ANALISIS KELEMAHAN PROTOKOL WIRELESS DENGAN METODE BRUTE FORCE ATTACK DI KALI LINUX (STUDI KASUS JARINGAN WIRELESS DI KOTA BATAM)

SKRIPSI

Oleh:
Richard Rolando
130210214

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2018

ANALISIS KELEMAHAN PROTOKOL WIRELESS DENGAN METODE BRUTE FORCE ATTACK DI KALI LINUX (STUDI KASUS JARINGAN WIRELESS DI KOTA BATAM)

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar sarjana

Oleh:
Richard Rolando
130210214

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2018

PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, dan/atau magister), baik di Universitas Putera Batam maupun di perguruan tinggi lain.
2. Skripsi ini adalah murni gagasan, rumusan, dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing.
3. Dalam skripsi ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi.

Batam, 3 Februari 2018
Yang membuat pernyataan,

Richard Rolando
130210214

ANALISIS KELEMAHAN PROTOKOL WIRELESS DENGAN METODE BRUTE FORCE ATTACK DI KALI LINUX (STUDI KASUS JARINGAN WIRELESS DI KOTA BATAM)

Oleh
Richard Rolando
130210214

SKRIPSI
Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Telah disetujui oleh Pembimbing pada tanggal
seperti tertera dibawah ini

Batam, 3 Februari 2018

Andi Maslan, S.T., M.SI.
Pembimbing

ABSTRAK

Perkembangan teknologi sekarang ini semakin pesat, dan hal itu pun berpengaruh dalam kehidupan manusia. Teknologi menjadi suatu kebutuhan yang semakin lama semakin utama. Salah satu teknlogi yang saat ini sedang banyak digunakan adalah *wireless local area network* (WLAN). Perangkat-perangkat elektronik yang menggunakan teknologi wireless semakin banyak diproduksi oleh karena kebutuhan akan informasi yang cukup mobile, maka banyak tempat-tempat seperti kantor, café, mall menyediakan layanan wifi *(wireless fidelity)*. Akan tetapi layanan tersebut sering kali kurang memperhatinkan pengaturan keamanan komunikasi data dalam jaringan tersebut. Kerentanan-kerentanan yang terjadi membuat pengguna wireless meragukan keamanannya. Implementasi WLAN membutuhkan suatu sistem keamanan yang memadai untuk menghindari pengguna yang tidak berhak memasuki jaringan. Penelitian ini bertujuan untuk mengetahui apakah *wireless* dengan menggunakan media access point memberikan tingkat keamanan yang baik terhadap data user yang sedang mengakses jaringan *wireless*, untuk mengetahui metode apa sajakah yang digunakan untuk mengamankan data *user* ketika mengkases jaringan *wireless*, untuk mengetahui bagaimana system keamanan *wireless* dengan menggunakan media access point *wireless* memiliki beberapa metode diantaranya SSID, MAC *Filtering*, WEP *(Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*). Secara umum *wireless* memiliki beberapa tipe serangan diantaranya *passive attacks, active attacks, man in the middle attacks, Brute Force Attacks*

Kata kunci: monitoring, keamanan , WLAN.

ABSTRACT

The innovations of technology is rapidly increasing and influted the human life. Technology become a necessity that is becoming important. One of technology that widely used is wireless local area network (WLAN). Most electronic device that using wireless technology is produced in large scale because the needs of information, so many place such as college, office, café, mall provides a wi-fi service (wireless fidelity). However, these service often pay less attention to secure the network. Vulnerabilities that happens make the user of wireless hesitated the secure of that network. Implementation of WLAN require a security system that sufficient to prevent unauthorized users to entering the network. This study aimed to determine wheter the wireless by using media access point provides a good levelof security for user data that is accessing the network wireless, to know what are the method used to secure user data when access ing the wireless, to know how to use wireless security system media wireless access point has a number of methods including SSID, MAC Filtering, WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access). In general has several type of attacks include passive attacks, active attacks, man in the middle attacks, Brute Force Attacks.

***Keyword**: monitoring, securyty, WLAN.*

KATA PENGANTAR

Dengan mengucap puji syukur kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-NYA, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam
3. Anggiat Marubah Siringo, S.Kom., M.Kom. selaku Dosen Pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Kedua orang tua saya yang senantiasa memberikan doa dan dukungan.
6. Keluarga yang turut memberikan doa dan dukungan.
7. Rekan-rekan mahasiswa/i Universitas Putera Batam yang saling mendukung dan memotivasi.

8. Jasmine Rafilidya azzahra yang memberikan masukkan dukungan moral doa dan motivasi.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Batam, 3 Februari 2018

Penulis

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

DAFTAR RUMUS

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang Penelitian

Berdasarkan Perkembangan dari sistem teknologi dan informasi disaat sekarang semakin berkembang dengan sangat pesatnya. Jika diamati setiap satu dekade maupun setiap saat, terjadi perkembangan yang cukup signifikan dari sistem teknologi dan informasi hal ini membawa cukup banyak perubahan terhadap berbagai kehidupan umat manusia baik di berbagai bidang, khususnya dapat kita rasakan pengaruhnya didalam kehidupan dunia usaha. Secara khusus dengan berlakunya sistem *Free Trade Zone* (FTZ) atau bebas pajak membuat wilayah Kota Batam menjadi lahan subur bagi penjualan teknologi seperti *smartphone* hingga perangkat *wireless* dari belahan negara lain.

Perkembangan teknologi komunikasi ini juga didukung dengan semakin mening-katnya kemajuan infrastruktur dan teknologi. Salah satu perkembangan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan *wireless*. Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol *Wireless Fidelity* (WiFi) yang berbasiskan standar IEEE 802.11. Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan peng-gunaan internet *online services* yang semakin cepat mendorong untuk memperoleh keuntungan dari *shared data* dan *shared resources*. Dengan *Wireless Local Area Network* (Wireless LAN) pengguna dapat

mengakses informasi tanpa mencari tempat untuk *plug in* dan dapat men-*setup* jaringan tanpa menarik kabel.

Dibandingkan dengan menggunakan media kabel, *wireless* banyak sekali keuntungan diantaranya *user* bisa melakukan koneksi *internet* kapan saja dan dimana saja asal masih berada dalam ruang lingkup *hot-spot*, selain itu dalam segi biaya pembangunan, *wireless* jauh lebih murah bila dibandingkan dengan kabel. Walaupun demikian, *wireless* memiliki lebih banyak kelemahan dibandingkan dengan kabel, khususnya di bidang segi keamanan.

Menurut (Gondohanindijo, 2012: 02) Kelemahan jaringan *wireless* terletak pada kelemahan pada konfigurasi dan jenis *enkripsi* yang digunakan. Dengan kemudahan dalam mengkonfigurasi sebuah jaringan *wireless*, tambah dengan banyaknya *vendor* yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan *wireless* yang masih menggunakan konfigurasi *wireless default* bawaan *vendor* seperti SSID, IP Address , *remote manajemen*, DHCP *enable*, *kanal frekuensi*, tanpa *enkripsi* bahkan *user/password* untuk *administrasi wireless* tersebut.

Menurut (Wahyudi & Purwanto, 2012: 18) Tingginya animo masyarakat, khususnya di kalangan komunitas internet menggunakan teknologi *wireless* dikarenakan paling tidak dua faktor tingginya animo masyarakat, khususnya di kalangan komunitas *internet* menggunakan teknologi *wireless* dikarenakan paling tidak dua faktor. pertama, kemudahan akses. Artinya, para pengguna dalam satu area dapat mengakses *internet* secara bersamaan tanpa perlu direpotkan dengan kabel. Konsekuensinya, pengguna yang ingin melakukan *surfing* atau

browsing berita dan informasi di *internet*, cukup membawa *pocket digital assistance* (PDA) atau laptop berkemampuan *wireless* ke tempat dimana terdapat *access point* atau *hotspot*. Keinginan para pengguna *hotspot* dapat sangat bervariasi sesuai dengan lingkungan sekitarnya. Sebagai contoh, para penguna dari kalangan industri atau perdagangan akan memiliki tingkat keinginan/ kebutuhan yang berbeda dengan pengguna yang berada di café. Orang yang bepergian untuk berbisnis tinggal di hotel yang dapat menggunakan *hotspot* akan memiliki keinginan yang berbeda juga. Jika keinginan para pengguna tidak dapat dimengerti sepenuhnya, maka kesuksesan dari *hotspot* akan sangat dipertanyakan. Agar pelayanan yang diperoleh oleh pelanggan dapat maksimal, perlu dilakukan perencanaan yang baik sebelum *hotspot* ini diimplementasikan. Saat ini kendala yang muncul adalah faktor biaya yang dapat dijangkau oleh para pengguna *wireless* sehingga bisa mendapatkan koneksi *internet* dilihat dari sisi *antenna*.

Menurut (Swati Sukhija, 2012: 01) terdapat 3 protokol keamanan jaringan yang umum digunakan yaitu WEP, WPA, WPA2, *Wired equivalent privacy* (WEP) adalah mekanisme kamanan untuk *wireless* LAN. Saat itu diperkenalkan pada bulan September 1999 sebagai bagian dari IEEE 802.11 standar keamanan. Tujuan dari *wired equivalent privacy* (WEP) adalah untuk menyediakan keamanan yang sebanding dengan jaringan kabel. RC4 *stream chipper* digunakan oleh WEP untuk menyediakan kerahasiaan dan CRC-32 untuk integritas data. Standar yang ditentukan untuk WEP menyediakan dukungan untuk kunci 40 *bit* kunci hanya tetapi ekstensi non standar telah disediakan oleh berbagai *vendor* yang memberikan dukungan untuk panjang kunci 128 dan 256 bit juga. Untuk

mengatasi kelemahan WEP, *Wi-Fi Protected access* (WPA) diperkenalkan pada tahun 2003 oleh Wi-Fi (*Wireless Fidelity) Alliance.*

WPA mengimplementasikan sebagain besar standar IEEE 802.11 li, sehingga merupakan solusi menengah. WPA dimaksudkan untuk mengatasi WEP masalah *kriptografi* tampa memerlukan perangkat keras baru. WPA2 diperkenalkan pada bulan September 2004 oleh *Wi-fi Alliance*. WPA2 sepenuhnya merupakan penerapan standar IEEE 802.11 li dan merupakan perkembangan lebih dari WPA. Perkembangan signifikan adalah pengenalan *Counter Mode With Chiper Block Chaining Message Authentication Code Protokol* (CCMP) yang menggunakan *Block Chiper Advanced Encryption Standard* (AES) untuk enkripsi data, tetapi aliran *chipper* TKIP tersedia untuk kompatibilitas dengan *hardware* WAP yang ada. Otentikasi WPA2 juga memiliki dua mode: *Pre-Shared Key* dan *Enterprise* mirip dengan WPA.

Untuk mengetahui kelemahan prtokol keamanan jaringan *wireless* tersebut, salah satu metode yang digunakan adalah menggunakan metode *Brute Force Attack*. Menurut (Maslan, 2012: 112) sebagian besar *access point* mengunakan satu kunci tunggal atau *password* yang dimiliki oleh *client* pada jaringan *wireless.* Serangan *Brute Force* ini mencoba melakukan uji coba terhadap kunci akses tersebut dengan memasukan beberapa kemungkinan.

Menurut (Dave, 2013: 75) Serangan dengan cara *Brute Force Attack* adalah serangan yang menggunakan metode *"Trial and Error"* dengan menebak *password*. *Attacker* menggumpulkan informasi mendasar tentang pemilik *wireless* contohnya nama pemilik, nomor kamar, nomor kendaraan, nama anak-anaknya.

Attacker terus menerus mencoba kata kunci acak berdasarkan informasi pribadi pemilik *wireless* sampai berhasil hal ini mungkin akan memerlukan waktu berjam-jam, hari, bulan dan juga tahun.

Penulis bermaksud untuk menulis penelitian berjudul **"ANALISIS KELEMAHAN PROTOKOL KEAMANAN JARINGAN DENGAN METODE BRUTE FORCE ATTACK (STUDI KASUS JARINGAN WIRELESS DI KOTA BATAM)".** Oleh karena itu penulis ingin membuat penjabaran mengenai kelemahan protocol keamanan jaringan *wireless* dengan menggunakan metode *Brute Force Attack* pada jaringan *wireless* di Kota Batam agar masyarakat mengetahui betapa pentingnya suatu pengamanan pada jaringan *wireless*.

1.2. Identifikasi Masalah

Berdasarkan latar belakang penelitian diatas maka identifikasi masalah dalam penelitian ini adalah :

1. Kelemahan jaringan *wireless* terletak pada kelemahan pada konfigurasi dan jenis enkripsi yang digunakan.
2. Kemanan jaringan nirkabel atau *wireless* sangat rentan terhadap penyadapan dan serangan *hacker*.
3. Penggunaan metode *Brute Force Atatck* yang dapat dilakukan untuk mencari celah berupa *password* pada keamanan jaringan *wireless*.

