BAB II

KAJIAN PUSTAKA

2.1. Teori Dasar

Bab ini akan membahas mengenai teori-teori dasar yang mendukung pendekatan dan pemecahan masalah, serta menjelaskan penelitina terdahulu yang telah dilakukan oleh peneliti sebelumnya.

2.1.1. Jaringan Komputer

Jaringan komputer adalah sebuah kumpulan dari komputer, printer, dan perangkat lainnya yang terhubung dalam suatu kesatuan dan membentuk satu sistem tertentu (Maslan & Wangdra, 2012:2). Informasi bergerak melalui kabel atau tanpa kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar informasi (data), mencetak data pada printer yang sama dan dapat secara simultan menggunakan program aplikasi yang sama. Adapun beberapa manfaat yang dapat kita rasakan dari terbentuknya jaringan komputer yaitu sebagai berikut:

1. Dapat saling sharing file

   Pengguna dapat saling sharing file kesesama komputer teman atau rekan kerja, baik itu menggunakan media kabel atau nirkabel, dan sewaktu melakukan sharing pengguna bisa mengatur hak akses user pada saat file akan digunakan.

2. Tukar menukar data, baik data suara, gambar dan video

Tukar menukar data ini maksudnya adalah kita bisa melakukan kirim file sesama teman dan rekan kerja dalam waktu yang sangat cepat, baik menggunakan media kabel ataupun media nirkabel. Contoh pemanfaatan *Bluetooth* dan WIFI.

3. Memungkinkan dapat memakai printer secara bersamaan

Untuk penghematan biaya maka dalam manajemen perusahaan,bahwa tiap-tiap departemen tidak diharuskan untuk menggunakan printer masing-masing, karena bisa saling berbagi printer.

4. Dapat menghemat biaya

Segala suatu pekerjaan dapat dikerjakan oleh satu alat saja, sehingga biaya pengeluaran dapat di minimalkan. Karena jaringan komputer segala perangkat keras bisa dihubungkan asalkan teknologi yang digunakan mendukung.

5. Efisiensi kerja meningkat

Segala pekerjaan dapat di tangani dengan memanfaatkan teknologi jaringan.Seperti tidak harus bolak-balik untuk menggunakan printer di kantor ditempat bekerja, kirim file dengan media POS dan segala proses surat menyurat sudah bersifat *Office Automation*.

6. File-file lebih mudah dipelihara

Pengelolaan file-file sangat mudah di perlihara karena tempat penyimpan bisa saja berpusat keserver dan keamanan terhadap data bisa terjamin, karena server dikelola oleh seorang admin server jaringan.

7. Dapat meningkatkan kinerja sistem

Kinerja sistem lebih baik karena pemeliharaan rutin dilakukan dengan mengecek komputer berdasarkan waktu yang telah ditentukan.

Selain keuntungan-keuntungan yang diberikan dari adanya jaringan komputer, ada juga konsekuensi yang ditimbulkan dengan penggunaan jaringan komputer. Diantaranya adalah masalah keamanan (*security*) baik pada pengaksesan berbagai sumberdaya dari pihak-pihak yang tidak berwenang maupun keamanan (ancaman virus) pada data yang dipertukarkan (NANIK S., 2013:8). Berikut beberapa kerugian dari implementasi jaringan :

1. Biaya yang tinggi kemudian semakin tinggi lagi.

Pembangunan jaringan meliputi berbagai aspek seperti pembelian *hardware*, *software*, biaya untuk konsultasi perencanaan jaringan, kemudian biaya untuk jasa pembangunan jaringan itu sendiri. Investasi yang tinggi ini tentunya untuk perusahaan yang besar dengan kebutuhan akan jaringan yang tinggi. Sedangkan untuk pengguna rumahan, biaya ini relatif kecil dan dapat ditekan. Tetapi *network* harus dirancang sedemikian rupa sejak awal sehingga tidak ada biaya *overhead* yang semakin membengkak karena misi untuk pemenuhan kebutuhan akan jaringan komputer ini.

2. Manajemen perangkat keras dan administrasi sistem.

Di suatu organisasi perusahaan yang telah memiliki sistem, administrasi ini dirasakan merupakan hal yang kecil, paling tidak apabila dibandingkan dengan besarnya biaya pekerjaan dan biaya yang dikeluarkan pada tahap implementasi. Akan tetapi hal ini merupakan tahapan yang paling

penting. Karena kesalahan pada *point* ini dapat mengakibatkan peninjauan ulang bahkan konstruksi ulang jaringan. Manajemen pemeliharaan ini bersifat berkelanjutan dan memerlukan seorang tenaga IT profesional, yang telah mengerti benar akan tugasnya. Atau paling tidak telah mengikuti *training* dan pelatihan jaringan yang bersifat khusus untuk kebutuhan kantornya.

3. *Sharing* file yang tidak diinginkan.

With the good comes the bad, ini selalu merupakan hal yang umum berlaku (ambigu). Kemudahan *sharing* file dalam jaringan yang ditujukan untuk pemakaian oleh orang-orang tertentu, seringkali mengakibatkan bocornya *sharing* folder dan dapat dibaca pula oleh orang lain yang tidak berhak. Hal ini akan selalu terjadi apabila tidak diatur oleh administrator jaringan.

4. Aplikasi virus dan metode *hacking*.

Hal-hal ini selalu menjadi momok yang menakutkan bagi semua orang, mengakibatkan jaringan menjadi *down* dan berhentinya pekerjaan. Permasalahan ini bersifat klasik karena sistem yang direncanakan secara tidak baik.

2.1.2. Standar Jaringan Komputer

Menurut Supriyanto (NANIK S., 2013:57), ada banyak standar wireless 802.11 yang digunakan secara industry yaitu sebagai berikut :

1. Standar *wireless* 802.11b
    a) Mentrasmit pada *rate* kecepatan sampai 11Mbps menggunakan frekuensi 2.4 GHzm berbagai jaringan dengan keluaran maksimum biasanya secara *real* terpatok pada 7 Mbps.
    b) 802.11b mempunyai jangkauan yang bagus akan tetapi bisa dipengaruhi oleh inferensi sinyal radio. Banyak dipakai untuk jaringan di rumah dan banyak kelemhan di sisi keamanan.
2. Standar *wireless* 802.11a
    a) Beroperasi pada frekuensi 5 GHz dengan transmisi maksimum sampai 54 Mbps.
    b) Sangat cocok dan bagus pada aplikasi konferensi dan video.
    c) Bekerja dengan bagus pada populasi yang padat.
    d) Tidak bisa beroperasi pada standar 802.11b/g.
3. Standar *wireless* 802.11g
    a. Pengembangan dari versi 802.11b dengan *rate* kecepatan sampai 54 Mbps.
    b. Jangkauan yang lebih pendek (beberapa jenis piranti *wireless*-G diperkuat dengan teknologi yang bisa mencakup area yang lebih luas seperti teknologi MIMO).
4. Standar *wireless* 802.11n
    a) Bisa mencapai kecepatan sampai 450 Mbps dengan tiga *spatial data stream* secara teoritis dengan kondisi ideal.

b) Dengan teknologi MIMO bisa mencakup area antara 300-400 meter.

c) Disamping kecepatannya yang jauh lebih tinggi dan juga jangkauannya yang lebih luas, *wireless*-N ini dilengkapi dengan standar keamanan *wireless* terkini yaitu *Wi-fi Protected Access* (WPA2).

5. Standar *wireless* AC 802.11ac

Adalah standar (masih *draft*) teknologi Wi-Fi generasi kelima yang bisa menembus kecepatan sampai 1300 Mbps. Sudah banyak diproduksi perangkat Wi-Fi dengan teknologi *wireless* AC ini diantaranya Netgear dengan R6300 *Wireless AC Dual Band,* Asus RT-AC66, TP-Link Acher dan lain-lain.

