) program studi Teknik Informatika dengan status Terdaftar berdasarkan surat keputusan nomor 608/DIKTI/EP/1993 tertanggal 23 Nopember 1993. Serta menunjuk surat dari Departemen Pendidikan dan Kebudayaan Direktorat Jendral Pendidikan Tinggi nomor 699/D4.II/1998 perihal penyelenggaraan Program D2 dan D1, sejak tahun Akademik 1998/1999 STMIK Bumigora Mataram membuka jenjang pendidikan D1 dan D2 Manajemen Informatika Komputer dengan status Terdaftar.

Sebagai perguruan tinggi yang taat pada peraturan pemerintah dan undang-undang tentang pendidikan tinggi, STMIK Bumigora secara tertib melaporkan laporan **EPSBED** (Evaluasi Program Studi Berbasis Evaluasi Diri) ke Direktorat Pendidikan Tinggi, serta melakukan **perpanjangan program studi** sesuai dengan waktu yang telah ditentukan. STMIK Bumigora juga sangat memperhatikan standar kualitas perguruan tinggi yang telah ditetapkan DIKTI dengan mengajukan **akreditasi** bagi program studi S1 Teknik Informatika, D3 Teknik Informatika, dan D3 Manajemen Informatika. Program Studi S1 Teknik Informatika telah terakreditasi dengan nilai C dengan nomor SK 015/BAN-PT/Ak-X/S1/VII/2007 tertanggal 10 Juli 2007. Program Studi D3 Teknik Informatika dan D3 Manajemen Informatika telah terakreditasi dengan nilai C dengan nomor SK 024/BAN-PT/Ak-VIII/Dpl-III/I/2009 tertanggal 10 Januari 2009.

Ke depan STMIK Bumigora bertekad untuk meningkatkan Akreditasi agar mutu penyelenggaraan pendididkan dan mutu lulusan dapat lebih diakui oleh masyarakat. Upaya yang dilakukan saat ini diantaranya adalah membentuk **Badan Penjaminan Mutu** sebagai pihak yang melakukan monitor dan evaluasi yang berkesinambungan terhadap kualitas layanan dan pengelolaan STMIK Bumigora. STMIK Bumigora telah pula memperoleh sertifikasi berstandar internasional **ISO 9001:2008** untuk **Pengelolaan Akademik pada tahun 2009**.

Sebagai perguruan tinggi yang ternama di Kopertis Wilayah VIII (Bali, NTB, dan NTT), STMIK Bumigora telah dipercaya untuk menerima hibah dari berbagai sumber yaitu : Hibah TPSDP ADB Loan pada tahun 2001 dengan jumlah dana yang dikelola sebesar 7,5 milyar rupiah dari Asian Development Bank, Hibah Kompetisi Peningkatan Mutu Pendidikan (PHK-PMP) dari DIKTI pada tahun 2006 untuk penguatan Laboratorium Multimedia dan Laboratorium Jairngan Komputer, dan Hibah Kompetisi PHK TIK K3 dari DIKTI pada tahun 2007 untuk membangun jaringan STMIK Bumigora dan INHERENT (*Indonesian Higher Education Network*).

STMIK Bumigora terlibat aktif di dalam berbagai program pemerintah seperti sebagai *provider* (pelaksana) Program Pendidikan Jarak Jauh Diploma III Teknik Komputer dan Jaringan (PJJ D3TKJ) yang berada dibawah SEAMOLEC serta telah memperoleh status sebagai *Local Academy* untuk *Java Education Network Indonesia* (JENI) dan *Cisco Computer Network Administrator* (CCNA). Disamping itu STMIK Bumigora berperan aktif dalam merancang *e-Government* NTB, melalui **Asosiasi Masyarakat Telematika NTB** yang bekerja sama dengan **Pemerintah Daerah NTB**. (Buku Panduan Mahasiswa Baru STMIK Bumigora Mataram 2009-2010)

### Fasilitas

Kampus STMIK Bumigora berdiri diatas tanah milik sendiri seluas 5600 m2 yang terdiri dari 3 buah gedung utama. Di dalam kampus terdapat fasilitas-fasilitas yang meliputi:

* + Ruang Perkuliahan

STMIK Bumigora mempunyai 8 ruang kelas, dengan luas total 560 m2, dan dapat menampung 420 orang . Setiap ruang kelas dilengkapi dengan kursi kuliah yang nyaman, AC atau kipas angin, dan LCD proyektor.

* + Perpustakaan

Perpustakaan STMIK Bumigora merupakan perpustakaan perguruan tinggi  terlengkap dan terbaik di NTB. Menyediakan  4000an judul buku dan sejumlah jurnal. Perpustakaan menyediakan pula beberapa unit computer untuk melihat katalog online.