1.3. Batasan Masalah

Dengan adanya batasan masalah maka dapat lebih disederhanakan dan diarahkan penelitian agar tidak menyimpang dari apa yang diteliti. Adapun batasan masalah sebagai berikut:

1. Penelitian dilakukan pada jaringan *wireless* di Kota Batam bertempat di Kantor Indosat, Kantor RRI Batam, Indomaret Baloi.
2. Pembahasannya meliputi analisis *protocol* keamanan jaringan *wireless* yaitu WPA2 dengan menggunakan metode *Brute Force Attack.*

1.4. Rumusan Masalah

Hasil dari identifikasi masalah maka dibuatlah rumusan masalah sebagai solusi dari permasalahan tersebut.

1. Bagaimana kelemahan protokol keamanan jaringan *wireless* dengan metode *Brute Force Attack*?
2. Bagaimana tingkat keamanan protokol jaringan *wireless* di Kota Batam?

1.5. Tujuan Penelitian

Berdasarkan rumusan masalah yang telah ditentukam, maka tujuan penelitian yang hendak dicapai sebagai berikut :

1. Untuk mengetahui kelemahan protokol keamanan jaringan *Wireless* dengan metode *Brute Force Attack.*

2. Untuk menggetahui tingkat keamanan protokol jaringan *Wireless* di Kota Batam.

1.6. Manfaat Penilitian

Adapun manfaat yang diharapkan setelah tujuan di atas dapat dicapai adalah sebagai berikut:

1. Manfaat Teoritis:

   Memberikan gambaran tingkat keamanan jaringan *Wireless* yang bisa diterapkan pada saat ini, sehingga dapat memberikan petunjuk untuk menghindari *system* keamanan yang lemah.

2. Manfaat Praktis:

   Hasil Penelitian ini diharapkan dapat memberikan informasi yang bermanfaat mengenai keamanan jaringan pada masyarakat umum.

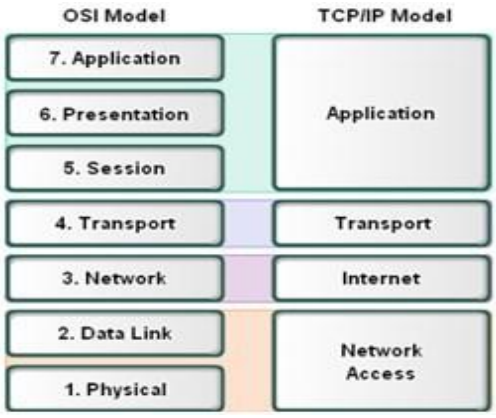
BAB II
KAJIAN PUSTAKA

2.1. Teori Dasar

2.1.1. *Internet* Protokol

Menurut (Wardoyo, Ryadi, & Fahrizal, 2014: 106) TCP/IP (*Transmission Control Protocol/Internet Protocol*) adalah standar komunikasi data yang digunakan oleh komunitas internet dalam proses tukar- menukar data dari satu komputer ke komputer lain di dalam suatu jaringan.

Prinsip pembagian lapisan pada TCP/IP menjadi protokol komunikasi data yang fleksibel dan dapat diterapkan dengan mudah di setiap jenis komputer dan antar-muka jaringan. Oleh karena sebagian besar isi kumpulan protokol ini tidak spesifik terhadap satu komputer atau peralatan jaringan tertentu. Berikut menunjukkan perbandingan model OSI dan TCP/IP.



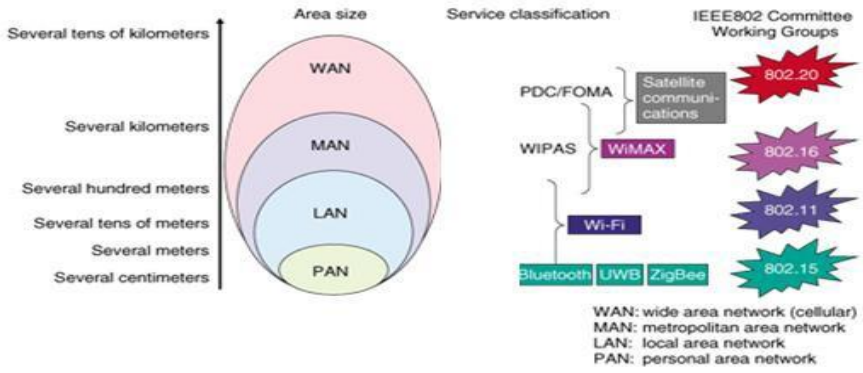
Gambar 2.1 Perbandingan Model OSI dan TCP/IP

2.1.2. Jaringan *Wireless*

Seiring perkembangan teknologi serta kebutuhan untuk akses jaringan bergerak, munculah *Wireless Local Area Network (Wireless LAN/WLAN)* di mana hubungan antar terminal atau komputer seperti pengiriman dan penerimaan data dilakukan melalui udara dengan menggunakan teknologi gelombang radio (RF).

Wireless LAN dapat didefinisikan sebagai sebuah sistem komunikasi data fleksibel yang dapat digunakan untuk menggantikan atau menambah jaringan LAN yang sudah ada untuk memberikan tambahan fungsi dan konsep jaringan komputer pada umumnya.

Menurut (Jutono Gondohanindijo, 2012:149) Jaringan *Wireless* berfungsi sebagai mekanisme pembawa antara peralatan atau antar peralatan dan jaringan kabel tradisional (jaringan perusahaan dan internet). Jaringan wireless banyak jenisnya tapi biasanya digolongkan ke dalam tiga kelompok berdasarkan jangkauannya: *Wireless Wide Area Network* (WWAN), WLAN, dan *Wireless Personal Area Network* (WPAN).



Gambar 2.2 Pembagain jaringan *wireless* berdasarkan jangkauanya.

1. WPAN: *Wireless Personal Area Network*

   mewakili teknologi personal *area network wireless* seperti *Bluetooth* (IEEE 802.15) dan *Infrared* (IR). Jaringan ini mengizinkan hubungan peralatan personal dalam suatu area berkisar 30 feet (1 feet=12 inch). Bagaimanapun juga *Infrared* membutuhkan hubungan langsung dan jangkauan yang lebih pendek.

2. WLAN: *Wireless Local Area Network*

   Mewakili *local area network wireless*, seperti lab atau perpustakaan, untuk membentuk suatu jaringan atau koneksi ke *internet*. Jaringan sementara dapat dibentuk oleh beberapa pemakai membutuhkan *access point*.

3. WMAN: *Wireless Metropolitan Area Network*

   Teknologi ini mengizinkan koneksi dari berbagai jaringan dalam suatu area metropolitan seperti bangunan-bangunan yang berbeda dalam suatu kota, yang mana dapat menjadi alternatif atau cadangan untuk memasang kabel tembaga atau *fiber*.

4. WWAN: *Wireless Wide Area Network*

   WWAN meliputi teknologi dengan daerah jangkauan yang luas seperti selular 2G, *Cellular Digital Packet Data* (CDPD), *Global System for Mobile Communications* (GSM).

Tabel 2.1 Pembagain jaringan *wireless* berdasarkan jangkauanya.

Jenis	Cakupan Area	Peformansi	Standarisasi	Penggunaan
WPAN	Hanya menjangkau area yang sangat dekat seperti didalam ruangan umumnya jangkauan sekitar 30 feet	Cukup, kecepatan bisa mencapai 2 MBps	*Bluetooth*, IEEE 802.15IrDa	Bertukar data antara PDA dengan laptop, koneksi ke printer *wireless*.
WLAN	Dalam suatu gedung, perkantoran atau lab.	Kuat, kecepatan transfer dapat mencapai 54 MBps	*Wi-Fi* IEEE 802.11	Sama seperti jaringan kabel lan, wlan bisa digunakan untuk bertukar data, akses aplikasi di komputer lain dalam satu kantor.
WMAN	Mencangkup area dalam satu kota.	Kuat	*Wimax* 802.16	Koneksiantar gedung dalam satu Kota
NWAN	Mencangkup Area yang sangat luas, seperti koneksi antar negara atau benua	Rendah, kecepatan data hanya mencapai 170 Kbps,	CDPD, cellular 2G, 3G	

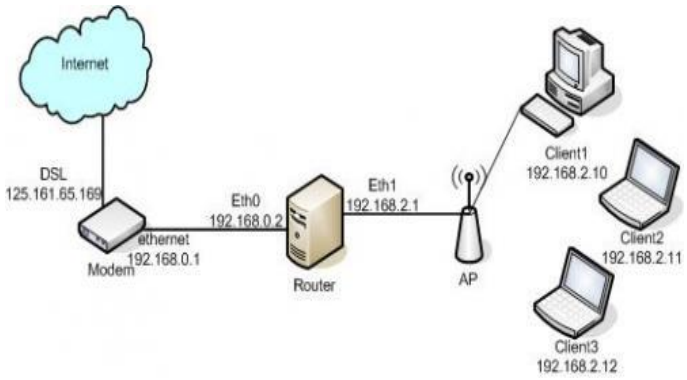
Dengan jaringan *wireless* memungkinkan para pengguna komputer terhubung tampa kabel *(Wirelessly)* ke dalam jaringan, suatu leptop atau *PDA (Personal Digital Assistant)* yang dilengkapi dengan PCMCIA *(Personal Computer Memory Card Industry Association)* yang dapat digunakan secara *mobile*.

2.1.2.1. Komponen Utama Jaringan *Wireless*

Menurut (Hantoro 2009: 19) Secara umum komponen *wireless* itu terdiri atas perangkat berikut ini:

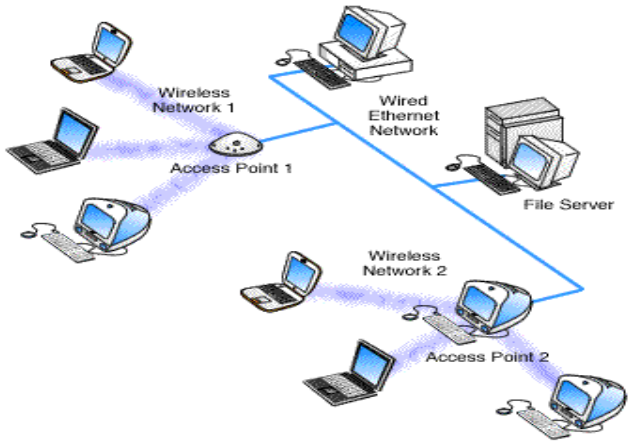
1. *Access Point* (AP)

   Pada *wireless* LAN, *device transceiver* disebut dengan *Access Point,* dan terhubung dengan jaringan (LAN) melalui kabel (biasanya berupa UTP). Fungsi dari *Access Point* adalah mengirim dan menerima data, serta berfungsi sebagai *buffer* data antara *wireless* LAN dengan *wired* LAN. Saru *Access Point* dapat melayani sejumlah *user* (beberapa *literature* menyatakan bahwa satu *Access Point* maksimal meng-*handle* sampai 30 *user*). Karena dengan semakin banyaknya *user* terhubung ke AP maka kecepatan yang diperoleh tiap *user* juga akan semakin berkurang.



Gambar 2.3 Model Kerja AP

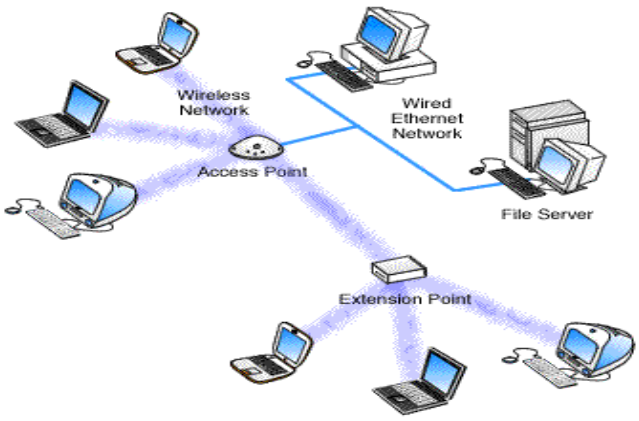
Bila AP dipasang lebih dari satu dan *coverange* tiap AP saling *overlap*, maka *user*/*client* dapat melakukan *roaming*. *Roaming* adalah kemampuan *client* untuk berpindah tampa kehilangan kontak dengan Jaringan



Gambar 2.4 AP yang lebih dari satu

2. *Extension Point*

Untuk mengatassi berbagai *problem* khusus dalam topologi jaringan *designer* dapat menambahkan *extension point* untuk menambah cangkupan jaringan. *Extension Point* hanya berfungsi layaknya *repeater* untuk *client* di tempat di tempat yang lebih jauh.



Gambar 2.5 Model AP dan *Extension Point*

Syarat dari AP yang digunakan sebagai *Extension Point* ini adalah terkait dengan *chanel* frekuensi yang digunakan. Antara AP induk (yang terhubung langsung dengan LAN *backbone*) dan AP *repeater*-nya harus memiliki

frekuensi yang sama. Disamping itu SSID yang digunakan juga harus sama sehingga antar-AP dapat saling berkomunikasi.