2.1.3. Jenis Jaringan Komputer

Jaringan komputer dibagi menjadi menjadi empat jenis, berikut adalah penjelasan dari masing-masing jenis jaringan (Maslan & Wangdra, 2012:25):

1. LAN (*Local Area Network*)

Merupakan jaringan milik pribadi didalam gedung atau kampus yang berukuran sampai dengan beberapa kilometer. LAN sering digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor atau perusahaan untuk pemakaian bersama dan saling bertukar informasi.

2. MAN (*Metropolitan Area Network*)

Merupakan versi LAN yang berukuran lebih besar, 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 atau umum. MAN mampu menunjang data dan suara bahkan dapat untuk aplikasi TV kabel.

3. WAN (*Wide Area Network*)

Jangkauannya mencakup daerah geografis yang luas seringkali mencakup negara bahkan benua. Teknologi yang digunakan hampir sama dengan LAN.

a) Teknologi Jaringan Area Luas (WAN)

Sebagian besar teknologi jaringan area luas (*Wide Area Network*) memiliki perbedaan yang sangat menyolok dengan kerabat LAN-nya, dalam aspek berikut ini :

a. Teknologi-teknologi ini dirancang untuk digunakan oleh para pengelola layanan telekomunikasi (*carrier*) yang sekaligus harus menangani puluhan ribu pelanggan sehingga ukuran dan kompoleksitasnya dengan mudah dapat disesuaikan dengan kebutuhan.

b. Spesifikasi untuk lapisak fisiknya tipikalnya memiliki jarak antara 2 hingga 40 mil.

c. Spesifikasi untuk mendefinisikan beragam kecepatan data, mulai dari 56 Kbps hingga 10 Gbps

d. Teknologi-teknologi ini seringkali memanfaatkan teknik *multiplexing*, untuk membawa beberapa sambungan logika sekaligus melalui jalur fisik yang sama

b) Frame Relay

Teknologi Frame Relay berawal di tahun 1998, ketika para pengambang ISDN mengetahui bahwa *Link Access Protocol-D* (Protokol-D Akses Saluran) (LAPD), yang sebelumnya hanya digunakan untuk menyediakan jalur pensinyalan bagi kanal-D sebuah jaringan ISDN, dapat dimanfaatkan untuk kepentingan-kepentingan yang lebih besar. Hal ini bermuara pada lahirnya rekomendasi ITU-T I.222, yang berjudul Kerangka kerja untuk layanan pembawa tambahan bermodus paket (*Framework for additional packet mode bearer service*). Protokol ini terdiri dari sejumlah standar ANSI dan ITU-T, dan setengah darinya merupakan standar bersama yang juga mendefinisikan ISDN, sehingga kita tidak dapat menemukan semua keterangan mengenai protocol ini dari satu sumber saja. Namun sebegai permulaannya, kita dapat merujuk ke informasi yang dipublikasikan oleh Forum *Frame Relay* dan yang terdapat didalam standar ITU-TQ.922 dan Standar Q.933. Forum *Frame Relay* adalah sebuah organisasi nirlaba yang terdiri dari kurang lebih 300 perusahaan, yang bertujuan untuk memasyarakatkan *Frame Relay* dan mempublikasi

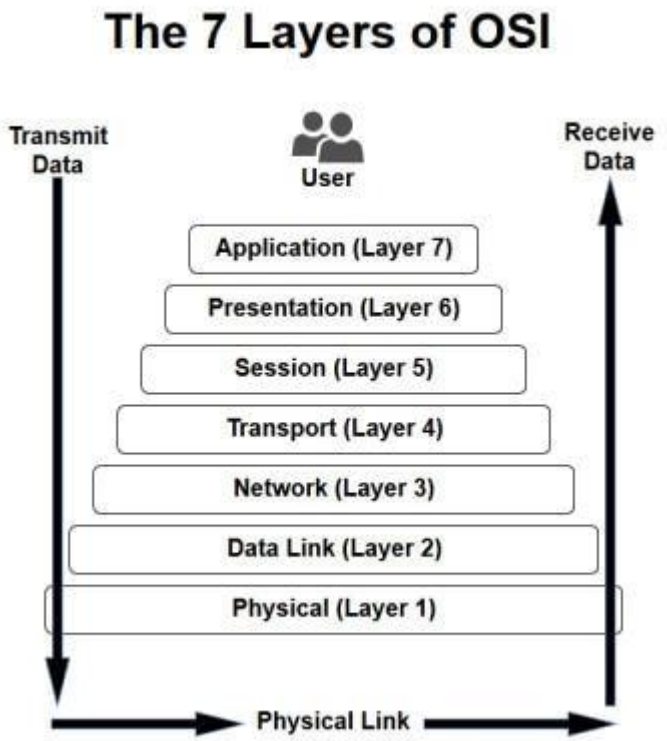
berbagai kesepakatan mengenaip pengimplementasiannya (*Implementation Agreement*). *Frame Relay* dirancang berdasarkan konsep *Virtual Circuit* (Jalur Sambungan Maya) (VC).

4. Internet

Jangkauannya mencakup seluruh dunia yang merupakan gabungan dari LAN, MAN, dan WAN yang ada

2.1.4. Model OSI Layer

Suatu Jaringan komputer LAN dibangun dengan memperhatikan arsitektur standar yang dibuat lembaga standar industry dunia. Standar jaringan yang saat ini diakui adalah *The Open System Connection* atau OSI yang dibuat oleh lembaga ISO (*The International Standar Organization*), Amerika Serikat. Seluruh fungsi kerja jaringa komuter dan komunikasi antarterminaal diatur dalam standar ini. OSI adalah suatu standar komunikasi antarmesin yang terdiri atas 7 lapisan. Ketujuh lapisan tersebut mempunyai peran dan fungsi yang berbeda satu terhadap yang lain. Setiap layer bertanggung jawab secara khusus pada proses komunikasi data. Model Osi dibagi dalam dua tingkatan grup yaitu : *upper layer* dan *lower layer*. Yang mana pada masing – masing grup mempunyai focus yang berbeda. Untuk *Upper layer* fokus pada aplikasi pengguna dan *file* direpresentasikan di komputer. Sedangkan untuk lower layer befokus pada para *network engineering* yang membuat *hardware.* (Maslan & Wangdra, 2012:34)



Gambar 2.1.4 Lapisan OSI

(Sumber : www.iso.org)

Tujuan utama penggunaan model OSI adalah untuk membantu desainer jaringan memahami fungsi dari tiap-tiap layer yang berhubungan dengan aliran komunikasi data, termasuk jenis-jenis protokol jaringan dan metode transmisi. Model dibagi menjadi 7 layer, dengan karakteristik dan fungsinya masing-masing. Tipe layer harus dapat berkomunikasi dengan layer diatasnya maupun dibawahnya secara langsung melalui serentetan protokol dan standar. Berikut adalah penjelasan masing-masing layernya.

1. *Physical Layer*

    a) Menangani pengiriman bit-bit data melalui saluran komunikasi.

b) Memastikan jika entity satu mengirim bit 1, maka entity yang lain juga harus menerima bit 1.

c) Fungsi utama untuk menentukan :

a. Beberapa volt untuk bit 1 dan 0.

b. Beberapa nanoseconds bit dapat bertahan di saluran komunikasi.

c. Kapan koneksi awal dibuat dan diputuskan ketika dua entity selesai melakukan pertukaran data.

d. Jumlah pin yang digunakan oleh *network connector* dan fungsi dari setiap pin.

d) Perangkat yang beroperasi di layer ini adalah *hub, repeater, network* adapter/*network interface card,* dan host bus adapter (digunakan di *storage area network*).