* + Laboratorium Komputer, sejumlah 3 ruang, dengan kapasitas @ 20-40 ruang.
  + Laboratorium Jaringan, sejumlah 1 ruang, dengan kapasitas 10 orang
  + Laboratorium Bahasa, sejumlah 1 ruang, dengan kapasitas 20 orang.
  + Laboratorium Multimedia, sejumlah 1 ruang, dengan kapasitas 15 orang.
  + Ruang *Training Center*, sejumlah 1 ruang, dengan kapasitas 20 orang.
  + Ruang Seminar, sejumlah 1 ruang, dengan kapasitas 20 orang.
  + Aula Serba Guna

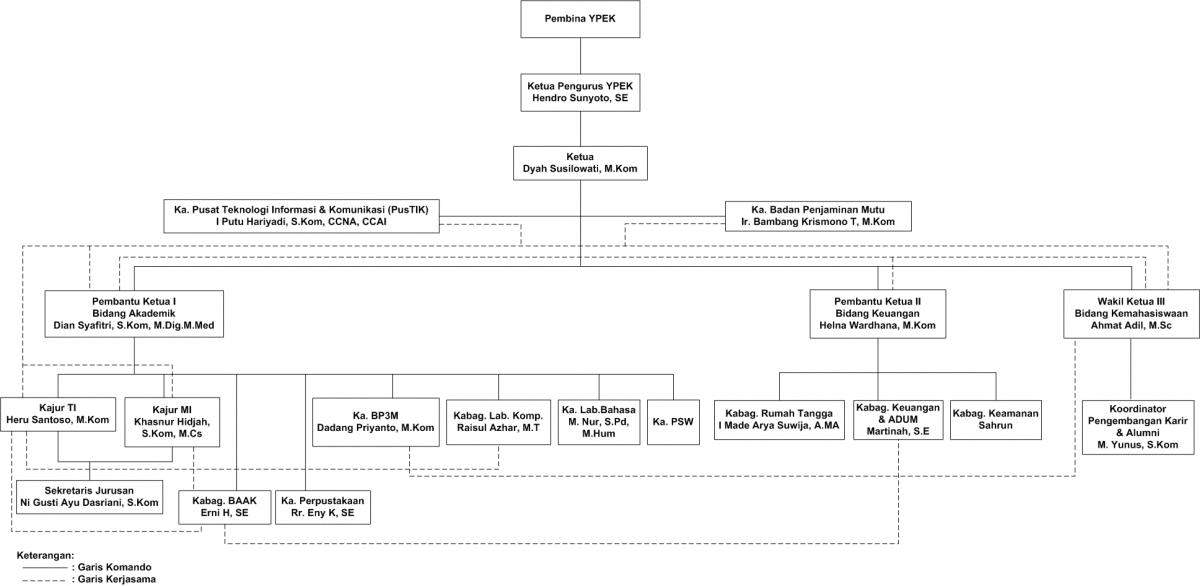
Aula STMIK Bumigora memiliki luas 240 m2 dan dapat menampung 200 orang untuk *event* seminar. Aula juga dipergunakan untuk perkuliahan.

* + Lapangan Olahraga
  + Mushola
  + *Video Conference*

Dengan peralatan video conference, STMIK Bumigora secara berkala mengadakan kuliah, seminar atau *meeting*  jarak jauh dengan perguruan tinggi lain seperti ITS, UGM, dan Universitas Gunadarma, serta DIKTI.

(STMIK Bumigora, 2011)

### Struktur Organisasi



**2.1 Gambar Struktur Organisasi STMIK Bumigora Mataram**

(sumber: website STMIK Bumigora Mataram, www.stmikbumigora.ac.id)

## Jaringan Komputer

Jaringan komputer adalah kumpulan dua atau lebih komputer yang saling berhubungan untuk melakukan komunikasi data. Komunikasi data yang bisa dilakukan melalui jaringan komputer dapat berupa data teks, gambar, video, dan suara (Daryanto, 2010). Sementara menurut (Sofana, 2008), Jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *printer, hub,* dan sebagainya) yang saling terhubung satu sama lain melalui media prantara.

Berdasarkan pengertian diatas dapat simpulkan bahwa jaringan komputer adalah merupakan kumpulan komputer dan alat-alat lain (*software/hadware*) untuk melakukan komunikasi data yang saling berhubungan menggunakan media komunikasi tertentu.

### Terminologi Jaringan Komputer

Komputer dalam jaringan dapat terkoneksi melalui kabel,serat optik, gelombang mikro, *wereless* atau satelit komunikasi (Sopandi, 2010). Interkoneksi antar computer ini dibagi menjadi 3 (tiga) tipe berdasarkan cakupan wilayah dan kompleksitas antara lain:

#### Local Area Network (LAN)

*Local Area Network* atau disingkat LAN adalah jaringan yang bersifat internal dan biasanya milik pribadi di dalam sebuah prusahaan kecil atau menengah dan bias anya berukuran sampai beberapa kilometer.

#### Metropolitan Area Network (MAN)

*Metropolitan Area Network* (MAN) adalah jaringan yang mencakup kantor-kantor perusahaan yang letaknya berdekatan atau antar sebuah kota dan dapat dimanfaatkan untuk keperluan pribadi (swasta) atau umum.

#### Wide Area Network (WAN)

*Wide Area Network* (WAN) adalah jaringan yang mencakup wilayah geografis yang lebih luas, seringkali mencakup sebuah negara bahkan benua .

### Transmission Control Protocol/Internet Protocol (TCP/IP)

Menurut (Sopandi, 2010), TCP/IP didefinisikan sebagai “sekumpulan protokol yang didesain untuk melakukan fungsi-fungsi komunikasi data pada *Wide Area Network* (WAN) (p.60)". *Transmission Control Protokol/Internet Protocol* (TCP/IP) juga bisa didefinisikan sebagai seperangkat protokol yang digunakan oleh sebagian besar lingkungan jaringan saat ini. TCP/IP telah di adopsi sebagai protokol internet dan diigunakan pada jaringan skala kecil, menengah, dan besar (clarke, 2009). Disisi lain, *Transmission Control Protokol/Internet Protocol* (TCP/IP) adalah merupakan format standar untuk transmisi data dalam paket-paket dari satu computer ke komputer lain. Dua bagian dari TCP/IP adalah TCP , yang berkaitan dengan pembangunan paket data, dan IP, yang rutenya dari mesin ke mesin (Downing & Covington, 2009).