3. Antena

   Terdapat beberapa tipe antenna yang dapat mendukung dalam implementasi *wireless* LAN. Ada yang tipe *omni*, *sectorized* serta *directional.* Khusus antenna *directional* umumnya digunakan jika diiginkan jaringan antar 2 gedung yang bersebelahan (Konfigurasi *Point to Point*).

4. *Wireless* LAN *Card*

   Wireless LAN *card* dapat berupa PCMCIA, ISA *card.* USB *card* atau *Ethernet card* dan sekarang banyak dijumpai sudah *embedded* di terminal (*Notebook* maupun HP). Biasanya PCMCIA digunakan untuk *notebook* sedangkan yang lain digunakan untuk komputer *desktop*. *Wireless* LAN *card* ini berfungsi sebagai *interface* antara *system operasi* jaringan *client* dengan format *interface* udara ke AP. Untuk kondisi sekarang, banyak sekali *mobile terminal* seperti *notebook, netbook,* PDA maupun *mobile phone* yang sudah memiliki *interface WiFi*. Sering juga sudah dilengkapi perangkat *wireless* lain seperti *Bluetooth* maupun *infrared.*

2.1.2.2. Standarisasi *Wireless*

Beberapa standar yang dikenal dan diterapkan pada produk-produk *wireless* LAN saat ini 802.11a, 802.11b dan 802.11g.

Karena *wireless* LAN mengirim menggunakan frekuensi radio, WLAN diatur oleh jenis hukum yang sama dan digunakan untuk mengatur hal-hal seperti

AM/FM radio. *Federal Communications Commission* (FCC) mengatur penggunaan alat dari *wireless LAN*. Dalam pemasaran *wireless LAN* sekarang, menerima beberapa *standard operasional* serta syarat dalam Amerika Serikat yang diciptakan dan dirawat oleh *Institute of Electrical Electronic Engineers* (IEEE) John Groenewegen (2010). Beberapa *Standar wireless* LAN Menurut (Wahyudi et al., 2012) :

1. Standar 802.11a

   Standar IEEE 802.11a yaitu *Wi-Fi* dengan frekuensi 5 GHz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 75 m.

2. Standart 802.11b

   Standar IEEE 802.11b yaitu *Wi-Fi* dengan frekuensi 2,4 GHz yang memiliki kecepatan 11 Mbps dan jangkauan jaringan 100 m.

3. Standar 802.11g

   Standar IEEE 802.11g yaitu *Wi-Fi* dengan frekuensi 2,4 GHz yang memiliki kecepatan 54 Mbps dan jangkauan jaringan 75 m.

Tabel 2.2 Standarisasi *wireless*

	IEE 802.11	**802.11b**	**802.11a**	**802.11g**
Frequency	2.4 GHz	2.4 GHz	5 GHz	2.4 GHz
RF Technology	FHSS or DSSS	DSSS	OFDM	OFDM
Max Transfer Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps
Typical Outdoor Range	100 meter	150 meter	120 meter	150 meter

Security	*Wired Equivalent Protection (WEP)*	*Wired Equivalent Protection (WEP) + optional WiFi Protected Acess (WPA)*	*Wired Equivalent Protection (WEP) + optional WiFi Protected Acess (WPA*)	*Wired Equivalent Protection (WEP) / WiFi Protected Acess (WPA) / 802.11i (WPA2)*
Encryption	*40-bit RC4*	*Up to 104-bit RC4 (WEP), 128-bit RC4 w/TKIP key scheduling (WPA)*	*Up to 104-bit RC4 (WEP), 128-bit RC4 w/TKIP key scheduling (WPA)*	*Up to 104-bit RC4 (WEP), 128-bit RC4 w/TKIP key scheduling (WPA), 128-bit AES (WPA2)*
Fixed network support	*Ethernet*	*Ethernet*	*Ethernet*	*Ethernet*
Applications		*Wireless Data*	*Wireless Data*	*Wireless Data*

Tingginya animo masyarakat, khususnya di kalangan komunitas *internet* menggunakan teknologi *wireless* dikarenakan paling tidak dua faktor Tingginya animo masyarakat, khususnya di kalangan komunitas *internet* menggunakan teknologi *wireless* dikarenakan paling tidak dua faktor. pertama, kemudahan akses. Artinya, para pengguna dalam satu area dapat mengakses *internet* secara bersamaan tanpa perlu direpotkan dengan kabel. Konsekuensinya, pengguna yang ingin melakukan *surfing* atau *browsing* berita dan informasi di internet, cukup membawa *pocket digital assistance* (PDA) atau *laptop* berkemampuan *wireless* ke tempat dimana terdapat *access point* atau *hotspot*.

2.1.2.3. Topologi Jaringan *Wireless*

Wireless LAN memungkinkan dua bentuk koneksi, yang dikenal sebagai *Ad-Hoc* dan *mode Infrastructure* (Arianto 2009:153). Berikut ini penjelasan singkatnya:

1. *Mode Ad-Hoc*

   Mode Ad-Hoc adalah suatu kondisi jaringan *wireless* yang tidak menggunakan *access point*. Artinya, antar *client* langsung terkoneksi satu dengan yang lainnya. Jika merasa asing dengan istilah Ad-Hoc, mungkin istilah *Peer-to-peer* dapat lebih mempermudah mengenali koneksi Ad-Hoc. Prinsip kerjanya sama saja dengan *Peer-to-peer*. Disini setiap *client* akan saling terkoneksi secara langsung.

2. Model *Infrastructure*

   Model *infrastructure* adalah kondisi suatu jaringan dengan menggunakan suatu titik pusat yaitu *access point*. Semua *client* terhubung ke jaringan harus terkoneksi ke *access point* terlebih dahulu, baru kemudian dapat mengakses *resource* dari *network*/*client* lain yang ada. Untuk topologi *infrastruktur*, tiap PC mengirim dan menerima data dari sebuah titik akses, yang dipasang di dinding atau langit-langit berupa sebuah kotak kecil berantena. Saat titik akses menerima data, ia akan mengirimkan kembali sinyal radio tersebut (dengan jangkauan yang lebih jauh) ke PC yang berada di area cakupannya, atau dapat mentransfer data melalui jaringan *Ethernet* kabel. Titik akses pada sebuah jaringan infrastruktur memiliki area cakupan yang lebih besar.

2.1.2.4. Keuntungan dan Kelemahan Jaringan *Wireless*

Menurut (Nugroho dan Sartika 2011: 38) terdapat beberapa keuntungan dan kelemahan pada *wireless*. Dibawah ini beberapa keuntungan *wireless* diantaranya adalah:

1. Harga *wireless* terus turun, membuat *wireless* merupakan pilihan yang sangat ekonomis mengenai jaringan.
2. Produk *wireless* tersedia di pasar secara luas.
3. *wireless* jaringan dukungan *roaming*, di mana sebuah stasiun klien mobile seperti komputer laptop dapat berpindah dari satu jalur akses ke jalur akses yang lainnya.
4. tersebar Luas di lebih dari 250.000 tempat umum, jutaan rumah, perusahaan dan universitas di seluruh dunia.

Sedangkan pada *wireless* juga terdapat kelemahan berikut adalah beberapa kelemahan pada *wireless*:

1. Penyaluran Gelombang dan keterbatasan operasional yang tidak konsisten di seluruh dunia.
2. Konsumsi Power yang cukup tinggi jika dibandingkan dengan beberapa standar lainnya, membuat masa pakai baterai berkurang dan panas.
3. Jaringan *WiFi* memiliki rentang yang terbatas. Sebuah router *WiFi* rumah mungkin memiliki kisaran 45m (150ft) *indoor* dan (300ft) di luar rumah.
4. *WiFi* menggunakan *spektrum* 2.4GHz tanpa izin, dimana yang sering bertabrakan dengan perangkat lain seperti *Bluetooth*, *oven microwave*, telepon

tanpa kabel, atau perangkat pengirim video, banyak lainnya. Hal ini dapat menyebabkan penurunan kinerja.

5. Keamanan/kerahasiaan data kurang terjamin jalur akses dapat digunakan untuk mencuri informasi pribadi dan rahasia ditransmisikan dari konsumen *WiFi*.

Menurut (Utomo, 2012:21) keuntungan menggunakan jaringan nirkabel adalah sebagai berikut:

1. Tingkat Mobilitas Tinggi

   Penggunaan jaringan *wireless* memberikan kemudahan terhadap pengguna untuk mengakses informasi dimanapun mereka berada selama dapat terjangkau jaringan *wireless* tersebut.

2. Proses instalasinya mudah dan cepat

   Instalasi sebuah jaringan *wireless* termasuk mudah dan cepat, tampa harus menarik kabel melalui dinding/lantai. Kabel sebuah AP ke sebuah jaringan (*hub*/pengalih/*router*), sementara koneksi ke komputer *client* dilakukan via gelombang radio dengan medium udara.

3. Lebih Fleksibel

   Penggunaan jaringan *wireless* memungkinkan kita membangun sebuah jaringan komputer pada tempat-tempat yang tidak mungkin atau sulit dijangkau oleh kabel.

4. Meningkatkan Produktifitas

   Karena dapat selalu tersambung ke jaringan *intranet* atau *internet*, dimanapun pengguna akan lebih cepat.

Selain sebagai keuntungan diatas, penggunaan jaringan nirkabel juga mempunyai beberapa kelemahan jika ditinjau dari beberapa faktor, yaitu:

1. Faktor Keamanan

   Karena jaringan nirkabel bekerja dengan medium udara, sebenarnya *transmisi* data dapat ditangkap dan disadap oleh siapa saja sehingga banyak sekali tipe serangan yang terjadi pada jaringan nirkabel.

2. Faktor Kecepatan

   Jaringan nirkabel dapat menyediakan *transmisi* data hingga 54 Mbps dan 11 Mbps. Namun, hal itu juga dipengaruhi oleh lingkungan sehingga laju data yang didapat menjadi 24 Mbps dan 11 Mbps. Faktor cuaca sanggat berpengaruh terhadap kualitas sinyal, menginggat bahwa sistem transmisi yang digunakan adalah medium gelombang radio di udara, sehingga bisa memberikan penundaan terhadap pengguna.

3. Faktor Biaya (*Cost*)

   Harga komponen untuk membuat jaringan nirkabel saat ini masih tergolong mahal sehingga implementasinya membutuhkan perencanaan yang tepat. Walaupun biaya awalnya sangga tinggi, biaya perawatannya masih lebih murah dibandingkan jaringan berkabel.

Menurut (Arianto 2009:156) keuntungan dari penggunaan *wireless* LAN menawarkan produktifitas, layanan, kemudahan, dan keuntungan biaya melebihi jaringan kabel tradisional. Beberapa keunggulan pemakaian *wireless* LAN yaitu:

1. Mobilitas

   Sistem *Wireless* LAN memberi kemudahan bagi *user* untuk mengakses informasi *realtime* dimanapun mereka berada. Faktor mobilitas ini mendukung produktifitas dan kesempatan layanan yang tidak mungkin dilakukan dengan jaringan kabel.

2. Kecepatan dan Kemudahan Pemasangan /Instalasi

   Wireless LAN dapat dipasang dengan cepat dan mudah, dan dapat membatasi keperluan pemasangan kabel melalui dinding dan langit-langit (*Plafon).*

3. Mengurangi biaya kepemilikan

   Biaya investasi awal yang dipelukan untuk *hardware wireless* LAN lebih mahal dari pada biaya *hardware* jaringan kabel. Akan tetapi secara keseluruhan, biaya seluruh instalasi dan biaya siklus hidup (*life-cycle*) jauh lebih rendah. Keuntungan biaya jangka panjang jauh lebih besar dalam lingkungan kerja dinamis yang sering kali memerlukan perpindahan, penambahan, dan perubahan jaringan.

4. *Skalabilitas*

   Sistem *Wireless* LAN dapat dikonfigurasikan dalam beberapa topologi, disesuaikan dengan kebutuhan aplikasi khusus *user* dan *instalasi*. *Konfigurasi* yang mudah diubah dan jarak dari jaringan *peer-to-peer* sesuai dengan jumlah *user* yang sedikit untuk memenuhi infrastruktur jaringan dari ribuan *user* sehingga memungkinkan untuk menjelajahi area luas.

5. *Fleksibilitas*/Kelenturan instalasi

   Teknologi *Wireless* memungkinkan jaringan ini dapat dipasang ditempat dimana jaringan kabel tidak dapat dipasang

6. Keamanan

   Melihat segala kebaikan dari teknologi *spread spectrum* yang banyak dibangun oleh LAN *frekwensi* radio, maka jaringan ini lebih aman sifatnya dari pada jaringan kabel.

Disamping berbagai keuntungan yang ditawarkan oleh *Wireless* LAN, terdapat pula beberapa kelemahan dari sistem ini, diantaranya yaitu:

1. *Interferensi*/benturan dengan frekuensi yang digunakan oleh *provider cellular.*
2. Karena frekuensi *Wireless* LAN sama dengan frekuensi yang digunakan oleh *provider cellular*, maka sering mengakibatkan terjadinya benturan frekuensi. Jadi benturan frekuensi tersebut juga sangat mempengaruhi sinyal *Wireless* LAN, dan akibat dari benturan tersebut adalah turunnya kemampuan *Wireless* LAN hingga 10% sampai 20%
3. Untuk daerah yang mempunyai banyak halangan tentunya diperlukan biaya tambahan untuk membangun antena *repeater* yang berfungsi sebagai penguat sinyal.
4. *Range* Lebih Rendah Dibanding Jaringan Kabel

   Biasanya jaringan tampa kabel memiliki kemampuan 1-2 Mbps, walaupun kini telah berhasil dikembangkan hingga 11 Mbps, tetapi masih tetap jauh lebih rendah dibandingkan dengan LAN kabel.