2. Data *Link Layer*

a) Menyediakan prosedur pengiriman data antar jaringan.

b) Mendeteksi dan mengkoreksi error yang mungkin terjadi di *Physical Layer*.

c) Memiliki address secara fisik yang sudah di-kode-kan secara langsung ke *network card* pada saat pembuatan *card* tersebut (disebut ***MAC Address***).

d) Contoh : Ethernet, HDLC, Aloha, IEEE 802 LAN, FDDI.

e) Perangkat yang beroperasi di layer ini adalah bridge dan layer-2 *switch.*

3. Network Layer

a) Menentukan prosedur pengiriman data sekuensial dengan berbagai macam ukuran, dari sumber ke tujuan, melalui satu atau beberapa jaringan, dengan tetap mempertahankan *Quality of Service* (*QoS*) yang diminta oleh *Transport Layer*.

b) Fungsi :

a. *Routing* : menentukan jalur pengiriman dari sumber ketujuan, bisa static (menggunakan *table static* yang cocok untuk jaringan yang jarang sekali berubah) atau dinamis (menetukan jalur baru untuk setiap data yang dikirimkan).

b. Pengendalian kongesti (kemacetan pada proses pengiriman data).

c. Mempertahankan QoS (*delay, transit time, jitter*, dll).

d. Menyediakan *interface* untuk jaringan-jaringan yang berbeda agar dapat saling berkomunikasi.

c) Contoh : *Internet Protocol* (IP).

d) Perangkat yang beroperasi di layer ini adalah router dan layer-3 switch.

Pada layer 3 di lapisan OSI terdapat 4 proses yang dilakukan agar data yang dikirim sampai ketujuannya dengan aman yaitu

a. *Addressing*

Pertama, *layer network* harus menyediakan mekanisme untuk menangani perangkat akhir ini. Jika -

individu bagian data yang harus diarahkan keperangkat akhir, perangkat harus memiliki alamat (*Addressing*) unik. Dalam sebuah jaringan IPv4, ketika alamat ini ditambahkan ke perangkat, perangkat ini kemudian disebut sebagai tuan rumah.

b. *Enkapsulasi*

Kedua, *layer Network* harus memberikan enkapsulasi. Tidak hanya harus perangkat diidentifikasi dengan alamat, potongan individu - PDUs *layer Network* - harus juga berisi alamat ini.Selama proses enkapsulasi, Layer 3 menerima Lapisan 4 PDU dan menambahkan sebuah Layer 3 *header*, atau *label*, untuk menciptakan PDU Layer 3. Ketika mengacu kepada *layer Network*, kita sebut ini sebuah paket PDU. Ketika sebuah paket dibuat, header harus berisi, di antara informasi lain, alamat untuk host yang sedang dikirim.Alamat ini disebut sebagai alamat tujuan. The Layer 3 *header* juga berisi alamat dari host asal. Alamat ini disebut sebagai alamat sumber.Setelah selesai dengan lapisan Jaringan proses enkapsulasi, paket dikirim ke layer *Data Link* harus disiapkan untuk transportasi atas media.

c. *Routing*

Selanjutnya, *layer Network* harus memberikan layanan untuk mengarahkan paket tersebut ke tujuan mereka tuan rumah. Sumber dan host tujuan tidak selalu terhubung ke jaringan yang sama. Bahkan, paket mungkin harus melakukan perjalanan melalui banyak jaringan yang berbeda. Sepanjang jalan, masingmasing paket harus dibimbing melalui jaringan untuk mencapai tujuan akhir. Intermediasi perangkat yang menghubungkan jaringan disebut router. Peran dari router adalah memilih jalur untuk paket-paket dan langsung menuju tujuan mereka. Proses ini dikenal sebagai routing.Selama routing melalui sebuah internetwork, paket dapat melewati banyak perangkat perantara. Setiap rute bahwa sebuah paket yang diperlukan untuk mencapai perangkat berikutnya disebut sebagai hop. Seperti paket diteruskan, isinya (lapisan Transport PDU), tetap utuh sampai host tujuan dicapai.

d. *Decapsulation*

Akhirnya, paket tiba di tujuan host dan diproses pada Layer 3. Host memeriksa alamat tujuan untuk memverifikasi bahwa paket ini ditujukan untuk perangkat ini. Jika alamat benar, paket ini decapsulated oleh lapisan jaringan dan Lapisan 4 PDU yang terkandung dalam paket

diteruskan kepada layanan yang tepat dilapisan Transport. Berbeda dengan lapisan Transport (OSI Layer 4), yang mengelola transportasi data antara proses yang berjalan pada host masing-masing ujung, Protocol lapisan jaringan menentukan struktur dan memproses paket digunakan untuk membawa data dari satu host ke host yang lain. Beroperasi tanpa memperhatikan data aplikasi dilakukan di masing-masing paket memungkinkan layer Network untuk membawa paket untuk beberapa jenis komunikasi antara beberapa host.

4. Transport Layer

a) Menerina data dari layer diatasnya, memecah data menjadi unit-unit yang lebih kecil (sering disebut *Packet*), meneruskannya ke network layer dan memastikan semua packet tiba diujung penerima tanpa ada error.

b) Layer ini harus melakukan proses diatas secara efisien dan memastikan layer diatas tidak terpengaruh terhadap perubahan teknologi hardware.

c) Fungsi :

a. *Flow Control*

b. *Segmentation/desegmentation*

c. *Error Control*

d) Contoh : *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP), *Stream Control Transmission Protocol* (SCTP).

5. Session Layer

a) Mengijinkan user-user yang menggunakan mesing yang berbeda untuk membuat dialog (*session)* diantara mereka

b) Fungsi :

a. Pengendalian dialog : memantau giliran pengiriman

b. Pengelolah token : mencegah dua pihak untuk melakukan operasi yang sangat kritis dan penting secara bersamaan.

c. Sinkronisasi : menandai bagian data yang belum terkirim sesaat crash pengriman terjadi, sehingga pengiriman bisa dilanjutkan tepat kebagiant tersebut.

6. Presentation Layer

a) Mengatur tetang *syntax* dan *semantics* dari data yang dikirimkan

b) Manipulasi data seperti *MIME encoding*, kompresi, dan enkripsi dilakukan di layer ini

7. Application Layer

a) Sangat dekat dengan user

b) Menyediakan user interface ke jaringan melalui aplikasi.

c) Contoh *protocol* aplikasi yang banyak digunakan : *Hypertext Transfer Protocol* (HTTP) yang digunakan di *World Wide Web, File Transfer Protocol* (FTP) untuk pengiriman file antar komputer, *simple mail transfer protocol* (SMTP) untuk email.

2.2 Teori Khusus

2.2.1. Keamanan Jaringan

Suhartono (Suhartono, n.d., 2015) mengatakan bahwa keamanan jaringan dapat digambarkan secara umum yaitu apabila komputer yang terhubung dengan jaringa yang lebih banyak mempunyai ancaman dari pada komputer yang tidak terhubung kemana-mana. Namun dengan adanya pengendalian maka resiko yang tidak diinginkan dapat dikurangi. Adanya keamanan jaringan maka para pemakai-berharap bahwa pesan yang dikirim dapat sampai dengan baik ke temapat yang dituju tanpa mengalami adanya keacatan yang diterima oleh si penerima. Biasanya jaringan yang aksesnya semakin mudah, maka keamananan jaringannya semakin rawan, namun apabila keamanan jaringan semakin baik maka pengaksessan jaringan juga semakin tidak nyaman.