Berdasarkan pada penjelasan diatas maka dapat disimpulkan TCP/IP adalah seperangkat protokol atau koleksi dari protokol yang merupakan format standar untuk transmisi paket-paket dari satu komputer ke komputer lain melalui rute tertentu dan telah digunakan oleh sebagian besar lingkungan jaringan saat ini. Seperti penjelasan diatas, TCP merupakan protokol yang berkaitan dengan pembangunan paket data dan IP merupakan protokol yang salah satu headernya berisi tentang rute terhadap komputer tujuan dan sumbernya. Oleh karena itu spesifikasi TCP/IP dapat dibagi menjadi 2 (dua) yaitu TCP dan IP.

Menurut (Daryanto, 2010), terdapat suatu lapisan (layer) yang memiliki tugas spesifik serta memiliki protokol tersendiri. Adapun rincian fungsi masing-masing layer arsitektur TCP/IP adalah sebagai berikut :

1. Physical Layer (Lapisan fisik)

Merupakan lapisan terbawah yang mendefinisikan besaran fisik seperti media komunikasi, tegangan, arus, dll. TCP/IP bersifat fleksibel sehingga dapat mengintegralkan berbagi jaringan dengan media fisik yang berbeda-beda.

1. Network Acces Layer

Protokol pada layer ini menyediakan media bagi sistem untuk mengirimkan data ke *device* lain yang terhubung secara langsung. Layer ini juga memberikan service untuk mendeteksi dan koreksi kesalahan dari data yang ditransmisikan.

1. Internet Layer

Pada jaringan internet, lapisan ini bertugas untuk menjamin agar suatu paket yang dikirimkan dapat menemukan tujuannya dimanapun berada. Layer ini memiliki peranan penting dalam mewujudkan internetworking yang meliputi wilayah luas.(*worldwide Internet*).

Beberapa tugas penting pada layer ini adalah :

1. Addressing, yakni melengkapi setiap datagram dengan alamat internet dari tujuan. Alamat pada protokol inilah yang dikenal dengan *Internet Protokol Address* (IP Adderess).
2. Routing, yakni menentukan kemana datagram akan dikirim agar mencapai tujuan yang diinginkan. Sebagai protokol yang bersifat connectionless. Proses routing sepenuhnya ditentukan oleh jaringan. Pengirim tidak memiliki kendali terhadap paket yang dikirimkan untuk bisa mencapai tujuan tetapi router yang menentukan dalam penyampaian datagram dari penerima ke tujuan
3. Transport Layer

Pada *Transport Layer* terdapat dua buah protokol yang digunakan yaitu :

1. *Transper Control Protokol* (TCP)

TCP memiliki fungsi *flow control yaitu* suatu teknik untuk menjamin bahwa entitas pengirim tidak akan membanjiri data kepada entitas penerima, dan *error detection* yang berarti kegiatan untuk memastikan bahwa data yang diterima sama dengan data yang diterima,dan bersifat *connection oriented* berarti sebelum melakukan pertukaran data, dua aplikasi pengguna *TCP* harus melakukan hubungan *(handshake)* terlebih dahulu.

1. *User Datagram Protokol* (UDP)

UDP juga menyediakan layanan pengiriman datagram yang bersifat connection oriented, tanpa dilengkapi deteksi dan koreksi kesalahan. Keuntungan penggunaan UDP adalah kecepatannya karena pada UDP tidak ada acknowledgements, sehingga traffic yang lewat jaringan rendah, dan itu yang membuat UDP lebih cepat dari pada TCP.

1. Aplication Layer

Merupakan Lapisan terakhir yang berfungsi mendefinisikan aplikasi-aplikasi yang dijalankan pada jaringan. Pada lapisan ini terdapat banyak protokol sesuai dengan banyaknya aplikasi TCP/IP yang dapat dijalankan.

### Internet protokol

*Internet Protocol* (IP) adalah protokol yang mengatur bagaimana suatu data dapat dikenal dan dikirim dari satu computer ke computer lain (Sofana, 2008).

*Internet Protocol* (IP) merupakan inti dari protokol TCP/IP seluruh data yang berasal dari protokol pada layer diatas IP harus dilewatkan, diolah oleh protokol IP, dan dilanjutkan sebagai paket IP agar sampai ke tujuan (Setiawan, 2013).

*Internet Protokol (IP)* pada awalnya dirancang untuk memfasilitasi hubungan antara beberapa organisasi yang tergabung dalam departemen pertahanan Amerika yaitu *Advanced Research Project Agency (ARPA)*. Sebelum terciptanya *Internet Protocol,* jaringan memiliki peralatan, dan protokol tersendiri yang digunakan untuk saling berhubungan. Perangkat jaringan yang dikeluarkan oleh vendor A tidak dapat berkomunikasi dengan perangkat jaringan dari vendir B, begitu pula sebaliknya. Karena dengan hal tersebut, maka dibuatlah suatu protokol yang dapat digunakn secara umum untuk menyatukan berbagai perbedaan dalam penggunaan perangkat yang terhubung di dalam jaringan.