5. Degradasi *Transmisi Data*

Pengiriman data melalui jalur udara mengalami degradasi dibandingkan mengirimkan data lewat kabel, meskipun jaringan kabel dipengaruhi oleh cuaca tetaspi dampaknya tidak terlalu besar.

6. Masalah *Interuperabilitas* Antar Prduk

   Wireless Komite IEEE 802.11 sebagai penentu standar *Wireless* LAN dihadapkan pada masalah interuperabilitas LAN dari berbagai *vendor* berbeda dan pencegahan *interferensi* sinyal yang mungkin disebabkan karena jaringan *Wireless* yang saling berdekatan satu sama lain. *Wireless* LAN bagaimanapun harus tetap konsisten, tidak saja dengan "penghuni" *spectrum* lainnya termasuk telepon nirkabel, peralatan insdustri, gangguan *background* alami maupun operator radio pemerintah.

7. Perbedaan *Performance* Nominal Dengan Jaringan Kabel

   Salah satu faktor utama yang membatasi penerimaan *user* terhadap *Wireless* LAN adalah perbedaan *performance* nominal antara jaringan kabel dengan jaringan *Wireless.* Sekilas pandang jurang *performance* terlihat amat lebar. Bandingkan jika *Ethernet* konvensional dioperasikan pada 10 Mbit/det dan *token ring* pada 16 Mbit/det. Padahal mayoritas *Wireless* LAN kurang dari 5 Mbit/detik.

2.1.3. Keamanan *Jaringan*

Menurut (Maslan, A., & Wangdra, 2012: 143) teknologi keamanan jaringan atau keamanan data (*Security*) selalu mengingatkan kita akan segala sesuatu yang berkaitan dengan perlindungan data dan pembatasan akses data. Lebih jauh lagi

istilah ini mencangkup banyak hal sehingga tidak ada suatu batasan tertentu untuk definisi keamanan jaringan. Dalam meninjau keamanan data, setiap data terkumpul dan kebutuhan-kebutuhan teridentifikasi, maka barulah kebijakan keamanan jaringan semua organisasi dapat dirumuskan dan diterapkan.

2.1.3.1. Indikator Protokol Kemanan Jaringan *Wireless*

Menurut (Kurnia, Setyawan, & Syafrizal, 2012: 14) standarisasi awal keamanan *wireless* 802.11 ini menentukan bahwa untuk bisa bergabung ke dalam jaringan AP, *host* harus diperbolehkan mengirim dan menerima data melalui AP, dan untuk melalukan itu terdapat 2 pintu yang harus dilalui yaitu *Authentication* dan *Association* dua Standarisasi 802.11 menggunakan 2 jenis *authentication*.

1. *Shared Key Authentication*

   Shared Key Authentication mengharuskan *client* untuk mengetahui lebih dahulu kode rahasia *(passphare key)* sebelum mengijinkan terkoneksi dengan AP.

2. *Open System Authentication*

   Open system authentication ini, dapat dikatakan tidak ada *authentication* yang terjadi karena *client* bisa langsung terkoneksi dengan AP *(Access point)*. Setelah client melalui proses *open system authentication* dan *Association, client* sudah diperbolehkan mengirim data melalui AP namun data yang dikirim tidak tidak serta merta dilanjutkan oleh AP kedalam jaringannya. Salah satu contoh sistem yang menggunakan *metode Open*

system authentication yaitu *Captive Portal*. *Captive Portal* adalah suatu teknik *autentikasi* dan pengamanan data yang lewat dari *network internal* ke *network eksternal*. *Captive Portal* sebenarnya merupakan mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik, hingga user melakukan registrasi. *Captive portal* juga mempunyai potensi untuk mengijinkan kita untuk melakukan berbagai hal secara aman melalui SSL, IPSec, dan mengset *rule quality of service* (QoS) per user, tapi tetap mempertahankan jaringan yang sifatnya terbuka di infrastruktur *wireless*.

Sedangkan menurut (Herdiana, 2014:27) dengan adanya kelemahan dan celah pada jaringan *wireless*, indikator protokol keamanan jaringan dapat diklafisikasikan sebagai berikut, yaitu:

1. Menyembunyikan SSID

   Banyak *administrator* menyembunyikan *Services Set Id (SSID)* jaringan *wireless* mereka dengan maksud agar hanya yang mengetahui SSID yang dapat terhubung ke jaringan mereka. Hal ini tidaklah benar, karena SSID sebenarnya tidak dapat disembuyikan secara sempurna. Pada saat-saat tertentu atau khususnya saat *client* akan terhubung (*assosiate*) atau ketika akan memutuskan diri (*deauthentication*) dari sebuah jaringan *wireless*, maka *client* akan tetap mengirimkan SSID dalam bentuk *plain text* (meskipun menggunakan enkripsi), sehingga jika bermaksut menyadapnya, dapat dengan mudah menemukan informasi tersebut. Beberapa *tools* yang dapat digunakan untuk mendapatkan ssid yang *hidden* antara lain, *kismet* (kisMAC), *ssid_jack* (*airjack*), *aircrack*, void11 dan masih banyak lagi.

2. Menggunakan kunci WEP

   WEP merupakan *standard* keamanan dan *enkripsi* pertama yang digunakan pada *wireless*, WEP memiliki berbagai kelemahan antara lain:

   a. Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
   b. WEP menggunakan kunci yang bersifat *statis*.
   c. Masalah *initialization vector* (IV) WEP.
   d. Masalah integritas pesan *Cyclic*.
   e. *Redundancy Check* (CRC-32).

   WEP terdiri dari dua tingkatan, yakni kunci 64bit, dan 128bit. Sebenarnya kunci rahasia pada kunci WEP 64bit hanya 40bit, sedang 24bit merupakan *Inisialisasi Vektor* (IV). Demikian juga pada kunci WEP 128bit, kunci rahasia terdiri dari 104bit. Serangan-serangan pada kelemahan WEP antara lain:

   a. Serangan terhadap kelemahan *inisialisasi vektor* (IV), sering disebut FMS *attack*. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan.
   b. Mendapatkan IV yang unik melalui *packet data* yang diperoleh untuk diolah untuk proses *cracking* kunci WEP ini dengan lebih cepat. Cara ini disebut *chopping attack*, pertama kali ditemukan oleh h1kari. Teknik ini

hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan *cracking* WEP.

c. Kedua serangan diatas membutuhkan waktu dan paket yang cukup, untuk mempersingkat waktu, para *hacker* biasanya melakukan *traffic injection*. *Traffic Injection* yang sering dilakukan adalah dengan cara mengumpulkan *packet* ARP kemudian mengirimkan kembali ke *access point*. Hal ini mengakibatkan pengumpulan *initial vector* lebih mudah dan cepat.

Berbeda dengan serangan pertama dan kedua, untuk serangan *traffic injection*, diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko, mulai dari *chipset, versi firmware*, dan *versi driver* serta tidak jarang harus melakukan *patching* terhadap *driver* dan aplikasinya.

3. Menggunakan kunci WPA-PSK atau WPA2-PSK.

   WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA *personal* (WPA-PSK), dan WPA- RADIUS. Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode *brute force attack* secara *offline*. *Brute force* dengan menggunakan mencoba banyak kata dari suatu kamus. Serangan ini akan berhasil jika *passphrase* yang digunakan *wireless* tersebut memang terapat pada kamus kata yang digunakan *hacker*. Untuk mencegah adanya serangan terhadap serangan wireleiss menggunakan WPA-PSK, gunakanlah *passphrase* yang cukup panjang (satu kalimat). *Tools* yang sangat terkenal digunakan melakukan serangan ini adalah *CoWPAtty* dan *aircrack.*

4. Memanfaatkan Fasilitas MAC *Filtering.*

Hampir setiap *wireless access point* maupun *router* difasilitasi dengan keamanan MAC *Filtering*. Hal ini sebenarnya tidak banyak membantu dalam mengamankan komunikasi *wireless,* karena MAC *address* sangat mudah di *spoofing* atau bahkan dirubah. *Tools ifconfig* pada *OS Linux/Unix* atau beragam *tools* seperti *network utilitis*, *regedit*, *smac*, *machanger* pada OS *windows* dengan mudah digunakan untuk *spoofing* atau mengganti MAC *address*. Masih sering ditemukan *wireless* di perkantoran dan bahkan ISP (yang biasanya digunakan oleh warnet) yang hanya menggunakan proteksi MAC *Filtering*. Dengan menggunakan aplikasi *wardriving* seperti *kismet*/*kisMAC* atau *aircrack tools,* dapat diperoleh informasi MAC *address* tiap *client* yang sedang terhubung ke sebuah *Access Point*. Setelah mendapatkan informasi tersebut, dapat terhubung ke *Access point* dengan mengubah MAC sesuai dengan *client* tadi. Pada jaringan *wireless,* duplikasi MAC *address* tidak mengakibatkan konflik. Hanya membutuhkan IP yang berbeda dengan *client* yang tadi.

5. *Captive Portal.*

   Infrastruktur *Captive Portal* awalnya didesign untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (*open network*). *Captive portal* sebenarnya merupakan mesin *router* atau *gateway* yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan *registrasi* atau *otentikasi*. Berikut cara kerja *captive portal* :

   a. *User* dengan *wireless client* diizinkan untuk terhubung *wireless* untuk mendapatkan IP *address* (DHCP)

b. *Block* semua trafik kecuali yang menuju ke *captive portal* (*registrasi*/*Otentikasi* berbasis web) yang terletak pada jaringan kabel

c. *Redirect* atau belokan semua trafik *web* ke *capital portal* Setelah user melakukan registrasi atau login, izinkan akses ke jaringan (*internet*)

Menurut (Maslan, A., & Wangdra, 2012: 112) sebagian besar *acces point* menggunakan suatu kunci tunggal atau *password* yang dimiliki oleh *client* pada jaringan *wireless*. Serangan *Brute Force* ini mencoba melakukan uji coba terhadap kunci akses tersebut dengan memasukan beberapa kemungkinan. Sedangkan menurut (Dave, 2013: 75) *Brute Force Attack* adalah serangan yang menggunakan metode *"trial dan error"* dengan menebak *password.* Seseorang penyerang terlebih dahulu mengumpulkan informasi mendasar tentang pengguna. Sebagai contoh, nama lengkap pengguna, nomor kamar, nomor kendaraan, nama anak-anak dll. Penyerang terus mencoba *password* secara acak berdasarkan informasi pribadi berguna. Penyerang mencoba ini sampai mendapatkan *password* tersebut. Ini mungkin memakan waktu berjam-jam, hari, bulan, dan bertahun-tahun.

2.1.3.2. Indikator *Brute Force Attack*

Menurut (Dave, 2013:76) terdapat 2 indikator pada metode *Brute Force Attack*, yaitu:

1. *Dictionary Attack*

   Dictionary Attack yaitu serangan berturut-turut dengan menggunakan daftar kata-kata, lalu *enkripsi*-nya, dan membandingkan dengan *one way hash* dari

sistem. Jika *hash* sama, maka *password* sukses di-*crack*, dan kata itu adalah *password*-nya. Sejumlah *dictionary cracker* bisa memanipulasi setiap kata dengan *filter*. *Filter* atau aturan tersebut mampu membangkitkan kata semacam "idiot" menjadi "1d10t" dan variasi lainnya yang sering dipergunakan. Jika *dictionary cracker* yang anda pakai tidak memungkinkan mutasi kata tersebut, tersedia pula sejumlah *tool* manipulasi daftar kata yang bisa melakukan *filter*, *expand*, dan mengubah kata. Jadi dari sejumlah kecil daftar kata bisa diperoleh banyak kata yang siap dipakai untuk *cracking*

2. *Hybrid Brute Force Attack*

   Hybrid Brute Force Attack yaitu serangan berturut-turut dengan menggunakan daftar kata-kata dari kamus yang telah dimodifikasi.

Sedangkan menurut Ambavkar (2012: 609) terdapat 2 celah keamanan pada WPA/WPA2 dengan *Brute Force Attack.* Adapun celah ini menjadi indikator yang digunakan pada *Brute Force Attack,* yaitu:

a. *Password* yaitu metode serangan dengan cara mencoba setiap kemungkinan *password* yang digunakan pengguna.
b. WPS *(Wi-Fi Protected Setup) PIN* yaitu suatu fitur pada *wireless* yang memudahkan cara pemasangan dan konfigurasi keamanan pada jaringan *wireless.* Pada perangkat *wireless* yang menggunakan fitur ini, terdapat celah keamanan bagi para *Hacker* untuk membobol dengan menggunakan *Brute Force Attack*

2.1.4. *Kali Linux*

Menurut (Sto, 2014: 3) Apa itu *kali linux*? Secara kasar bisa dikatakan bahwa *kali linux* adalah *Backtrack versi* 6. Lalu kenapa nama *Backtrack* harus diganti? Tidak secara jelas dijelaskan oleh *Offensive Security* namun diperkirakan karena adanya perubahan sangat mendasar dari *system operasi* yang digunakan. Jika dulunya *Backtrack* dibuat berdasarkan sistem *operasi Ubuntu*, kini *Kali Linux* menggunakan *Debian* sebagai *system operasi* dasarnya.