Di dalam keamanan jaringan terdapat pula resiko jaringan komputer yang merupakan segala bentuk ancaman baik secara fisik maupun *logic* yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan. Resiko dalam jaringan komputer disebabkan oleh beberapa factor yaitu :

1. Kelemahan manusia
2. Kelemahan perangkat keras komputer
3. Kelemahan sistem operasi jaringan
4. Kelemahan sistem jaringan komunikasi

Selain itu keamanan jaringan juga mempunyai tujuan yang dapat membuat kemanan jaringan lebih ditingkatkan lagi, yaitu :

1. *Confidentiality* : Adanya data – data yang paling penting yang biasanya tidak boleh di akses oleh seseorang, maka dilakukan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Biasanya confidentiality ini berhubungan dengan informasi yang diberikan ke pihak lain.
2. *Integrity* : Bahwa pesan yang disampaikan tetap orisinil yang tidak diragukan keaslianya, tidak dimodifikasi selama dalam perjalanan dari sumber ke penerimanya.
3. *Avaibility* : Dimana user yan mempunyai hak akses diberi akses tepat pada waktunya, biasanya ini berhubungan dengan ketersediaan informasi atau data ketika dibutuhkan. Apabila sistem informasi ini diserang maka akan menghambat bahkan menyebabkan tidak dapat mengakses informasi tersebut.

Menurut Monika (Kusumawati, M, 2014) pada dasarnya, terdapat tiga jenis *mode* keamanan jaringan nirkabel :

1. *Wired Equivalent Privacy* (WEP)

   Merupakan standar keamanan pertama dari jaringan nirkabel yang dibuat dengan menggunakan algoritma enkripsi RC4. Algoritma ini sederhana dan mudah diimplementasikan karena tidak membutuhkan perhitungan yang berat, sehingga tidak membutuhkan

hardware yang canggih. Walaupun pengamanan metode WEP ini memiliki banyak celah keamanan, masih banyak orang menggunakannya.

2. *Wi-fi Protected Access* (WPA)

   WPA dikenal juga dengan sebutan WEPv2 alias WEP versi 2, yang dirilis pada bulan April 2003. WPA merupakan perbaikan dari WEP, jadi bukan merupakan sebuah metode keamanan yang baru, sehingga kelemahan yang terdapat pada WEP masih tetap ada pada WPA. Dimana sistem enkripsi yang digunakan masih menerapkan RC4. Konfigurasi kemanan pada WPA sangatlah sederhana karena hanya perlu memilih WPA sebagai metode pada klien dan juga pada *access point.*

3. *Wi-fi Protected Access* 2 (WPA2)

   WPA2 diperkenalkan pada bulan septermber 2014 oleh Wi-Fi Alliance. WPA2 sepenuhnya menerapkan standar IEEE 802.11i dan merupakan pengembangan lebih dari WPA. Perkembangan signifikan adalah perkenalan *Coutner Mode with Chiper Block Chaining Message Uthentication Code Protocol* (CCMP) yang menggunakan *block chipper Advanced Encryption Standard* (AES) utnuk enkripsi data, tetapi aliran *chipper* TKIP tersedia untuk kompabilitas dengn hardware WAP yang ada. Otentikasi WPA2 juga memiliki dua mode : *Pre-Shared Key* dan *Enterprise* mirip dengan WPA.

2.2.2. Penetrasi Testing dan PTES (Penetration Testing Execution Standard)

Penetration test, atau dalam Bahasa sehari-harinya dikenal dengan pen test, adalah sebuah serangan simulasi yang disahkan pada sistem komputer, yang dilakukan untuk mengevaluasi keamanan sistem. Pengujian dilakukan untuk mengidentifikasi kelemahan (juga disebut *vulnerabilities* / kerentanan), termasuk potensi pihak yang tidak berwenang untuk mendapatkan akses ke fitur dan data sistem, serta kekuatan, memungkinkan resiko penuh penilaian akan selesai.

Proses ini biasanya mengidentifikasi sistem target dan sasaran tertentu, kemudian meninjau informasi yang tersedia dan melakukan berbagai cara untuk mencapai tujuan tersebut. Target penetrasi tes mungkin berupa *white box* (yang menyediakan informasi latar belakang dan sistem atau *black box* (yang hanya menyediakan informasi dasar atau tidak ada kecuali nama perusahaan. Penetrasi test dapat membantu menentukan apakah suatu sistem rentan terhadap serangan, jika pertahanannya memadai, dan yang pertahanannya (jika ada) tesnya dikalahkan.

PTES (*Penetration Testing Execution Standard)* (Team, 2017) adalah standar baru yang dirancang untuk menyediakan layanan keamanan dan bisnis dengan Bahasa dan ruang lingkup yang sama untuk melakukan penetrasi testing. PTES dimulai dari pada tahun 2009 setelah sebuah diskusi yang memicu antara beberapa anggota pendiri mengenai nilai (atau kurangnya) penetrasi testing di industri ini. Diawali dengan sekeompok praktisi kemanan informasi dari semua bidang industri, yang diketuai oleh Chris Nickerson dan Dave Kennedy. Tujuan utama dibangunnya PTES adalah untuk menciptakan standar yang sebenarnya sehingga bisnis dapat memiliki dasar tentang apa yang dibutuhkan saat mereka

mendapatkan pentest serta pemahaman tentang jenis pengujian yang mereka perlukan atau akan memberikan nilai bagi bisnis mereka. Kurangnnya standarisasi sekarang hanya merugikan industry karena bisnis mendapatkan pekerjaan berkualitas rendah, dan praktisi kurang memiliki panduan dalam hal apa yang dibutuhkan untuk meberikan layanan berkualitas.

PTES terdiri dari tujuh bagian utama. Ini mencakut segala sesuatu yang berhubungan dengan tes penetrasi, dari komunikasi awal dan penalaran dibalik pentest, melalui fase pengumpulan intelijen dan pemodelan ancaman dimana penguji bekerja dibelakang layar untuk mendapatkan pemahaman yang lebih baik tentang organisasi yang diuji, melalui penelitian kerentanan, ekspoitasi dan eksploitasi pasca, di mana keamanan teknis keahlihan penguji ikut bermain dan digabungkan dengan pemahaman bisnis tentang keterlibatan dan akhirnya pelaporan, yang mencakup keseluruhan proses, dengan cara yang masuk akal bagi pelanggan dan memberikan nilai terbaik untuknya.

2.2.3. Evil Twin Attack

Baloch (Baloch, 2015 : 340) mengatakan bahwa, *Evil Twin Attack* adalah jenis serangan yang (*social engineering*) yang sangat populer terhadap klien. Gagasan dibalik serangan ini adalah untuk menciptakan jalur akses dengan nama yang mirip dengan apa yang menjadi korban dan menyebabkan penolakan layanan kejalur akses point semula (*Denial of Service to The Original Access Point*). Ini akan membuat korban kita terhubung ke akses point palsu kita dengan pemikiran bahwa itu adalah yang asli. Selanjutnya, penyerang juga akan menipu alamat MAC dari *interface* untuk mencocokkan alamat MAC dari akses point sebenarnya.

Sehingga menjadi lebih sulit untuk dideteksi. Secara umum, proses yang akan kita lalui dengan menggunakan metode ini adalah sebagai berikut :

1. Menggunakan *airodump-ng* untuk men-*scan* semua akses point terdekat.
2. Mencatat BSSID dan mengubah alamat MAC dari *interface* kita agar sama persis dengan BSSID dari akses point sebenarnya.
3. Kemudian meluncurkan akses point palsu dengan nama yang sama seperti aslinya.
4. Terakhir melakukan serangan *deauthentication* dengan Mk3 atau aireplay.

2.2.4. Kali Linux

Berdasarkan Allen, Heriyanto & Ali (Allen, Heriyanto, & Ali, 2014 : 9), Kali Linux (Kali) adalah sebuah sistem distribusi Linux yang dikembangkan dengan focus pada tugas pengujian penetrasi. Sebelumnya, Kali Linux dikenal sebagai BackTrack, yang mana merupakan gabungan dari tiga jenis distribusi Linux untuk penetrasi testing yaitu IWHAX, WHOPPIX, dan Auditor.