Protocol IP memiliki beberapa fungsi utama (Sofana, 2008), yaitu:

1. Mendefinisikan paket yang menjadi unit satuan terkecil pada transmisi data di *Internet.*
2. Memindahkan data antara *Transport Layer* dan *Network Interface Layer.*
3. Mendefinisikan skema pengelamatan *Internet* atau IP *address.*
4. Menentukan *routing* paket.
5. Melakukan pragmentasi dan penyusunan ulang paket.

### Internet Protocol Address versi 4 (IPv4)

*IP Address* atau alamat IP (dalam hal ini IPv4) adalah alamat yang digunakan untuk mengidentifikasi interface jaringan pada host komputer. Alamat IP merupakan kombinasi bilangan biner 32 bit yang terdiri dari Network ID dan Host ID, serta dipisahkan oleh tanda pemisah berupa titik setiap 8 bit-nya. Tiap 8 bit ini disebut sebagai oktet.

Alamat IPv4 terbagi menjadi 5 bagian, yaitu kelas A, kelas B, kelas C, kelas D, dan kelas E. Namun kelas yang umum digunakan adalah kelas A, B, dan C. Untuk kelas D digunakan untuk alamat multicast yang tidak memiliki network ID, dan Host ID, sedangkan Kelas E digunakan untuk keperluan khusus, seperti untuk riset. Pembagian kelas dalam IPv4 dapat dilihat pada table berikut:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kelas | Format (a.b.c.d) | Address Range | Number of Network | Number of Host per Network |
| A | 0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhhh | 1.0.0.1 – 126.255.255.255 | 126 | 16.777.214 |
| B | 10nnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh | 128.0.0.1 – 192.255.255.255 | 16.385 | 65.536 |
| C | 110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhhh | 192.0.1.1 – 239.255.255255 | 2.096.152 | 254 |
| D | 1110nnnn.nnnnnnn.nnnnnnnn.nnnnnnnn | 224.0.0.0 – 239.255.255.255 | - | - |
| E | 1111nnnn.nnnnnnnn.nnnnnnnn.nnnnnnnn | 240.0.0.0 – 254.255.255.255 |  |  |

Tabel 2.1 Pembagian Kelas Alamat IP

## Keamanan Jaringan

Keamanan jaringan adalah bidang yang komplek dan terus berkembang. Dalam keamanan jaringan harus tetap memantau ancaman baru, solusi, proaktif dalam menilai resiko dan selalu melindungi jaringan. Langkah pertama untuk memahami keamanan jaringan adalah mengenali ancaman actual kedalam jaringan. Pemahaman dasar tentang terminologi juga sangat penting (easttom, 2012).

### Terminologi Keamanan Jaringan

Dalam *Network Security* sangat penting untuk mengetahui beberapa terminology keamanan jaringan dasar. Adapun beberapa terminology keamanan jaringan dasar adalah sebagai berikut (easttom, 2012).

#### Terminologi hacker

1. Hacker

*Hacker* adalah seseorang yang ahli dalam sistem tertentu dan hanya ingin mempelajari lebih lanjut tentang sistem. *Hacker* akan mencari kelemahan dalam system kemudian akan berusaha untuk memperbaikinya. Hacker dibedakan menjadi 3 (tiga) yaitu, (Easttom,2012) :

1. *White Hat Hacker* adalah seseorang yang mencari kelemahan, kemudian akan memberitahukan kelemahan tersebut ke perusahaan. *White Hat Hacker* juga memiliki sertifikasi yaitu *Certified Ethical Hacker tes.*
2. *Black Hat Hacker* adalah orang yang biasanya mempunyai tujuan untuk membahayakan system. Misalnya mencuri data, menghapus atau merubah. *Black Hat Hacker* biasanya disebut *Crackers.*
3. *Gray Hat Hacker* adalah orang yang biasanya taat hokum. Tetapi kadang-kadang juga melakukan penjelajahan secara illegal.
4. Script Kiddies

*Script Kiddies* adalah istilah untuk seseorang yang menyebut dirinya *hacker* tetapi tidak memiliki keahlian. Orang seperti ini biasanya menggunakan utilitas yang didownload dari *internet.*

1. Sneakers

*Sneakers* adalah istilah unutuk orang yang diberikan ijin unutuk menerobos kesuatu system guna untuk mengetahui kelemahan dari sistem tersebut.

1. Phreaking

*Phreaking* adalah suatu tindakan dengan menggunkan cara yang ilegal untuk membobol system telepon dengan tujuan untuk tidak mebayar telekomunikasi.