Kali Linux versi pertama yang direlease pertama kali tanggal 13 maret 2013 ini terus mendapatkan penyempurnaan karena menganti sistem operasi dasar yang digunakan sama juga dengan membangun dari awal semua yang sudah pernah dikerjakan.

Kali Linux sudah mendapatkan beberapa kali penyempurnaan dalam waktu yang sanggat singkat.

Tabel 2.3 Data versi *Kali Linux* hingga Januari 2014

Kali 1.0	*13th March, 2013 – Initial release.*
Kali 1.0.1	*14th March, 2013 – Minor Bugfix Release.*
Kali 1.0.2	*27th March, 2013 – Minor Bugix Release and updare roll-up.*
Kali 1.0.3	*26th April, 2013 – Bugfix roll-up. New accessibility features. Added live Desktop installer.*
Kali 1.0.4	*25th July, 2013 - Bugfix rollup. Penetration testing tool additions and updates.*
Kali 1.0.5	*5th September, 2013 – Bugfix rollup. LVM Encrypted installs,*

	Software Defined Radio (SDR) tools.
Kali 1.0.6	*9th January, 2014 – Kernel 3.12, cryptsetup nuke option, Amazon AMI, ARM build Scripts*

Seiring dengan perubahan nama yang dilakukan, *Kali linux* juga menggunakan domain baru sebagai tempat tinggalnya yaitu di *http://www.kali.org* Melalui *web* baru ini kita dapat men-*download Kali Linux versi* terakhir secara gratis. Hingga saat ini *Kali Linux* telah menggeluarkan versi *Kali* 2.2

2.2. *Tools*

2.2.1. *Aircrack-ng*

Menurut (Aaron Johns, 2015: 26) *Aircrac*k-*ng* merupakan program yang dituliskan dengan bahasa C Sebagai *Interface* untuk seorang *network security. Aircrack-ng* terdiri dari *detector,* paket *sniffer*, pemecah dan penganalisis WEP maupun WPA/WPA2 untuk jaringan WLAN 802.11. *Aircrack-ng* bekerja pada *wireless network interface* yang mendukung *mode monitor* dan bisa mendeteksi trafik dari 802.11a, 802.11b and 802.11g. Ada beberapa *tools* yang bisa bekerja di dalam *Aircrack-ng* seperti *Airodump-ng, Aireplay-ng, Nmap, Dnsiff, Arpspoof, Urlsnarf. Aircrack-ng* dapat digunakan oleh seorang *hacker* untuk tujuan jahat, juga dapat digunakan oleh seorang *network security* untuk memulihkan atau melakukan *penetrasi* terhadap *password wireless. Aircrack-ng* merupakan alat yang hebat untuk seorang *network security professional.* Berikut ini adalah fitur yang tersedia pada paket *Aircrack-ng*:

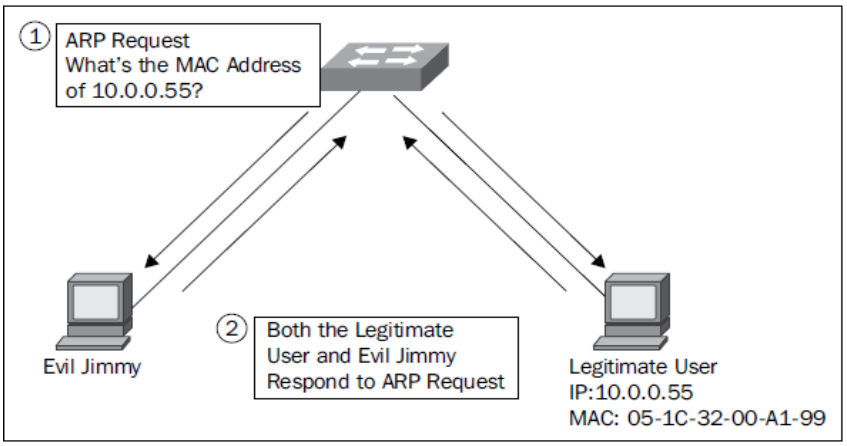
Tabel 2.4 *List Tools Aircrack-ng*

Name	*Description*
Aircrack-ng	*Crack WEP and WPA (Dictionary attack) keys.*
Airmon-ng	*Decrypts WEP or WPA encrypted capture file with known key.*
Airmon-ng	*Placing differents cards in monitor mode.*
Aireplay-ng	*Packet injector (Linux and Windows with CommView drivers).*
Airodump-ng	*Packett sniffer: Places air traffic into PCAP or IVS files and shows information about networks.*
Airtun-ng	*Virtual tunnel interface creator.*
Packetforget-ng	*Create encrypted packets for injection.*
Ivstools	*Tools to merge and convert.*
Airbase-ng	*Incorporates techniques for attacking client, as opposed to Access Points.*
Airdecloack-ng	*Removes WEP cloacking from pcap files.*
Airdriver-ng	*Incorporates techniques for attacking client, as opposed to Access Points.*
Airolib-ng	*Stores and manages ESSID and password list and compute Pairwise Master Keys.*
Airserv-ng	*Allows you to access the wireless card from other computer.*
Buddy-ng	*The helper server for easside-ng, run on a remote computer.*
Easside-ng	*A tool communicating to an access point, without the WEP*

	key
Tkiptun-ng	*WPA/TKIP attack.*
Wesside-ng	*Automatic tool for recovering WEP key.*

2.2.2. *Macchanger*

Menurut (Aaron Johns, 2015: 101) melakukan *filtering* MAC *Address* tidak benar-benar aman jauh lebih efektif daripada *enkripsi* WEP karena mudah dipalsukan. Ini bukan berarti melakukan MAC *filtering* tidak berguna. Apapun yang anda lakukan jangan pernah menghandalkan MAC *filtering*, *Enkripsi* WEP akan lebih baik daripada tidak sama sekali. Dibawah ini adalah ilustrasi melakukan MAC *Spoofing*.



Gambar 2.6 MAC *address spoofing*

Tidak butuh banyak skill untuk melakukan pengubahan MAC *Address*. Yang harus anda lakukan adalah *listen network traffic* dan mengganti MAC *address* kita dengan MAC *address* seseorang yang sudah terhubung ke *wireless* tersebut. secara *default tools macchanger* sudah ter-*instal* di *kali linux*, apabila

belum ter-*instal* bisa di *install* dengan perintah pada terminal *"apt-get install macchanger"*

2.2.3. *Crunch*

Crunch merupakan sebuah *tools generator* untuk membuat *dictionary wordlist*. *Crunch* memiliki kemampuan untuk membuat *wordlist* dengan mengkombinasikan semua angka, symbol, karakter (tergantung pada opsi yang digunakan) dan dapat diatur minimal panjang serta maksimal panjang dari *wordlist* yang ingin dibuat. secara *default crunch* sudah di-*install* di *kali linux*, apabila belum bisa di *install* dengan perintah pada terminal *"apt-get install crunch"*

2.3. Penelitian Terdahulu

Sebagai bahan pertimbangan dalam penelitian ini akan dicantumkan beberapa hasil penelitian terdahulu oleh beberapa peneliti yang pernah penulis baca diantaranya yaitu:

Indra Gunawan, dengan jurnal Elektronik berjudul ***"Pengembangan Brute Force Attack Dan Penerapannya Pada Crypt8 Dan CSA-Rainbow Tool Bagian 2"*** Volume 1, No.2 (ISSN: 2302-6618).

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian per-masalahan kode *cracking* dengan menggunakan *algoritma brute force* akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter

dan panjang kode tertentu tentunya dengan banyak sekali kombinasi kode. *Algoritma brute force* adalah algoritma yang lempang atau apa adanya. Pengguna hanya tinggal mendefinisikan karakter set yang diinginkan dan berapa ukuran dari kodenya. Definisi *Brute Force Attack* serangan *brute force* adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia. Sebagai contoh, untuk menyelesaikan sebuah persamaan kuadrat seperti $x^2+7x-44=0$, di mana x adalah sebuah integer, dengan menggunakan teknik serangan *brute force*, penggunanya hanya dituntut untuk membuat program yang mencoba semua nilai integer yang mungkin untuk persamaan tersebut hingga nilai x sebagai jawabannya muncul.

Istilah *brute force* sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: *"When in doubt, use brute-force"* (jika ragu, gunakan *brute force*). Secara sederhana, menebak kode dengan mencoba semua kombinasi karakter yang mungkin. *Brute force attack* digunakan untuk menjebol akses ke suatu *host (server/workstation/network)* atau kepada data yang ter-*enkripsi*.

Metode ini dipakai para *cracker* untuk mendapatkan *account* secara tidak sah, dan sangat berguna untuk memecahkan *enkripsi*. *Enkripsi* macam apapun, seperti *Blowfish*, AES, DES, Triple DES dsb secara teoritis dapat dipecahkan dengan *brute force attack*.

Pemakaian kode sembarangan, memakai kode yang cuma sepanjang 3 karakter, menggunakan kata kunci yang mudah ditebak, menggunakan kode yang sama, menggunakan nama, memakai nomor telepon, sudah pasti sangat tidak aman. Namun *brute force attack* bisa saja memakan waktu bahkan sampai berbulan bulan atau tahun bergantung dari bagaimana rumit kodenya. *Brute Force attack* tidak serumit dan *lowtech* seperti algoritma *hacking* yang berkembang sekarang. Seorang penyerang hanya cukup menebak nama dan kombinasi kode sampai dia menemukan yang cocok. Mungkin terlihat bahwa *brute force attack* atau *dictionary attack* tidak mungkin berhasil. Namun yang mengejutkan, kemungkinan berhasil *brute force attack* menjadi membaik ketika site yang ingin diretasi tidak dikonfigurasikan dengan baik.

Baihaqi, Yeni Yanti & Zulfan, dengan jurnal Teknik tahun 2018 di Banda Aceh berjudul ***"Implementasi Sistem Keamanan WPA2-PSK Pada Jaringan WiFi"***. Volume III, No.1.

Teknologi jaringan *wireless* saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Komputer, *notebook*, PDA, telepon seluler (*handphone*) dan *periferal* lainnya mendominasi pemakaian teknologi jaringan *wireless*. Penggunaan teknologi jaringan *wireless* yang di implementasikan dalam suatu jaringan lokal sering dinamakan WLAN *(Wireless Local Area Network).* Teknologi jaringan *wireless* memanfaatkan *frekuensi* tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat

komunikasi yang di gunakan oleh *user* maupun oleh operator yang memberikan layanan komunikasi. Namun dengan adanya *user* yang memanfaatkan teknologi jaringan *WiFi*, maka dapat memberikan sedikit celah keamanan kepada penyerang, sehingga penyerang dapat mengetahui *password* keamanan WPA2-PSK pada saat user terhubung ke jaringan *WiFi*. Kelemahan jaringan *wireless* secara umum dapat dibagi menjadi dua jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar,celah pada jaringan *wireless* terbentang di atas empat layer di mana keempat lapis layer tersebut sebenarnya merupakan proses terjadinya komunikasi data pada media *wireless*. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi.

Keamanan sistem jaringan *wireless* menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet yang sifatnya publik dan *global* pada dasarnya tidak aman. Adanya lubang-lubang keamanan pada sistem jaringan menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para *hacker*, *cracker* dan *script kiddies* untuk memanfaatkan pengaksesan jaringan secara bebas, pembobolan *password* keamanan pada jaringan *wireless*, dan lain-lain.

Luqman Hakim, dengan jurnal Prosiding Seminar Nasional Manajemen Teknologi XVII tahun 2013 di surabaya berjudul ***"Perbandingan teknik Penetration tes: Brute force dan Dictionary Attack"***. (ISBN: 978-602-97491-6-8). Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi layanan berbasis *web*. Ancaman *autentifikasi* tidak sah meningkat tajam

tahun belakangan ini. Diharapkan penelitian ini dapat mengukur kecepatan teknik yang digunakan pentester untuk mengevaluasi keamanan manajemen *user* sehingga pentester dapat melakukan proses penetration tes dengan efisien sesuai dengan waktu SDLC *(Software Development Life Cycle).*

Mengingat waktu perbaikan dikejar oleh serangan *attacker* dan kerawanan (*vulnerability*) pada web. Tes *autentifikasi* mencoba untuk menguji kelemahan dari *user* dan *password* web *admin*. Keberlangsungan akunnya tergantung dari kombinasi dan panjang karakter *password* agar terjamin dari *autentifikasi* tidak sah (*modifikasi* dan *validasi*). Dari

210 akun, 14,7 % berhasil *dicrack* dengan teknik *dictionary attack* dan 13,8% dapat di crack oleh *brute force*. Hasil dari penelitian ini adalah teknik *dictionary attack* lebih didahulukan penggunaannya ketimbang teknik *brute force* mengingat efektifitas dan reabilitas waktu *penetration* tes. Hasil ini juga dapat dijadikan rekomendasi manajemen *user* dan pemilihan kekuatan *password*.

diperoleh kesimpulan terhadap analisa performansi *brute force* dan *dictionary attack* dengan *tool* brutus terhadap akun admin web sebagai berikut:

1. Dalam mengimplementasikan suatu teknik penetration tes, penggunaan teknik *dictionary attack* lebih didahulukan ketimbang teknik *brute force* sebagai tahapan pengecekan *autentifikasi* halaman *login* website.
2. Kombinasi dan panjang *password* menjamin keberlangsungan akunnya dari *autentifikasi* tidak sah.