Backtrack adalah satu dari distribusi Linux yang terkenal, yang dapat dibuktikan dengan banyaknya *download* mencapai lebih dari empat juga seperti pada Linux BackTrack 4.0 pre final.

Kali Linux Versi 1.0 dirilis pada 12 Maret 2013. Lima tahun kemudian, Versi 1.0.1 dirilis, yang mana memperbaiki masalah pada USB keyboard. Dalam lima

hari, Kali telah diunduh lebih dari 90.000 kali. Berikut adalah fitur utama Kali Linux :

1. Kali Linux dibuat berdasarkan distribusi Linux Debian
2. Kali Linux mempunyai lebih dari 300 aplikasi penetrasi testing
3. Kali Linux mendukung kartu nirkabel yang luas
4. Kali Linux memiliki kernel khusus yang diluncurkan untuk injeksi paket
5. Semua paket *software* Kali GPG ditandatangani oleh masing-masing *developer*
6. Pengguna dapat menyesuaikan Kali Linux agar sesuai dengan kebutuhan mereka
7. Kali Linux mendukung sistem *ARM-Based*

Kali Linux berisi sejumlah *tools* yang bisa digunakan selama proses pengujian penetrasi. *Tools* penetrasi yang termasuk dalam Kali Linux dapat diketegorikan ke dalam kategori berikut :

1. *Information gathering*

   Kategori ini terdiri dari beberapa *tools* yang dapat digunakan untuk mengumpulkan informasi mengenai DNS, IDS/IPS, *network scanning*, sistem operasi, routing, SSL, SMB, VPN, *voice over* IP, SNMP, alamat email, dan VPN.

2. *Vulnerability assessment*

Pada ketegori ini, kamu dapat menemukan *tools* untuk *scan* kerentanan secara umum. Ini juga terdiri dari *tools* untuk mengakses jaringan Cisco, dan *tools* untuk akses kerentanan didalam beberapa server database. Kategori ini juga termasuk beberapa *fuzzing tools.*

3. *Web applications*

Kategori ini berisi *tools* yang berhubungan dengan aplikasi web seperti *content management system scanner, database exploitation, web application fuzzers, web application proxies, web crawlers,* dan *web vulnerability scanners.*

4. *Password attacks*

Didalam kategori ini, kamu akan menemukan beberapa *tools* yang dapat digunakan untuk melakukan penyerangan *password*, secara *online* atau *offline.*

5. *Exploitation tools*

Kategori ini berisi *tools* yang dapat digunakan untuk memanfaatkan kerentantan yang ditemukan di lingkungan sasaran/target. Kamu bisa menemukan *tools* untuk eksploitasi pada jaringan, web dan database. Ada juga *tools* untuk melakukan serangan rekayasa social dan mencari tahu tentang informasi eksploitasi.

6. *Sniffing and spoofing*

Tools dalam kategori ini bisa digunakan untuk memantau lalu lintas jaringan dan web. Kategori ini juga termasuk *tools spoofing* jaringan seperti *Ettercap* dan *Yersinia.*

7. *Maintaining access*

Tools dalam kategori ini akan dapat membantu kamu mempertahankan akses ke mesin target. Kamu mungkin perlu pendapatkan hak akses tertinggi pada mesin, sebelum kamu dapat meng-*install tools* dalam kategori ini. Disini, kamu dapat menemukan *tools* untuk *backdooring* sistem operasi dan aplikasi web. Kamu juga dapat menemukan *tools* untuk *Tunneling.*

8. *Reporting tools*

Didalam kategori ini, kamu akan menemukan *tools* yang dapat membantumu mendokumentasi proses penetrasi testing dan hasilnya.

9. *System services*

Kategori ini terdiri dari beberapa layanan yang dapat berguna saat penugasan penetrasi testing, seperti *Apache service,* MySQL *service,* SSH *service,* dan *Metasploit service.*

Untuk mempermudah kehidupan pentester penetrasi, Kali Linux telah memberikan kita sebuah kategori yang disebut Top 10 *Security Tools.* Berdasarkan namanya, ini adalah top 10 *tools security* yang biasanya digunakan oleh penetrasi tester. *Tools* yang termasuk ketegori ini adalah *aircrack-ng, burp-suite, hydra, john, meltego, metasploit, nmap, sqlmap, wireshark,* dan *zaproxy.*

Selain berisi *tools* yang dapat digunakan untuk penetrasi testing, Kali Linux juga berisi beberapa *tools* yang dapat digunakan sebagai berikut :

1. *Wireless attacks*

   Kategori ini berisi *tools* untuk menyerang *Bluetooth,* RFID/NFC dan perangkat *wireless.*

2. *Reverse engineering*

   Kategori ini berisi *tools* yang dapat digunakan untuk debug sebuah program atau membongkar file yang dapat di eksekusi.

3. *Stress testing*

   Kategori ini terdiri dari *tools* yang dapat digunakan untuk membantumu dalam *stress testing* jaringanmu, *wireless,* web, dan VOIP environment.

4. *Hardware hacking*

   Tools dalam ketegori ini dapat digunakan jika kamu ingin bekerja menggunakan Android dan aplikasi Arduino.

5. *Forensics*

   Pada kategori ini, kamu dapat menemukan beberapa *tools* yang dpat digunakan untuk *forensics* digital, seperti mendapatkan *hard disk image*, *crafing files,* dan analisis *hard disk image*. Untuk menggunakan kemampuan *forensics* di Kali Linux dengan benar, kamu perlu menavigasikan ke *Kali Linux Forensics | No Drives or Swap Mount* pada menu *booting*. Dengan opsi ini, Kali Linux tidak akan me-*mount* drive secara otomatis, sehingga akan manjaga integritas drive.

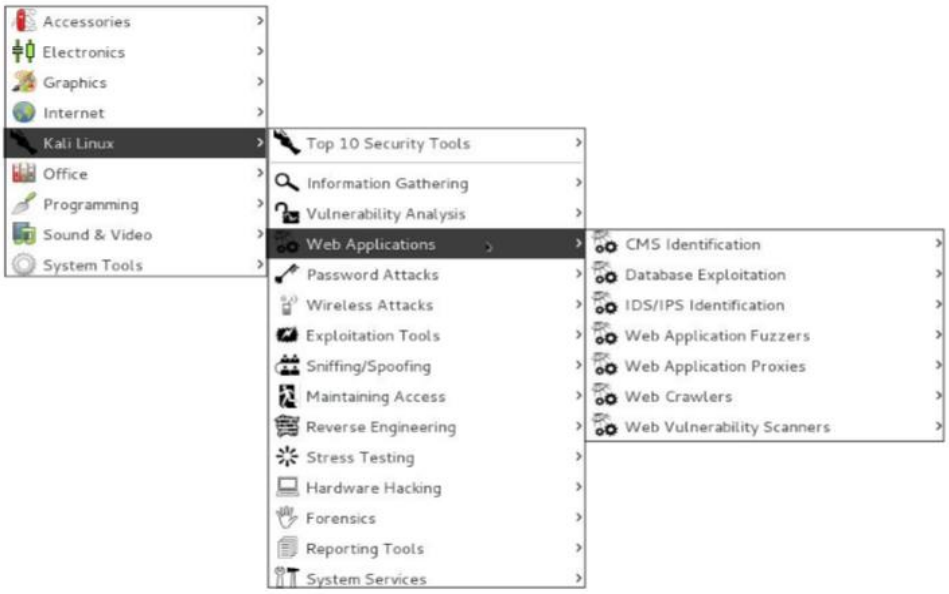
2.3. Tools

2.3.1. Kali Linux

Menurut Beggs (Beggs, 2014 : 33) Kali Linux (Kali) adalah penerus platform penetrasi testing BackTrack yang umunya dianggap sebagai paket standar yang digunakan untuk memudahkan penetrasi pengujian untuk data yang aman dan jaringan suara. Backtrack dirilis untuk menyediakan beragam penetrasi pengujian dan defensive alat-alat yang sempurna utnuk auditor dan administrator jaringan tertarik dalam menilai dan mengamankan jaringan mereka. Alat yang sama digunakan oleh penetrasi tester resmi dan tidak resmi (*Hacker*).