#### Terminologi Professional Terms

*Professional Terms* adalah istilah dalam penghalang mengenai perangkat yang digunakan, prosedur dan kebijakan. Adapun terminology *professional terms* adalah sebagai berikut (easttom, 2012) :

1. *Security Device* adalah suatu perangkat keamanan, dan yang paling dasar dari perangkat keamanan ini adalah *firewall. Firewall* adalah penghalang antaran jaringan dalam dengan jaringan luar. Beberapa perangkat yang bisa dijadikan *firewall*  seperti *server, router* dan perangkat lunak yang berjalan di dalam mesin computer. Konsep kerja *firewall* semuanya sama yaitu memfilter lalu lintas yang masuk dan keluar. Sebuah server proxy juga sering digunakan sebagai *firewall.*
2. *Security Activities* adalah kegiatan keamanan yang paliing dasar seperti *otentikasi* *username* dan *password.*

### Proses hacking

*Hacking* merupakan seni tersendiri yang melibatkan proses mencari serpihan-serpihan informasi yang berterbaran dimana-mana dan seolah-olah tidak ada hubungannya satu sama lainnya. Antara *hacker*. *Cracker* dan *Security Professional* perbedaannya sangat tipis, karena sama-sama menggunakan tools yang sama hanya perbedaannya pada cara pandang (*view*) terhadap berbagai hal, misalnya mengenai kegiatan *probing* atau *port scanning* *system* orang lain dapat dilegalkan atau tidak (utomo, 2009).

Adapun langkah-langkah untuk memberi gambaran tentang keseluruhan proses hacking adalah sebagai berikut (utomo, 2009):

* 1. Footprinting, Mencari rincian informasi terhadap system-system untuk dijadikan sasaran, mencakup pencarian informasi dengan *search engine, whois*, dan DNS *zone transfer*.
  2. Scanning. Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan port scan.
  3. Enumeration. Telaah intensif terhadap sasaran, yang mencari *user account* absah, *network resource* and *share*, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.
  4. Gaining Access. Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas *password*, menebak *password*, serta melakukan *buffer overflow*.
  5. Escalating Privilege. Bila baru mendapatkan *user password* di tahap sebelumnya, di tahap ini diusahakan mendapat *privilese admin* jaringan dengan *password cracking* atau *exploit* sejenis *getadmin*, *sechole*, atau *lc\_messages*.
  6. Pilfering. Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke *trusted system*. Mencakup evaluasi *trust* dan pencarian *cleartext password* di *regiatry*, *config file*, dan *user* data.
  7. Covering Tracks. Begitu kontrol penuh terhadap system diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam *rootkit* dan *file streaming*.
  8. Creating Backdoors. Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu, menjadwalkan *batch job*, mengubah *startup file*, menanamkan *service* pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan trojan.
  9. Denial of Service. Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik-teknik ICMP, *Supernuke*, *land/latierra*, *teardrop, bonk, newtear, trincoo*, dan lain-lain.

## Mikrotik RouterOs

Mikrotik RouterOs adalah system operasi *Linux base* yang diperlukan sebagai *network* router. Didesain untuk memberikan kemudahan bagi penggunanya. Administrasinya bisa dilakukan melalui *Windows Application* (WinBox). *Webbrowser* serta via *Remote Shell* (telnet dan SSH). Selain itu instalasi dapat dilakukan pada Standar computerPC. PC yang akan dijadikan router mikrotikpun tidak memerlukan resource yang cukup besar untuk penggunaan standard, minsalnya hanya sebagai *gateway.* Untuk keperluan beban besar (Network yang kompleks, routing yang rumit.dll) disarankan untuk mempertimbangkan pemilihan *resource* PC yang memadai (Herlambang, et al. 2008)

## Pre Hypertext Processor (PHP)

Pre Hypertext processor (PHP) adalah bahasa pemrograman script disisi sercer yang dibangun khusus untuk pengembangan web site dan bisa digabungkan dengan Hypertext Markup Language (HTML). Pada awalnya PHP merupakan kepanjangan dari Personal Home Page dan dibangun oleh Rasmus Lerdorf pada tahun 1995. Selanjutnya Rusmus merilis kode sumber PHP untuk umum dan open source sehingga banyak pemrograman yang tertarik untuk ikut mengembangkan PHP (ullman, 2009).

Pada bulan November tahun 1997, PHP/FI 2.0 dirilis dengan mengimplementasikan bahasa pemrograman C dan pada tahun yang sama sebuah perusahaan bernama Zend menulis ulang *interpreter* PHP menjadi lebih bersih, lebih baik dan lebih cepat. Kemudian pada bulan Juni tahun 1998, Zend meresmikan penulisan ulang kode Sumber PHP dengan nama resmi PHP 3.0 dan mengganti singkatan PHP dengan akronim ulang *PHP: Hypertext Preprocessor*.

PHP yang dirilis oleh Zend memiliki kemampuan sangat handal dalam membangun aplikasi web yang kompleks dengan kecepatan dan stabilitas yang tinggi. PHP bisa dijalankan diberbagai platform sistem operasi seperti Microsoft Windows, Linux, Macintosh, Sun Solaris, dan sebagainya. Selain itu kemampuan PHP yang bisa digabungkan dengan HTML menjadikan PHP sebagai salah satu bahasa pemrograman terpopuler untuk pembangunan web site dinamis saat ini.