3. Semakin banyak kamus dalam *dictionary attack* maka semakin besar kemungkinan berhasil meng-*crack*. Begitu pula semakin besar kombinasi dan panjang karakter set pada *brute force*, maka kemungkinan *crack* lebih besar.

Saran yang dapat diberikan terhadap analisa *password* dan teknik *autentifikasi* tes adalah:

1. Manajemen *user password* pada sebuah web wajib mempertimbangkan kombinasi karakter dan jumlah karakter untuk menjaga sistem informasi dari akses *unprevilled*.
2. Penggunaan teknik *delay*, *captcha*, dan IP *blocking* dapat mengurangi serangan *brute force* dan *dictionary attack* **.**

Rialda Annisya, dengan jurnal Sistem Komputer tahun 2012 berjudul ***"Security System Layanan Internet Banking PT BANK MANDIRI (Persero) Tbk.".*** (ISSN: 2087-4685). Kesempatan Indonesia untuk mengembangkan *internet banking* sangat terbuka luas.Hal itu dimungkinkan karena pertumbuhan penggunaan internet di kawasan Asia sangat tinggi dan nasabah perbankan memerlukan layanan yang lebih lagi.

Salah satu isu yang menjadi permasalahan dalam penggunaan *internet banking* adalah sistem kemanan bertransaksi perbankan dengan menggunakan *internet*. Masalah yang sering muncul adalah adanya pencurian nomor kredit dan MITM *Attack*. MITM *attack* adalah serangan dimana *attacker* berada di tengah bebas mendengarkan dan mengubah percakapan antara dua pihak. Sedangkan pencurian dalam nomor kredit, nomor curian kemudian dimanfaatkan oleh orang yang sesungguhnya tidak berhak. Nasabah harus

diyakinkan oleh pihak bank bahwa transaksi perbankan berjalan aman karena bank bersangkutan memiliki perangkat keamanan untuk mencegah para *hacker* mengganggu transaksi mereka. ada dua jenis sistem keamanan yang dipakai dalam *internet banking*, antara lain:

1. Sistem *Cryptography*

   Sistem ini menggunakan angka-angka yang dikenal dengan kunci *(key).* Sistem ini disebut juga dengan sistem sandi. Ada dua tipe *cryptography,* yaitu simetris dan asimetris. Pada sistem *simestris* menggunakan kode kunci yang sama bagi penerima dan pengirim pesan. Kelemahan dari *cryptography simestris* adalah kunci ini harus dikirim pada pihak penerima dan hal ini memungkingkan seseorang untuk mengganggu di tengah jalan. Sistem *cryptography asimetris* juga mempunyai kelemahan yaitu jumlah kecepatan pengiriman data menjadi berkurang karena adanya tambahan kode. Sistem ini biasanya digunakan untuk mengenali nasabah dan melindungi informasi finansial nasabah.

3. Sistem *Firewall*

   Firewall merupakan sistem yang digunakan untuk mencegah pihak-pihak yang tidak diijinkan untuk memasuki daerah yang dilindungi dalam unit pusat kerja perusahaan. *Firewall* berusaha untuk mencegah pihak-pihak yang mencoba masuk tanpa ijin dengan cara melipatgandakan dan mempersulit hambatan-hambatan yang ada. Namun, yang perlu diingatkan adalah bahwa sitem *firewall* ini tidak dapat mencegah masuknya *virus* atau gangguan yang berasala dari dalam perusahaan itu sendiri.

UU ITE kini mampu mengatur sistem *internet* banking sebagai salah satu layanan perbankan yang merupakan wujud perbankan teknologi informasi. Kendala seperti aspek teknologi dan aspek hukum kini bukan lagi menjadi faktor penghambat sistem *internet banking* di Indonesia.

Dalam surat keputusan Direksi Bank Indonesia No. 27/164/KEP/DIR dan surat edaran Bank Indonesia No. 27/9/UPPB tanggal 31 Maret 1995 mengenai pengguanan sistem informasi oleh bank dapat dilihat bahwa pelaksanaan teknologi sistem informasi diserahkan kepada masing-masing bank. Bank Indonesia hanya memberikan pedoman sehingga di dalam pelaksanaannya tidak merugikan nasabah dan bank itu sendiri. Pada bagian III pasal 1 surat edaran Bank Indonesia No. 27/9/UPPB tanggal

Ancaman yang terjadi pada Internet Banking Mandiri antara lain *Active* Snifing, *Passive Snifing*, *Keylogger*, *Typo Site*, *Brute Force Attacking*, *Web Deface*, *Phissing*, *Denial of Service*, dan *Virus Worm Trojan*.

Yudi Herdiana, dengan jurnal Isu Teknologi STT Mandala tahun 2014 di Bandung berjudul ***"Kemanan Pada Jaringan Wireless"***. Volume 7, No.2 (ISSN: 1979-4819). Teknologi *wireless* (tanpa kabel / nirkabel) saat ini berkembang sangat pesat dengan hadirnya perangkat teknologi informasi dan komunikasi. Komputer, laptop, telepon seluler (*handphone*) dansmartphone mendominasi pemakaian teknologi *wireless*. Penggunaan teknologi *wireless* yang diimplementasikan dalam suatu jaringan local sering dinamakan WLAN *(Wireless Local Area Network).* Namun perkembangan teknologi *wireless*

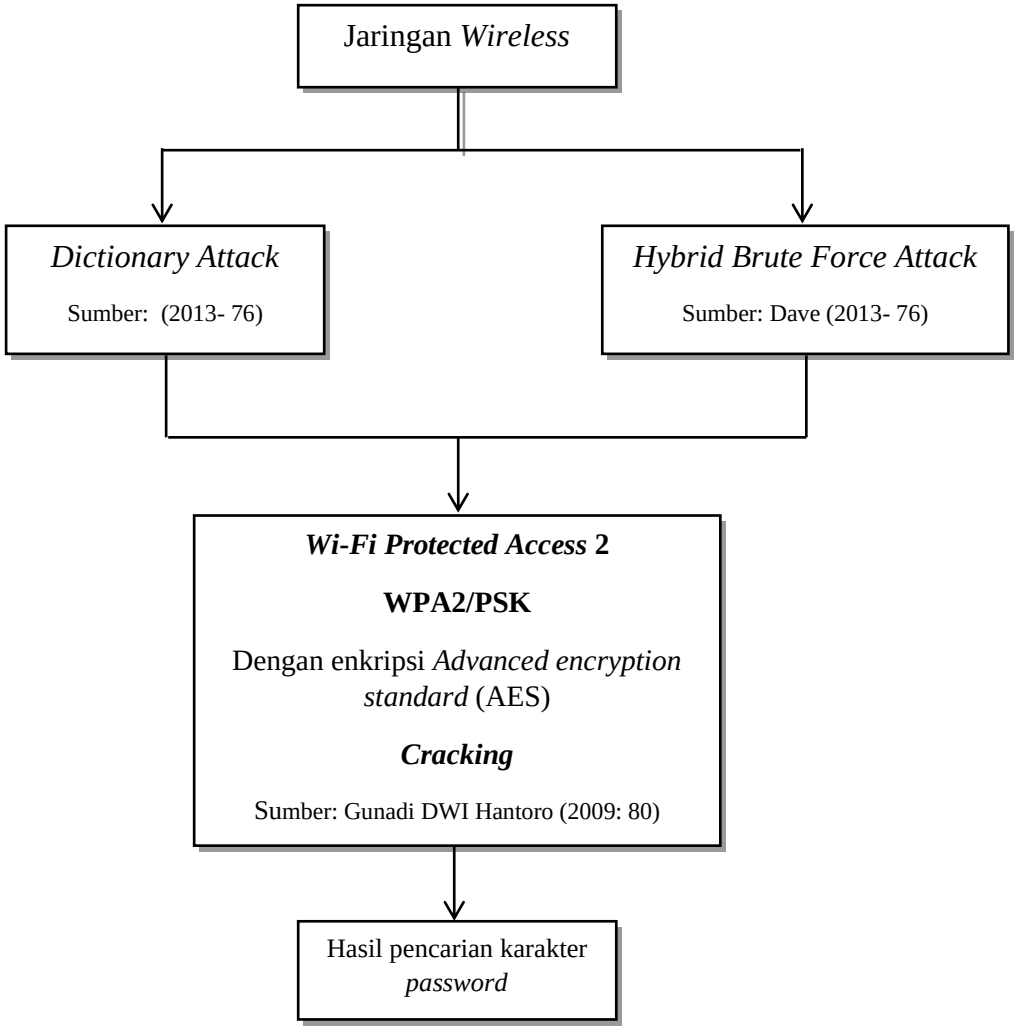
yang terus berkembang sehingga terdapat istilah yang mendampingi WLAN seperti WMAN (*Metropolitan*), WWAN (*Wide*), dan WPAN (*Personal*/*Private*).

Dengan adanya teknologi *wireless* seseorang dapat bergerak atau beraktifitas kemanan dan dimanapun untuk melakukan komunikasi data. Jaringan *wireless* merupakan teknologi jaringan komputer tanpa kabel, yaitu menggunakan gelombang berfrekuensi tinggi. Sehingga komputer- komputer itu bisa saling terhubung tanpa menggunakan kabel. Data ditransmisikan di *frekuennsi* 2.4GHz (802.11b) atau 5GHz (802.11a).

Pemakaian teknologi *wireless* secara umum dibagi atas tanpa pengamanan (*nonsecure*) dan dengan pengamanan *(Share Key / Secure)* yaitu tanpa menggunakan keamanan, dimana komputer yang memiliki pancaran gelombang dapat mendengar *transmisi* sebuah pancaran gelombang dan langsung masuk kedalam jaringan. Sedangkan *share key*, yaitu alternatif untuk pemakaian kunci atau *password*. Sebagai contoh, sebuah *network* yang mengunakan WEP.

2.4. Kerangka Pemikiran

kerangka berfikir merupakan model konseptual tentang bagaimana teori berhubungan dengan berbagai faktor yang telah diidentifikasi sebagai masalah yang penting (Sugiyono, 2012: 60)**.** Berdasarkan kerangka pemikiran diatas maka kerangka berpikir dari penelitian ini adalah sebagai berikut:



Tabel 2.5 Kerangka Pemikiran

Penelitian ini dilakukan dengan menganalisis protokol keamanan jaringan *wireless* yaitu WPA2 (Wi-Fi *Protected Access* 2) dengan menggunakan metode *Brute Force Attack* berupa *Dictionary Attack* dan *Hybrid Brute Force Attack.* Pengujian dilakukan di protokol WPA2 dengan menggunakan metode *Brute Force Attack* yang diterapkan untuk mengetahui tingkat keamanan dari protokol WPA2 pada jaringan *wireless.*