Di Maret 2013, BackTrack digantikan oleh Kali Linux, yang menggunakan arsitektur platform baru berdasarkan sistem operasi Debian GNU/Linux. Debian berpegang pada *Filesystem Hierarchy Standar*(FHS), yang merupakan keuntungan yang signifikan BacktTrack. Bukan perlu untuk menavigasi memalui pohon/pentest, kamu dapat menghubungi alat dari mana saja karena aplikasi termasuk dalam jalur sistem.

Ketika Kali diluncurkan, pengguna akan dibawa ke *default* GUI desktop dengan menu bar di bagian atas dan beberapa ikon sederhana. Dengan memilih item menu aplikasi, dan kemudian Kali Linux, pengguna akan mendapatkan akses kesistem menu yang berisi Top 10 alat-alat keamanan serta serangkaian *folder*, disusun dalam urutan umum yang akan diikuti selama penetrasi test, yang mana dapat dilihat pada ganbar berikut :

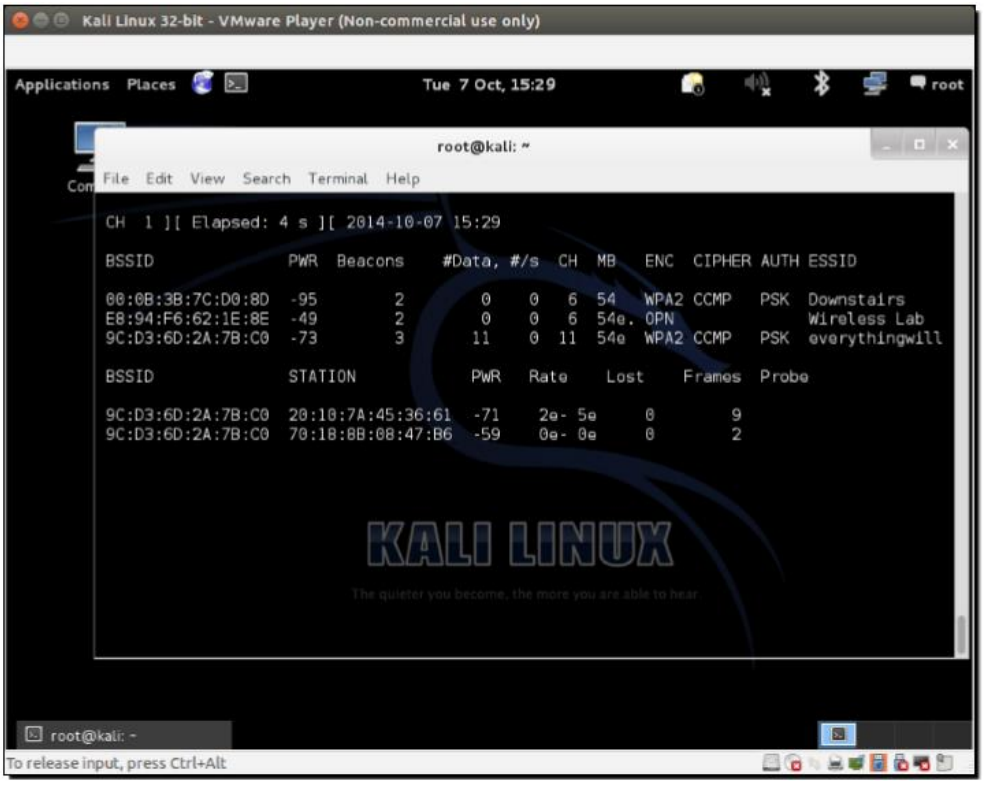


Gambar 2.3.1 Menu Bar Kali Linux

(Sumber : Beggs, 2014)

2.3.1.1. Airodump-ng

Airodump-ng adalah salah satu *command* dalam Kali Linux yang digunakan untuk melacak BSSID dan ESSID yang ada diwilayah sekitar kita (Ramachandran & Buchanan, 2015 : 101). Hal-hal yang akan ditampilkan setelah kita menjalankan *command* ini berupa BSSID, PWR(*power*), *Beacons*, Data, *Channel*, *Encryption*, *Authentication*, ESSID yang dapat kita lihat pada gambar berikut :

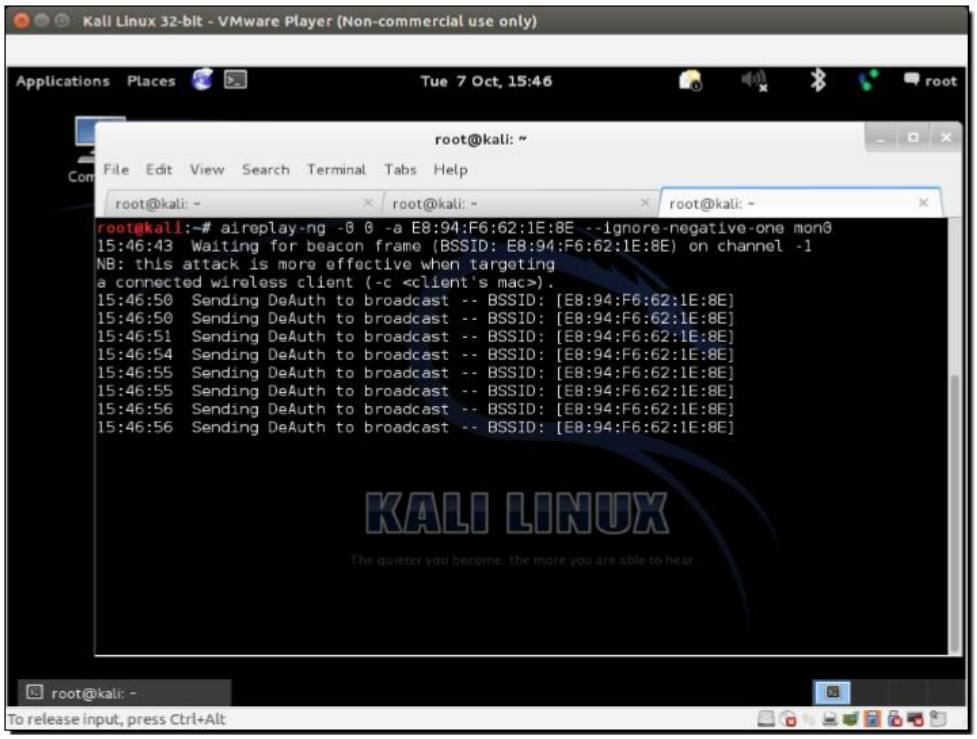


Gambar 2.3.1.1 Airodump-ng

(Sumber : Beggs, 2014)

2.3.1.2. Airbase-ng

Airebase-ng juga merupakan sebuah *command* dalam Kali Linux yang digunakan untuk membuat *access point* baru (Ramachandran & Buchanan, 2015 : 104). *Command* ini sering digunakan oleh pentester yang melakukan penyerangan dengan metode *Evil Twin*. *Access Point* yang dibuat akan berupa ESSID yang sama tetapi dengan BSSID dan MAC address yang berbeda dari sumbernya. Ketika kita telah berhasil menjalankan *command* ini, maka seluruh pengguna yang terhubung dalam jaringan tersebut akan dikirim sebuah *deauthentication frame* yang membuat mereka terputus dan segera mencoba untuk menghubungkan jaringannya kembali (*Reconnect*).