### Codeigniter Framework

Codeigneter adalah sebuah *Framework* berbasis PHP dengan ukuran sangat kecil yang dibangun untuk pemrograman PHP yang membutuhkan tookit sederhana dan elegan dalam membangun web site dengan fitur lengkap (Ellislab Incorporated, 2011)

Pembangun PHP yaitu Rasmus Lerdorf menyarankan untuk menghindari PHP Framework dalam membangun aplikasi web karena waktu eksekusi PHP Framework lebih lambat. Namun dalam *Free and Open Source Conference* (FrosCon) bulan Agustus tahun 2008. Rusmus Lerdorf menyatakan bahwa dia menyukai CodeIgneter karena lebih cepat dan lebih ringan. Selain cepat dan lebih ringan, CodeIgneter memiliki docementasi yang lengkap dan handal. Hal ini yang menjadikan CodeIgneter sebagai salah satu PHP Framework favorite yang memiliki pengguna yang paling banyak (lardorf, 2008)

### Spark

Spark adalah package manager untuk CodeIgneter. Dengan spark kita bisa menginstall library yang kita perlukan untuk aplikasi kita dengan cepat dan mudah. Dengan spark, kita telah disediakan daftar package yang sudah teruji oleh komunitas, kita bisa dengan mudah dan cepat mencari, menginstall dan menggunakannya didalam aplikasi kita. Ini adalah perubahan yang cukup signifikan yang disediakan untuk defelover CodeIgneter terutama yang berkaitan dengan masalah koleksi library. Dengan adanaya spark juga semakin memudahkan defelover untuk memanage library di dalam aplikasi ([www.getsparks.org](http://www.getsparks.org)).

### Twitter Bootstrap

Twitter Bootstrap merupakan frameworkCSS yang dilengkapi oleh pustaka JavaScript dalam bentuk sederhana dan intuitif dengan front-end yang kuat untuk mempercepat dan mempermudah dalam pengembangan sebuah web (Otto & Thornton, 2011). Twitter Bootstrap memiliki banyak komponen antara lain, scaffolding layout, Dropdown, Button Groups, Navbar, Pagination dan lain-lain. Beberapa komponen-komponen tersebut memiliki kombinasi dengan pustaka JavaScript sehingga antar muka pada halaman web menjadi lebih interaktif dan intuitif. Komponen-komponen Twitter Bootstrap dirancang untuk dapat menerima perubahan warna dan layout, sehingga pemrogram bisa menyesuaikan rancangan antarmuka web yang dibangun menjadi lebih intuitif.

### JavaScript Objek Notation (JSON)

JavaScript Objek Notation (JSON) adalah format data yang ringan untuk pertukaran data. Hal ini didasarkan pada subset notasi objek literal javascript, dapat digunakan untuk pertukaran data antara program yang ditulis dalam semua bahasa pemrograman modern (Crockford, 2008)

JSON merupakan format teks yang tidak bergantung pada bahasa pemprograman apapun karena menggunakan gaya bahasa yang umum digunakan oleh programmer keluarga C termasuk C, C++, C#, Java, php, JavaScript, Perl, Python dan lain-lain. Oleh karena sifat-sifat tersebut, menjadikan JSON ideal sebagai bahasa pertukaran-data

### Asynchronous JavaScript and XML (AJAX)

Ajax merupakan salah satu teknik pemrograman berbasis web untuk menciptakan aplikasi web yang interaktif. Tujuannya adalah dalam melakukan pertukaran data dengan server dapat dilakukan dibelakang layar, sehingga halaman web tidak harus dibaca ulang secara keseluruhan setiap kali seorang pengguna melakukan perubahan. Hal ini akan meningkatkan interaktivitas, kecepatan, dan usability.

## MySQL

MySQL (dibaca: *mai-se-kyu-el*) merupakan software yang tergolong sebagai DBMS (Database Management System) yang bersifat *open source*. *Open source* menyatakan bahwa aplikasi ini dilengkapi dengan *source code* (kode yang dipakai untuk membuat MySQL), selain itu tentu saja bentuk *excutable*-nya atau kode yang dapat dijalankan secara langsung dalam sistem operasi dan dapat diperoleh dengan cara mengunduh di Internet secara gratis (Kadir, 2008).

MySQL awalnya dibuat oleh perusahaan konsultan bernama TcX yang berlokasi di Swedia. Saat ini pengembangan MySQL berada di bawah naungan perusahaan MySQL AB. Adapun aplikasi MySQL dapat diunduh di situs resmi MySQL([www.mysql.com](http://www.mysql.com)). Sebagai software DBMS, MySQL memiliki beberapa fitur diantaranya (Kadir, 2008):

1. Multiplatform

MySQL tersedia pada beberapa platform diantaranya Windows, Linux MacOS, Unix dan lain-lain.

1. Handal, cepat dan mudah digunakan

MySQL tergolong dalam database server yang handal, dapat menangani database yang besar dengan kecepatan yang tinggi, mendukung banyak sekali fungsi untuk mengakses database dan sekaligus mudah untuk digunakan. Berbagai *tools* pendukung juga tersedia seperti *MySQL workbench, phpMyadmin, case studio* dan banyak yang lainnya. Perlu diketahui, MySQL dapat menangani ukuran yang berukuran *terabyte*. Namun, ukuran yang sesungguhnya sangat bergantung pada sistem operasi, sebagai contoh pada system operasi Ubuntu 10.04, batasan ukuran file sebesar 16 terabyte.

1. Jaminan keamanan akses

MySQL mendukung pengamanan database dengan berbagai kriteria pengaksesan. Sebagai gambaran, dimungkinkan untuk mengatur user tertentu agar bisa mengakses data yang bersifat rahasia, sebagai contoh data gaji pegawai dan otentikasi database yang boleh digunakan oleh user yang lain.

1. Dukungan SQL

MySQL mendukung perintah SQL (*Structured Query Language*). Sebagai mana diketahui, SQL merupakan standar dalam pengaksesan database relasional. Pengetahuan akan SQL akan memudahkan siapa pun untuk menggunakan MySQL.