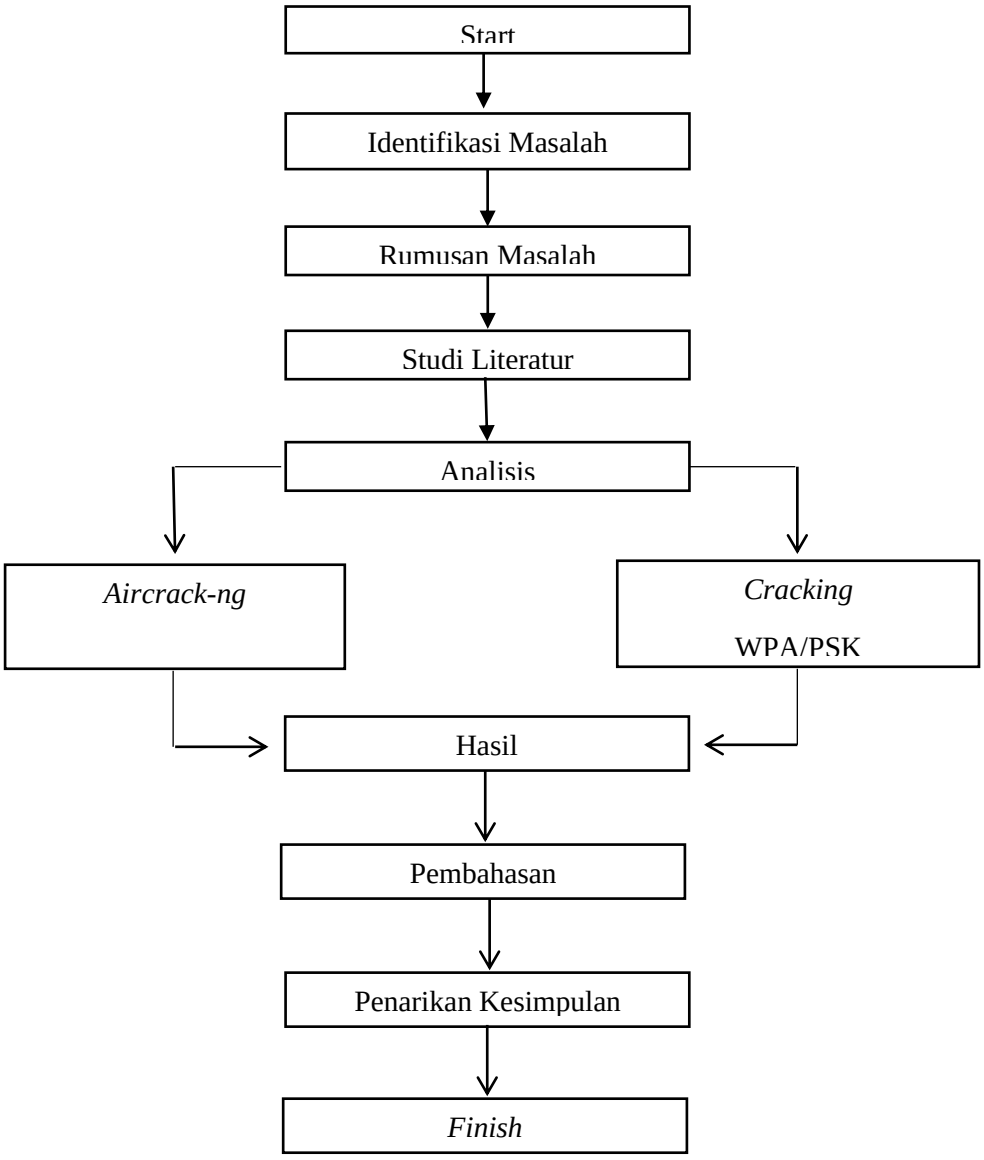
BAB III
METODE PENELITIAN

3.1. Desain Penelitian

Desain penelitian merupakan rencana induk yang berisi metode dan prosedur untuk mengumpulkan dan menganalisis informasi yang dibutuhkan, menetapkan sumber-sumber informasi, teknik yang akan digunakan, metode sampling sampai dengan analisis data untuk dapat menjawab pertanyaan-pertanyaan penelitian (Erlina, 2011:73).

Desain penelitian yang baik harus memuat hal-hal berupa rencana tentang sumber dan tipe informasi yang relevan sesuai dengan kebutuhan peneliti, strategi atau gambaran pendekatan yang digunakan dalam pengumpulan dan analisis data, serta jadwal dan anngaran penelitian yang diperlukan harus diuraikan secara jelas.

Menurut (Suryabrata, 2010: 94) penelitian *action research* atau penelitian tindakan bertujuan untuk mengembangkan keterampilan-keterampilan baru atau cara pendekatan baru dan untuk memecahkan masalah dengan penerapan langsung di dunia kerja atau dunia actual yang lain. Sedangkan menurut (Darmadi, 2011: 6) penelitian *action research* bertujuan untuk memecahkan masalah-masalah setempat dengan menggunakan metode ilmiah. Penelitian ini hanya memperhatikan masalah setempat, tidak peduli apakah hasil-hasil yang diperoleh juga dapat diberlakukan ditempat-tempat lain atau tidak.



Gambar 3.1 Desain Penelitian

Berikut adalah penjelasan dari desain penelitian yang ada pada gambar diatas:

a. Identifikasi masalah

Penelitian diawali dengan melakukan studi pendahuluan untuk mengidentifikasi permasalahan yang berkaitan dengan topik penelitian agar

peneliti mendapatkan apa yang sesungguhnya menjadi masalah untuk dipecahkan.

b. Perumusan masalah

Pada tahap ini, peneliti merumuskan masalah yang telah didapatkan secara lebih spesifik agar masalah tersebut dapat dijawab dengan baik melalui penelitian.

c. Studi Literatur

Mempelajari buku-buku dan jurnal-jurnal refrensi yang berhubungan dengan penelitian yang dijalankan, yaitu: Buku *Metode Penelitian Bisnis* (Sugiyono, 2012). Buku *Metode Penelitian Pendidikan* (Darmadi, 2011). Buku *Belajar Cepat Teori, Praktek dan Simulasi Jaringan Komputer & Internet* (Maslan, 2012). Buku *Wireless Networking: Panduan Lengkap Membangun Jaringan Wireless Tampa Teknisi* (Utomo, 2012). Buku *Mastering Wireless Penetration Testing for Highly Secured Environments* (John, 2015). Buku *Kali Linux 200% Attack* (Sto, 2014). Jurnal *Wireless Network Security Protocols A Comparative Study* (Sukhija & Gupta, 2012). Jurnal *Keamanan pada jaringan wireless* (Herdiana, 2014). Jurnal *Analisis Keamanan Jaringan Wireless Yang Menggunakan Captive Portal* (setyawan, Bangkit Kurnia Ari Syafrizal, 2012).

d. Analisis

Analisis data merupakan kegiatan setelah data dari seluruh responden atau sumber data lain terkumpul. Kegiatan dalam analisis adalah

menggelompokkan data berdasarkan variable yang diteliti, melakukan perhitungan untuk menjawab rumus (Sudaryono, 2015)

e. *Aircrack-ng*

Aircrack-ng adalah *tools auditor security* yang ditunjukan melakukan *penetrasi* pada keamanan jaringan *wireless*. *Aircrack-ng* memiliki kemampuan untuk melakukan *cracking* pada protokol 802.11 (*wireless*) dengan *endkripsi* WEP WPA/WPA2-PSK dengan berbagai metode seperti *brute force attack.*

f. *Cracking*

Kegiatan membobol suatu sistem komputer dengan tujuan mengambil atau membobol *password*. *Cracker* biasanya mencoba masuk kedalam suatu sistem komputer tampa izin, tergantung individu ini biasanya berniat jahat/buruk.

g. Hasil

Hasil diambil dari penulis setelah melakukan percobaan dengan memaparkan sebagaimana yang direncanakan atau menghadapi kendala tertentu menjelaskan kendala yang dihadapi. Penyajian hasil penelitian dapat diawali dari hasil implementasi.

h. Pembahasan

Mengungkapkan berbagai penyelesaian dari masalah-masalah yang ditetapkan sebelumnya dan memberi jawaban terhadap masalah yang akhirnya akan mengarahkan kepada kesimpulan yang akan diambil.

i. Penarikan Kesimpulan

Kesimpulan merupakan bagian penutup dari masalah yang ditunjukan kepada objek yang berhubungan dengan tujuan penulisan.

3.2. Operasional Variable

Menurut (Erlina, 2011: 48) operasional *variable* atau disebut dengan Menurut (Erlina, 2011: 48) operasional variable atau disebut dengan mendefinisikan konsep secara operasional adalah menjelaskan karakteristik dari objek ke dalam elemen-elemen yang dapat diobesrvasi yang menyebabkan konsep dapat diukur dan dioperasionalkan ke dalam penelitian. Setiap konsep variablel yang digunakan dalam penelitian harus memiliki definisi yang jelas. Dengan operasional variable, peneliti dapat mengumpulkasn, mengukur, atau menghitung informasi melalui logika empiris. Istilah-istilah dalam operasional variable harus dapat diuji dan mempunyai rujukan empiris.

3.2.1. Variabel Penelitian

Variabel penelitian adalah sesuatu yang dapat membedakan atau mengubah nilai. Nilai dapat berbeda pada waktu yang berbeda untuk objek atau orang yang sama, atau nilai dapat berubah dalam waktu yang sama untuk orang atau obyek yang berbeda (Erlina, 2011: 36)

3.2.1.1. Protokol Keamanan Jaringan *Brute Force Attack*

Pada penelitian ini *Brute Force Attack* bukanlah sebagai variable tapi berfungsi sebagai alat atau metode mengumpulkan data mengenai kelemahan *protocol* keamanan jaringan *wireless* di Kota Batam. *Brute Force Attack* melakukan serangan *Password guessing* secara terus menerus pada suatu jaringan *wireless* , Hingga *Password* tersebut didapatkan.

Tabel 3.1 *Brute Force Attack*

Variabel	**Indikator**	***Value***
Brute Force Attack	*Dictonary Attack*	*Ordinal*
	Hybrid Brute Force Attack	*Ordinal*

3.3. Objek Monitoring

Objek monitoring dalam penelitian ini adalah segala sesuatu yang dijadikan subjek atau objek penelitian yang dikehendaki peneliti. Maka yang akan dijadikan objek dalam melakukan penelitian ini sebagai berikut.

Penelitian ini dilakukan dengan menggunakan perangkat berupa *laptop Dell* dengan *system operasi Kali Linux 2.2, Processor Core i7 2.00Ghz dan RAM 6 GB.* Perangkat jaringan *wireless* yang digunakan yaitu *modem router TP-Link TD-W8151N, modem router TP-Link TD-W8101G, modem router TP-Link TD-W8951ND.* Peneliti menggunakan *Tools Airodump-ng* untuk *wireless* melakukan *capture packet data* pada jaringan *wireless* yang menggunakan protokol keamanan WPA2. Selanjutnya hasil *capture packet data* tersebut akan diuji

dengan *sotware Aircrack-ng 1.2 RC 3* untuk melakukan *capture Handshake* dan *serangan Brute Force Attack.*

3.4. Teknik Pengumpulan Data

Ada beberapa metode pengumpulan data diantaranya dari arsip/dokumentasi (data *sekunder*), wawancara (data *primer*), dan observasi (data *primer*), kuesioner (data *primer*). Secara umum, terdapat dua sumber data untuk menentukan proses pengumpulan data yang akan dilakukan yaitu data *primer* dan *sekunder*. Data *primer* merupakan data yang dikumpulkan berdasarkan interaksi langsung antara pengumpul data dan sumber data. Ada beberapa teknik pengumpulan data *primer*, yaitu *survey*, *observasi* dan *eksperimen*. Sedangkan data *sekunder* dikumpulkan dari sumber-sumber tercetak, dimana data itu telah dikumpulkan oleh pihak lain sebelumnya. Sumber data *sekunder* misalnya buku, laporan perusahaan, jurnal, internet dan sebagainya (Erlina, 2011: 31) Teknik pengumpulan data yang digunakan peneliti adalah *observasi* (data *primer*) dan kajian dokumen (data *sekunder*).

Metode *observasi* merupakan prosedur yang sistematis dan standar dalam pengumpulan data. Pemakaian cara ini didasarkan pada konsep, devinisi dan pengukuran variabelnya. Dengan observasi, peneliti dapat memperoleh ukuran variable yang bukti empirisnya dapat diambil melalui pernyataan yang di ajukan. Disini peneliti tidak hanya berkomunikasi dengan orang, tetapi juga objek penelitian yang lain (Suryabrata, 2010: 92) Observasi dalam penelitian ini melakukan pengamatan pengujian indikator protocol keamanan jaringan yaitu,

WPA2 (*Wi-Fi Protected Access 2*) terhadap serangan *Brute Force Attack* pada jaringan *wireless.*

Dalam melakukan observasi pada jaringan *wireless*, peneliti menggunakan *tools Aircrack-ng 1.2 RC 3*. Dalam penelitiaan ini menggunakan, peneliti menggunakan *tools* tersebut pada *system operasi Kali Linux 2.2*

3.5. Metode Analisis Data

Analisis data adalah proses mencari dan menyusun secara sistematis data yang diperoleh dari hasil wawancara, catatan lapangan, dan dokumentasi, dengan cara mengorganisasikan data ke dalam kategori, menjabarkan ke dalam unit-unit, melakukan sintesa, menyusun kedalam pola, memilih mana yang penting dan yang akan dipelajari, dalam membuat kesimpulan sehingga mudah dipahami oleh diri sendiri maupun orang lain (Sugiyono, 2012: 428)

3.5.1. Metode *Brute Force Attcak*

Brute Force Attack adalah metode yang digunakan untuk meretas *password* atau *kriptografi* dengan *algoritma Brute Force*. Kecepatan peretasan ini bergantung pada panjang pendeknya *password* atau *kriptografi* yang ingin dipecahkan.