Gambar 2.3.1.2 Airebase-ng

(Sumber : Beggs, 2014)

2.3.1.3. Fluxion

Fluxion adalah sebuah audit keamanan dan *social-engineering research tool*. Ini adalah sebuah paket yang dibuat ulang dari Linset (Linset Is Not Social Enginering Tool) yang merupakan proyek yang memiliki tujuan sebagai edukasi dalam dunia *programming* dan *Wireless*. Linset pertama kali dipublikasi pada tanggal 6 November 2013 dengan nama LINSET 0.1. pada bulan Februari 2016, Linset berganti nama dengan Fluxion,dan secara resmi dipublikasikan. Fluxion disebut juga sebagai sebuah *script* dimana berisi paket-paket linux yang digunakan dalam melakukan uji keamanan jaringan nirkabel. paket-paket tersebut terdiri dari aircrack-ng, aireplay-ng, airmon-ng, airodump-ng, awk, curl, dhcpd, hostapd, iwconfig, lighttpd, machanger, mdk3, nmap, php-cgi, pyrit, phyton, unzip, xterm,

openssl, rfkill, strings, dan fuser. Paket-paket tersebut dijadikan menjadi satu *script* yang dijalankan secara bersamaan dan dengan tujuan memudahkan dan mempercepat proses persiapan dalam melakukan penetrasi testing sebuah jaringan. Berikut adalah gambaran bagaimana fluxion bekerja dalam proses secara bertahap :

1. *Scan* jaringan nirkabel target
2. Meluncurkan penyerangan *Handshake Snooper*
3. Menangkap sebuah *Handshake* (diperlukan untuk verifikasi *password*)
4. Meluncurkan *Captive Portal attack*
5. Meluncurkan *access point* palsu, meniru AP yang asli
6. Menjalankan sebuah DNS *server*, mengalihkan semua *requests* ke *host* penyerang yang menjalankan *Captive Portal*
7. Menjalankan web server, melayani *Captive Portal* yang meminta pengguna untuk memasukkan kunci WPA / WPA 2 mereka
8. Menjalankan *Jammer*, men-*deauthenticate* semua *clients* dari AP asli, dan memancing mereka ke AP palsu
9. Semua percobaan *authentication* pada *captive portal* dicek dengan *handshake file* yang ditangkap sebelumnya.
10. Serangan akan berakhir secara otomatis setelah kunci yang benar telah dikirim.
11. Kunci akan dicatat dan *clients* akan diizinkan untuk terhubung kembali kejalur akses target (AP asli).

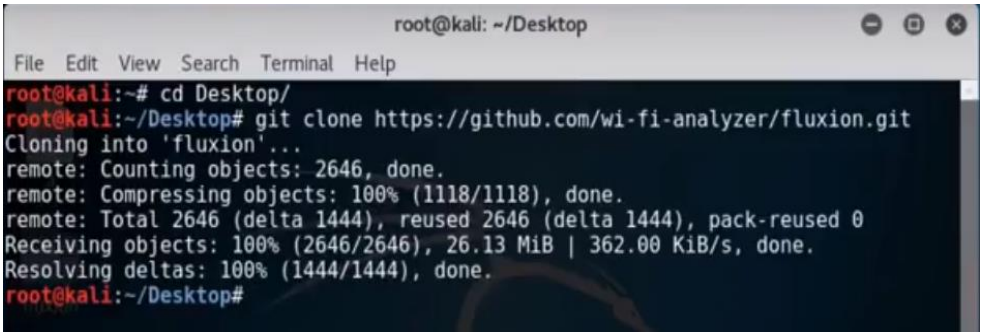
Gambar 2.3.1.3.1 Fluxion

(Sumber : Beggs, 2014)

Untuk mejalankan Fluxion, maka harus melakukan installasi yang dapat dilakukan dengan mengikuti tahapan-tahapan berikut ini

1. Buka terminal dan jalankan *command* berikut

   git clone --recursive git@github.com:FluxionNetwork/fluxion.git



Gambar 2.3.1.3.1 Installasi Fluxion
(Sumber : Olahan Penulis)

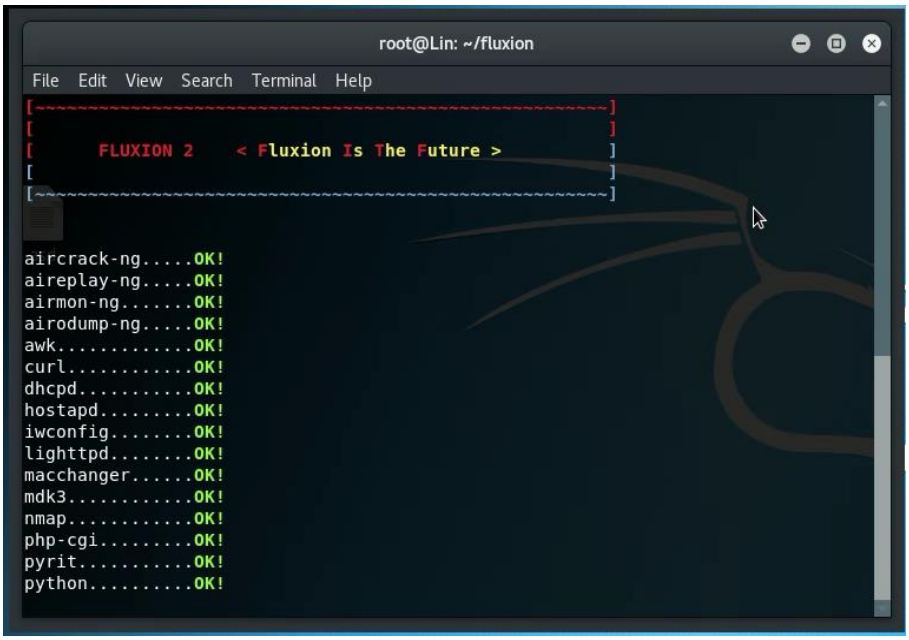
2. Kemudian masuk kedalam folder install fluxion

```
cd fluxion
cd install
```

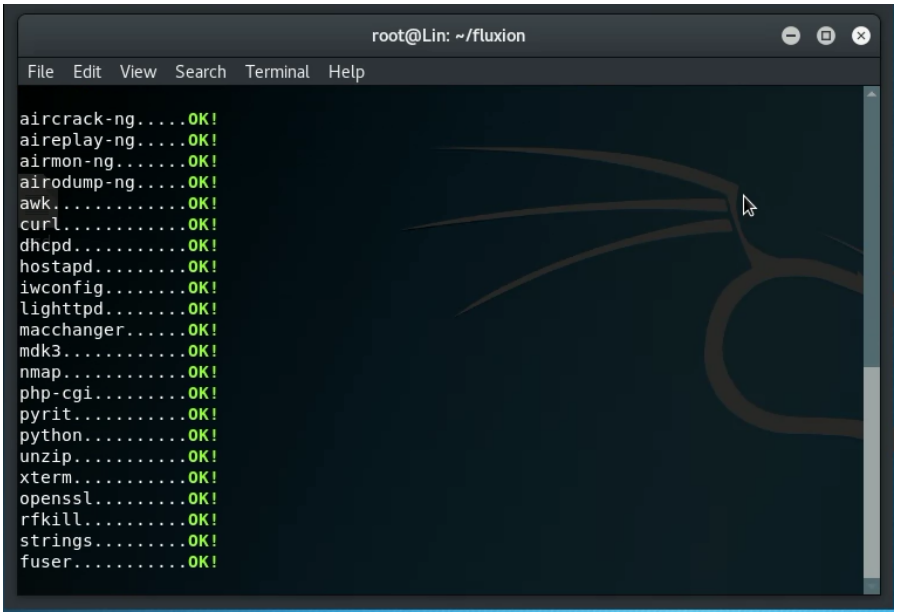
3. Lakukan installasi

   ```
   ./install.sh
   ```

4. Jika instalasi berjalan dengan benar, maka akan terlihat sebagia berikut saat kita menjalankan fluxion



Gambar 2.3.1.3.2 Installasi Fluxion
(Sumber : Olahan Penulis)