MySQL juga mendukung konektivitas ke berbagai bahasa pemrograman. Sebagai contoh, dengan menggunakan ODBC (*Open Database Connectivity*), database yang ditangani MySQL dapat diakses melalui program yang dibuat dengan Visual Basic. MySQL juga mendukung client berbasis Java untuk berkomunikasi dengan database MySQL melalui JDBC (*Java Database Connectivity*). MySQL juga bisa diakses melalui aplikasi berbasis web misalnya, dengan menggunakan bahasa pemrograman PHP, antara MySQL dan PHP bisa melakukan komunikasi dengan mengunakan fungsi (*MySQL\_connect()*) untuk melakukan konektivitas yang sudah disediakan pada bahasa pemrograman PHP.

## Netcut

Menurut Inanta (2010), Istilah netcut diambil dari kata Net yang artinya internet, dan Cut yang dalam bahasa inggrisya yaitu memotong. Jadi pengertian Netcut itu sendiri adalah memotong jaringgan internet. Dimana orang yang menggunakan jaringan internet seperti Wi-Fi / LAN, jaringgan yang digunakan pengguna dapat dipotong menggunakan software ini.

*NetCut* adalah suatu aplikasi pemotong *bandwidth* yang berorientasi pada jaringan LAN/Hotspot. Yang menjadikan dirinya sebagai *gateway* dan bebas untuk mengatur *trafick* *in* dan *out*. Metode *Attack*-nya adalah mengirimkan *ping* *request* terlebih dahulu ke dalam *IP*-*Table* (rentang *IP* blok) untuk kemudian mengirimkan *request random MAC* (*Dynamic based DHCP*) kepada *IP* yang dituju (*IP* yg aktif) dengan mengacaukan alamat *MAC* *Address* pada *request one by one* menuju *gateway*. *NetCut* men-*scan* jaringan dengan membuat *IP-Table* sesuai dengan kondisi *netmask* atau *scope* pada suatu jaringan sehingga *NetCut* mampu untuk menampilkan *IP* aktif beserta *MAC*-*Address* nya pada jaringan victim-nya. Misalkan *IP LAN* jaringan tersebut menggunakan slash (/) 24 = *254 ip-address*, maka *NetCut* akan melakukan *scanning* *IP* pada rentang *IP* yang dimaksud tersebut diatas dan memunculkannya ke dalam *list* *IP* beserta *MAC*-*address* komputer yang aktif untuk kemudian melakukan *action*-nya. Efek yang ditimbulkan dari jenis serangan *NetCut* ini adalah, koneksi yang telah terbagi kepada IP pemakai (koneksi ke user) akan terputus dan beralih kepada si pengguna NetCut. Dengan cara melakukan spoofing kepada ARP (*Address Resolution Protocol*) *IP* target nya

## Port Scanning

Menurut (ari, 2009) *Port scanning* adalah sebuah aktivitas untuk mendapatkan informasi yang menyeluruh mengenai status *port* (biasanya *port* TCP) pada sebuah *host*. Dengan *port scanning*, seseorang dapat mengetahui *port-port* mana saja yang terbuka pada sebuah *host*.

## Komunikasi jaringan protokol

### Hypertext Transper Protocol (HTTP)

HTTP adalah suatu protokol yang digunakan untuk mentransfer dokumen/halaman dalam **World Wide Web (WWW)**. HTTP mendefinisikan bagaimana suatu pesan dapat diformat dan dikirimkan dari client ke server atau sebaliknya. Pengembangan standar HTTP dilaksanakan oleh Konsorsium World Wide Web (World Wide Web Consortium/W3C) dan juga Internet Engineering Task Force (IETF), yang menghasilkan publikasi beberapa dokumen Request for Comments (RFC), antara lain RFC 2616 yang mendefinisikan tentang HTTP/1.1 (Septian, 2011). HTTP merupakan sebuah protokol untuk meminta/menjawab antara klien dan server. Sebuah klien HTTP (seperti *web browser*), biasanya memulai permintaan dengan membuat hubungan ke port tertentu di sebuah server *Web hosting* tertentu (biasanya *port* 80). Klien yang mengirimkan permintaan HTTP juga dikenal dengan *user agent*. Server yang meresponsnya, yang menyimpan sumber daya seperti berkas HTML dan gambar, dikenal juga sebagai *origin server*. Di antara user agent dan juga *origin server*, bisa saja ada penghubung, seperti halnya *proxy*, *gateway*, dan juga *tunnel*. Sumber yang hendak diakses dengan menggunakan HTTP diidentifikasi dengan menggunakan Uniform Resource Identifier (URI), atau lebih khusus melalui Uniform Resource Locator (URL), menggunakan skema URI http: atau https:.

Adapun menurut Idris (2010), Biasanya untuk mentransfer dokumen dalam World Wide Web (WWW), menggunakan HTTP. Protokol ini adalah protokol ringan, tidak berstatus dan generik yang dapat dipergunakan dalam berbagai macam tipe dokumen. Namun dalam protokol ini segi keamanan data yang dikirim belum diperhatikan, data yang dikirimkan tidak dienkripsi, sehingga data yang dikirim rawan, dapat dibaca/dirusak oleh orang yang tidak diizinkan.