Feasibilityn dari sebuah *brute force attack* tergantung dari panjangnya *chiper* yang ingin dipecahkan, dan jumlah komputasi yang tersedia untuk penyerang. Salah satu contohnya bernama *Aircrack-ng* mencoba semua kombinasi yang mungkin dari karakter yang telah didefinisikan sebelum atau set

karakter yang kustom melawan sebuah *password* yang telah terenkripsi di *brute force dialog.*

Kuncinya adalah mencoba semua kemungkinan *password* dengan *formula* seperti berikut.

$$KS = L^{(m)} + L^{(m+1)} + L^{(m+2)} + ... + L^{(M)}$$

Rumus 3.1 Rumus mencari total *password*

L = jumlah karakter yang kita ingin definsikan

m = panjang minimum dari kunci

M = panjang maksimal dari kunci

Contohnya saat kita ingin meretas sebuah *wireless pasword* dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter, dengan panjang *password* 7 maka *brute force cracker* harus mencoba KS = 26^1 + 26^2 + 26^3 + ... + 26^7 = 8353082582 kunci yang berbeda. Jika ingin meretas *password* yang sama dengan set karakter set.

Berikut metode sederhana *Brute Force Attack* Dengan karakter set “ABCDEFGHIJKLMNOPQRSTUVWXYZ” dengan jumlah 26 karakter dengan panjang *password* 2 maka *brute force* dapat melakukan kemungkinan 676 kunci yang berbeda. Dengan mencari *Password* “BC”

Tabel 3.2 Metode *Brute Force Attack* mencari “BC”

No	Password
1	AA
2	AB
3	AC
4	AD

No	Password
12	AL
13	AM
14	AO
15	AP

No	Password
24	AX
25	AY
26	AZ
27	BA

5	AE		16	AQ		28	BB
6	AF		17	AR		29	BC
7	AG		18	AS			
8	AH		19	AT			
9	AI		20	AU			
10	AJ		21	AV			
11	AK		23	AW			

Berikut metode sederhana *Brute Force Attack* Dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter dengan panjang *password* 2 maka *brute force* dapat melakukan kemungkinan 676 kunci yang berbeda. Dengan mencari *Password* "CL"

Tabel 3.3 Metode *Brute Force Attack* mencari "CL"

No	Password	No	Password	No	Password	No	Password
1	AA	17	AQ	33	BG	49	BW
2	AB	18	AR	34	BH	50	BX
3	AC	19	AS	35	BI	51	BY
4	AD	20	AT	36	BJ	52	BZ
5	AE	21	AU	37	BK	53	CA
6	AF	22	AV	38	BL	54	CB
7	AG	23	AW	39	BM	55	CC

8	AH	24	AX	40	BN	56	CD
9	AI	25	AY	41	BO	57	CE
10	AJ	26	AZ	42	BP	58	CF
11	AK	27	BA	43	BQ	59	CG
12	AL	28	BB	44	BR	60	CH
13	AM	29	BC	45	BS	61	CI
14	AN	30	BD	46	BT	62	CJ
15	AO	31	BE	47	BU	63	CK
16	AP	32	BF	48	BV	64	CL

Berikut metode sederhana *Brute Force Attack* Dengan karakter set "ABCDEFGHIJKLMNOPQRSTUVWXYZ" dengan jumlah 26 karakter dengan panjang *password* 2 maka *brute force* dapat melakukan kemungkinan 676 kunci yang berbeda. Dengan mencari *Password* "DI"

Tabel 3.4 Metode *Brute Force Attack* Mencari "DI"

No	Password	No	Password	No	Password	No	Password
1	AA	24	AX	47	BU	70	CR
2	AB	25	AY	48	BV	71	CS
3	AC	26	BZ	49	BW	72	CT
4	AD	27	BA	50	BX	73	CU
5	AE	28	BB	51	BY	74	CV

6	AF		39	BC		52	BZ		75	CW
7	AG		30	BD		53	CA		76	CX
8	AH		31	BE		54	CB		77	CY
9	AI		32	BF		55	CC		78	DZ
10	AJ		33	BG		56	CD		79	DA
11	AK		34	BH		57	CE		80	DB
12	AL		35	BI		58	CF		81	DC
13	AM		36	BJ		59	CG		82	DD
14	AN		37	BK		60	CH		83	DE
15	AO		38	BL		61	CI		84	DF
16	AP		39	BM		62	CJ		85	DG
17	AQ		40	BN		63	CK		86	DH
18	AR		41	BO		64	CL		87	DI
19	AS		42	BP		65	CM			
20	AT		43	BQ		66	CN			
21	AU		44	BR		67	CO			
22	AV		45	BS		68	CP			
23	AW		46	BT		69	CQ			

3.5.2. Pengujian *Dictionary Attack*

Dictionary Attack serangan berturut-turut dengan menggunakan daftar kata-kata, lalu mengenkripsinya, dan membandingkan dengan *one way hash* dari sistem. Jika *hash* sama, maka *password* sukses di-*crack*, dan kata itu adalah *password*.

Serangan *Brute Force* pada suatu jaringan dengan cara *Dictionary Attack* memerlukan daftar *password* dengan jumlah yang banyak. Semakin banyak jumlah *password* yang dimiliki maka kemungkinan *password* yang akan ditemukan semakin tinggi. Penulis menggunakan daftar *password* yang di buat melalu**i** *Crunch* di *Kali Linux.*

Berikut ini adalah tabel *Password List* untuk *wireless dictionary attack* di RRI Batam dengan jumlah 20 *password* dari total 282,475,249 *password* yang penulis gunakan.

Tabel 3.5 *Password List Dictionary Attack* RRI Batam

Password List Dictionary Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	aaaaaadeui	Alphabet	10
2	aaaayadeui	Alphabet	10
3	aaaayadeui	Alphabet	10
4	ddddddeui	Alphabet	10
5	ddddyadeui	Alphabet	10
6	deuayadeui	Alphabet	10
7	eeeeeeeeui	Alphabet	10
8	deeeeedeui	Alphabet	10
9	eeeeeyadeui	Alphabet	10
10	iiiiiiiiui	Alphabet	10
11	iiiiiideui	Alphabet	10
12	uuuuuuueui	Alphabet	10
13	uuuayadeui	Alphabet	10

14	ueuayadeui	Alphabet	10
15	ttuayadeui	Alphabet	10
16	tttayadeui	Alphabet	10
17	teuayadeui	Alphabet	10
18	yyyyyydeui	Alphabet	10
19	yyyayadeui	Alphabet	10
20	yeuayadeui	Alphabet	10

Berikut ini adalah tabel *Password List* untuk *wireless dictionary attack* di Indosat Batam dengan jumlah 20 *password* dari total 10,077,696 *password* yang penulis gunakan.

Tabel 3.6 *Password List Dictionary Attack* Indosat Batam

Password List Dictionary Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	3ddeemoor	Alphabet	9
2	33demoorr	Alphabet	9
3	333demmor	Alphabet	9
4	ddemmor33	Alphabet	9
5	ddddemor3	Alphabet	9
6	eeemmor33	Alphabet	9
7	eemmmmor3	Alphabet	9
8	eemmoorr3	Alphabet	9
9	meeeoorr3	Alphabet	9
10	mmeeoorr3	Alphabet	9

11	mmeeor333	Alphabet	9
12	mmeeoor33	Alphabet	9
13	mmeeorr33	Alphabet	9
14	orreomm33	Alphabet	9
15	oreoomm33	Alphabet	9
16	oredoom3	Alphabet	9
17	oredoom33	Alphabet	9
18	reedoom33	Alphabet	9
19	reddoom33	Alphabet	9
20	reddom333	Alphabet	9

Berikut ini adalah tabel *Password List* untuk *wireless dictionary attack* di Indomaret Baloi dengan jumlah 20 *password* dari total 134,217,728 *password* yang penulis gunakan.

Tabel 3.7 *Password List Dictionary Attack* Indomaret Baloi

Password List Dictionary Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	001admnrt	Alphabet	9
2	011admnrt	Alphabet	9
3	01aadmnrt	Alphabet	9
4	01addmnrt	Alphabet	9
5	1aadmnrt0	Alphabet	9
6	11admnrt0	Alphabet	9
7	1addmnr0t	Alphabet	9

8	a0dm1nnrt	Alphabet	9
9	addm0n1rt	Alphabet	9
10	admnn0r1t	Alphabet	9
11	damnrat01	Alphabet	9
12	d1ndmrat0	Alphabet	9
13	d1nd0mart	Alphabet	9
14	m1d0nar1t	Alphabet	9
15	mdnan0r1t	Alphabet	9
16	martmldor	Alphabet	9
17	martd1nd0	Alphabet	9
18	nartd1nd0	Alphabet	9
19	rtmartd10	Alphabet	9
20	tdmnn0ra1	Alphabet	9

Pengujian *Dictionary Attack* dilakukan dengan *software Aircrack-ng* 1.2 RC 3. Hasil pengujian dari *Dictionary Attack* dirumuskan dalam bentuk tabel.

3.5.3. Pengujian *Hybrid Brute Force Attack*

Hybrid Brute Force Attack merupakan serangan berturut-turut dengan menggunakan daftar kata-kata dalam kamus yang telah dimodifikasi. *Password* dimodifikasi dengan menambahkan pada *password* list kemungkinan *password* yang digunakan oleh pemilik jaringan *wireless* yang di *attack*.

Berikut adalah *password* yang penulis modifikasi untuk *Hybrid Brute Force Attack* dengan jumlah 20 *password* dari total 92,600 *password* yang digunakan:

Tabel 3.8 *Password List Hybrid Brute Force Attack*

Password List Hybrid Brute Force Attack			
No	***Password***	**Jenis *Password***	**Panjang *Characters***
1	Chocoverona	Alphabet	11
2	poldakepri123	Alphanumeric	13
3	Lewishamilton	Alphabet	13
4	Teuayadeui	Alphabet	10
5	Barcelona	Alphabet	9
6	Zakizari678	Alphanumeric	11
7	Rachmimustar6	Alphanumeric	13
8	Rriindonesia	Alphabet	12
9	Kapoldabatam	Alphabet	12
10	Indomaret9966	Numeric	13
11	Speedy123	Alphanumeric	9
12	Admin123	Alphanumeric	8
13	Love123456	Alphanumeric	10
14	Administrator	Alphabet	13
15	Samsung123	Alphanumeric	10
16	Internet	Alphabet	8
17	Sweetlove	Alphabet	9
18	Cafe9876	Alphanumeric	8
19	Afterall79	Alphanumeric	10
20	Aircraft3340	Alphanumeric	12

Pengujian *Hybrid Brute Force Attack* dilakukan dengan *software Aircrack-ng 1.2 RC 3*. Hasil pengujian dari *Hybrid Brute Force Attack* dirumuskan dalam bentuk tabel.

3.5.4. Pengujian Protokol Keamanan WPA2

Wi-FI *Protected Access* (WPA2) menerapkan standar IEEE 802.11i dan merupakan pengembangan lebih dari WPA. WPA2 diperkenalkan pada bulan September 2004 oleh Wi-Fi *Alliance*. Pengujian ini dilakukan pada beberapa lokasi di Kota Batam yaitu kantor RRI Batam, Indomaret Baloi, Indosat Batam Center.

Pengujian dilakukan dengan *tools Aircrack-ng* 1.2 RC 3. Untuk melakukan serangan *dictionary Attack dan Hybrid Brute Force Attack.* Hasil dari pengujian protokol keamanan WPA2 dirumuskan dalam bentuk tabel.

Tabel 3.9 Data Protokol Keamanan WPA2

Lokasi	Lokasi pengujian *Dictionary Attack* dan *Hybrid Brute Force Attack*
Password	*Password* yang digunakan pada jaringan *wireless*
Jenis *Password*	Jenis *password* yang digunakan terdiri dari *alphabet, numeric* dan *alphanumeric*
Panjang *Password*	Panjang karakter *password* yang digunakan
Posisi *Password*	Posisi *password* yang ditemukan pada *password list*
k/s (key/second)	Kecepatan *Dictionary Attack* dan *Hybrid Brute Force Attack* melakukan *brute force password* pada jaringan *wireless* per detik

Password Ditemukan	Berhasil atau tidak serangan *Dictionary Attack* dan *Hybrid Brute Force Attack* yang dilakukan pada jaringan *wireless*

3.6. Lokasi dan jadwal Penelitian

Lokasi dan jadwal penelitian ini berdasarkan lokasi dan jadwal yang sudah dijalani oleh peneliti dimulai dari penginputan judul penelitian sampai dengan sebelum batas akhir pengumpulan hasil penelitian.

3.6.1. Lokasi

Penelitian dilakukan pada jaringan wireless yang menggunakan protokol keamanan jaringan WPA2 *(Wi-Fi Protected Access 2)*, yang berada di kota batam diantaranya kantor RRI Batam Center, Indomaret Baloi, Kantor Indosat Batam Center

3.6.2. Jadwal Penelitian

Penelitian ini dilakukan pada tanggal Maret 2017 sampai Agustus 2017. Pengumpulan data tidak akan menggangu aktivitas yang sedang dilakukan oleh responden dan disesuaikan dengan jadwal penelitian yang terjadwal.

Tabel 3.10 Jadwal Penelitian

No	Kegiatan	Tahun 2016 – 2017																							
		Maret 2017				April 2017				Mei 2017				Juni 2017				Juli 2017				Agustus 2017			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Penyusunan Pendahuluan																								
2	Penyusunan Tinjauan Pustaka																								
3	Penyusunan Metode Penelitian																								
4	Hasil Penelitan dan Pembahasan																								
5	Simpulan dan Saran																								