Gambar 2.3.1.3.3 Installasi Fluxion
(Sumber : Olahan Penulis)

2.4. Penelitian Terdahulu

1. Penelitian (Thite, Vanjale, & Mane, 2013) dengan judul "Elimination of Rogue Access Point in Wireless Network". Penelitian ini berpendapat bahwa sistem deteksi *rouge* akses point telah menjadi area penelitian utama karena meningkatnya pengguna jaringan nirkabel. Dalam makalah ini kami mengusulkan sebuah pendekatan baru untuk mendeteksi akses point *rogue* ini. Sistem yang diusulkan adalah sejenis sistem deteksi intrusi nirkabel. Ini menggunakan pendekatan gabungan (*hybrid*). Teknik yang sudah ada tidak memberikan solusi yang ringan. Tetapi pendekatan yang diusulkan mempertimbangkan semua parameter saat mendeteksi dan memberikan solusi ringan tanpa memodifikasi arsitektur jaringan. Solusinya adalah biaya yang efektif, terukur dan dapat digunakan dijaringan manapun. Teknik ini bekerja

pada sinya yang kuat. Kekuatan sinyal dapat dipengaruhi oleh kondisi lingkungan yang memberikan nilai kekuatan sinyal yang salah. Jadi masih ada cakupan yang cukup luas untuk penelitian masa depan.

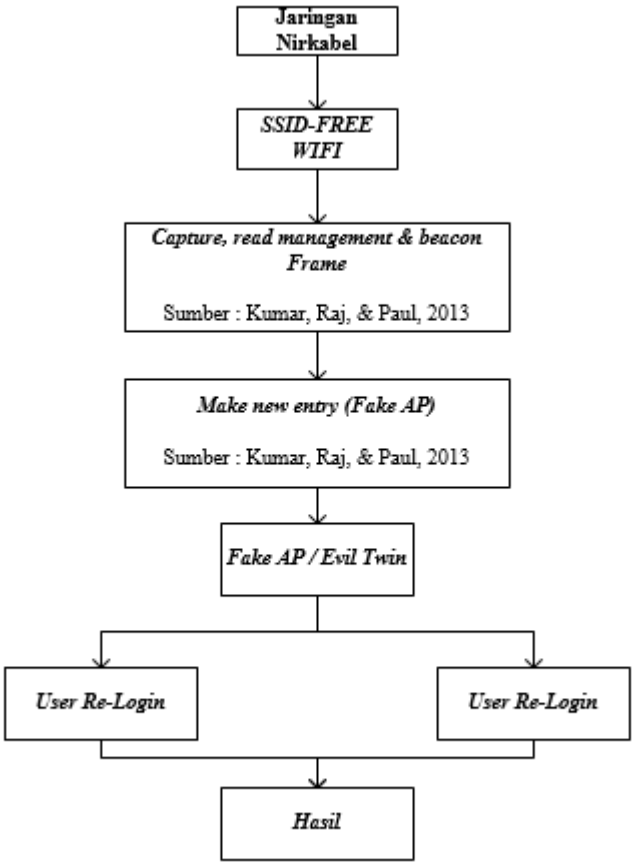
2. Penelitian (Science & Engineering, 2013) dengan judul "Study of Different Rogue Access Point Detection and Prevention Techniques in WLAN". Penelitian ini berkesimpulan bahwa peneliti masih jauh dari menemukan teknik yang dapat dengan jelas mengidentifikasi *Rogue* akses point. Seperti teknik mengumpulkan informasi konstruktif atau tepat dari jaringan untuk menentukan apakah perangkat itu "*rogue"* atau tidak. Ini cukup menantang karena lalu lintas jaringan dipenetrasi melalui beberapa perangkat. Jadi butuh untuk menemukan teknik yang akan menjadi gabungan untuk jaringan kabel dan nirkabel. Ini akan meminimalkan kelemahan teknik kabel dan nirkabel sekaligus memaksimalkan kekuatan mereka.
3. Penelitian (Mohtadi & Rahimi, 2015) dengan judul "New Attacks on Wi-Fi Protected Setup". Kesimpulan dari penelitian ini adalah standar WPS memiliki beberapa kelemahan. Desain protoko registrasi yang buruk dan juga beberapa kesalahan dalam penerapan standar ini menjadikannya sebagai ancaman terhadap keaman jaringan Wi-Fi. Ini adalah contoh yang sempurna dari konsekuensi yang bisa membuat standar yang lemah. Sepertinya WPS harus segera dinonaktifkan oleh pengguna. Pabrik peralatan nirkabel harus memodifikasi firmware pada perangkat mereka atau berhenti menggunakannya sepenuhnya. Selain

itu, semua implementasi standar harus segera dikaji dan dimodifikasi secepat mungkin.

4. Penelitian (Masiukiewicz, Tarykin, & Podvornyi, 2016) dengan judul "Security Threats in Wi-Fi Networks". Penelitian ini berkesimpulan bahwa jarigan Wi-Fi terpantau jauh lebih luas oleh intervensi pihak ketiga dalam sesi komunikasi. Bisakah kita memblokir kerentanan jaringan Wi-Fi terhadap ancaman ? jawabannya adalah tidak. Kita mempunyai *tools* seperti *hiding the SSID, MAC address filtering,* enkripsi, *authentication* menggunakan WEP, WPA, WPA2, *tools* untuk memonitoring lingkungan jaringan. Semua keamanan yang tersedia, bagaimanapun, cenderung rawan di *breaking* atau *bypassing*. Bisakah kita melarang penggunaan perangkat Wi-Fi dilingkungan kita ? jawabannya adalah tidak. Yang bisa kita menggunakan semua *tools* yang dapat digunakan. Namun perlu diingat bahwa alat ini terdedia bagi para *Hackers* dan mereka dapat dengan bebas menguji *software*-nya dan kemampuannya untuk menembus atau menghindari keamanan. Tampaknya dalam situasi ini sangat penting kesadaran akan jaringan pengguna melalui teknologi Wi-Fi dan tidak menggunakan jaringan dalam situasi tertentu. Jika kamu menggunakan Hotspot yang tidak diketahui janganlah pergi ke situs bank kita dan jangan sampai kita mencantumkan data kita. Tampaknya untuk meningkatkan kesadaran pengguna Internet dapat secara signifikan memperbaiki aspek keamanan jaringan mereka.

5. Penelitian (Siahaan & Lubis, 2016) dengan judul “WLAN Penetration Examination of The University of Pembangunan Panca Budi”. Kesimpulan penelitiannya mengatakan di jaringan global, tingkat keamanannya sangat penting. Mungkin kita kehilangan informasi berharga kita karena kelalaian kita. Tidak semua SSID bisa ditembus dengan metode ini. Mungkin jika pemilik jaringan tidak memiliki pengetahuan keamanan, makan akan rentan. Perdebatan masih dalam penetrasi testing dan *vulnerability*. Alat ini tidak bermaksud mencuri informasi rahasia. Ini membantu orang untuk meningkatkan keamanan dari celah yang ditemukan dengan menggunakan penetrasi test.

2.5. Kerangka Pemikiran



Gambar 2.5 Kerangka Pemikiran

(Sumber : Data Olahan Penulis)