### Hypertext Transper protocol Secure (HTTPS)

HTTPS merupakan bentuk protokol yang aman karena segala perintah dan data yang lewat protokol ini akan di-encryp dengan berbagai format sehingga sulit untuk dibajak isinya maupun dilihat perintah-perintah yang di-eksekusi (Arjuna, 2011). Adapun pengertian HTTPS menurut Glossarium (n.d), bahwa HTTPS memiliki pengertian sama dengan HTTP tetapi dengan alasan keamanan (security), HTTPS memberi tambahan Secure Socket Layer (SSL). Teknologi HTTPS protokol mencegah kemungkinan "dicurinya" informasi penting selama proses komunikasi berlangsung antara user dengan web server (atau sebaliknya). Secara teknis, website yang menggunakan HTTPS akan melakukan enkripsi terhadap informasi (data) menggunakan teknik enkripsi SSL. Dengan cara ini meskipun seseorang berhasil "mencuri" data tersebut selama dalam perjalanan user web server, orang tersebut tidak akan bisa membacanya karena sudah diubah oleh teknik enkripsi SSL. HTTPS ditemukan oleh Netscape Communication Corporation untuk menyedaikan otentikasi dan komunikasi tersandi. Selain menggunakan komunikasi tersandi HTTPS juga menyediakan data sesi menggunakan protocol SSL (Secure Socket Layer) yang dimana bekerja pada port HTTPS adalah 443.

## Nmap

Nmap adalah sebuah tool gratis yang berguna untuk melakukan scan port atau tool port scanner. Sebagian besar type dari scan yang dilakukan nmap adalah sebagai berikut (easttom, 2012) :

1. Ping Scan

*Ping Scan* adalah proses yang paling simple untuk mengirim ping ke port target. Banyak administrator jaringan memblokir port paket-paket ICMP untuk menghentikan terjadinya *ping scan.*

1. Connect Scan

*Connect Scan* adalah sebagian besar yang paling banyak digunakan karena dapat dipercaya.

1. SYN Scan

SYN *Scan* serupa denganSYN *Flood DoS Attac.* Dalam *scan* ini mengirim paket data hanya mengirim satu paket per *port*. Kemudian tidak akan pernah merespon ketika system mengirimkan SYN/SYN

1. FIN Scan

*FIN Scan* adalah proses penyelesain dalam koneksi atau proses untuk mengakhiri koneksi.

## Open Secure Socket Layer (OpenSSL)

*OpenSSL* merupakan *tool* untuk enkripsi atau desikripsi atau kriptografi dengan mengimplementasikan *Secure Socket Layer* (*SSL*) dan *Protocol Transport Layer Security*, dengan ditulis dalam bahasa pemrograman C dan diimplementasikan untuk fungsi kriptografi basic. OpenSSL sendiri tersedia dalam berbagai sistem operasi seperti : *Unix*, *Solaris*, *Linux*, *Mac OS X*, serta *Open BSD* (Triwanda, 2011). *SSL* merupakan suatu enkripsi yang mendukung beberapa protokol enkripsi seperti pada *internet* yang bekerja pada protokol *plain text* atau *HTTP* sehingga menghasilkan protokol *HTTPS*.

Adapun dalam artikel Triwanda (2011), berikut merupakan rilis dari *OpenSSL* (terakhir modifikasi 17 Maret 2011 dari *wikipedia.org*), antara lain :

* *OpenSSL 1.0.0 was released on March 29, 2010;*
* *OpenSSL 0.9.8 was released on July 05, 2005;*
* *OpenSSL 0.9.7 was released on December 31, 2002;*
* *OpenSSL 0.9.6 was released on September 25, 2000;*
* *OpenSSL 0.9.5 was released on February 28, 2000;*
* *OpenSSL 0.9.4 was released on August 9, 1999;*
* *OpenSSL 0.9.3 was released on Mei 25, 1999;*
* *OpenSSL 0.9.2b was released on March 22, 1999;*
* *OpenSSL 0.9.1c was the first released on Decembert 9, 1998;*

Berikut algoritma-algoritma yang mendukung dari *tool OpenSSL* adalah, antara lain (Triwanda, 2011).

* 1. *Chipers*

Adapun berikut algoritma enkripsi yang terdapat pada penggunaan *tool Chipers OpenSSL* : *AES*, *Blowfish*, *Calelia*, *SEED*, *CAST-128*, *DES*, *RC2*, *RC4*, *RC5*, *Triple DES*, *GOST 28147-89.*

* 1. *Cryptographic Hash Fuctions*

Adapun berikut algoritma enkripsi yang terdapat pada penggunaan *tool Cryptographic Hash Fuctions OpenSSL* : *MD5*, *MD2*, *SHA-1*, *SHA-2*, *RIPEMD-160*, *MDC-2*, *GOST R 34.11-94*.

* 1. *Public-key Cryptography*

Adapun berikut algoritma enkripsi yang terdapat pada penggunaan *tool Public-key Cryptography OpenSSL* : *RSA*, *DSA*, *Diffie–Hellman key exchange*, *Elliptic curve*, *GOST R 34.10-2001*.

## Port

*Port* adalah sebuah jalur untuk komunikasi tertentu pada komputer yang satu dengan yang lainnya. Menggunakan media koneksi seperti NIC, kabel dan membawa informasi berupa *biner* menggunakan protokol tertentu (easttom, 2012).

## FileZilla

FileZila adalah polder untuk