ANALISIS KELEMAHAN CELAH LAPISAN KEAMANAN PADA JARINGAN NIRKABEL

Rico, S.Kom, M.S.I
Teknik Informatika, STIKOM Dinamika Bangsa
email : reecho86@gmail.com

Abstrak

Pemakaian perangkat teknologi berbasis nirkabel pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi nirkabel 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 digunakan oleh user maupun oleh operator yang memberikan layanan komunikasi. Kelemahan jaringan nirkabel secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan nirkabel terbentang di atas empat layer dimana keempat lapis (layer) tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media nirkabel. Keempat lapisan tersebut adalah lapisan fisik, lapisan jaringan, lapisan user, dan lapisan aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapisan pada teknologi nirkabel tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasifasilitas MAC filtering, pemasangan infrastruktur captiveportal.

The use of wireless devices based on the technology are now so many , whether used for voice and data communications . Due to utilize wireless technology to deliver a high -frequency communications , the security vulnerability was also higher than with other communication technologies . Various security measures can be carried out via the communication device used by the user or by operators who provide communication services . The weakness of a wireless network can be generally divided into two types , namely the weakness in the configuration and weaknesses on the type of encryption used . Broadly speaking , a gap in wireless network spread over four layers where the fourth tier (layer) is actually a process of the data communication on the wireless medium . The fourth layer is the physical layer , network layer , user layer and application layer . Security management models that occur at each layer of the wireless technologies that can be done for example by way of hiding the SSID , utilizing a WEP key, WPA - PSK or WPA2 - PSK , MAC filtering implementations facilities , infrastructure installation captiveportal.

Keywords: Networking, Wireless, Encryption

1. Pendahuluan

1.1 Latar Belakang Masalah

Teknologi jaringan nirkabel sebenarnya terbentang luas mulai dari komunikasi suara sampai dengan jaringan data, yang mana membolehkan pengguna untuk membangun koneksi nirkabel pada suatu jarak tertentu. Ini termasuk teknologi infrared, frekuensi radio dan lain sebagainya. Peranti yang umumnya digunakan untuk jaringan nirkabel termasuk di dalamnya adalah komputer, komputer genggam, PDA, telepon seluler, tablet PC dan lain sebagainya. Teknologi nirkabel ini memiliki kegunaan yang sangat banyak. Contohnya, pengguna mengakses website melalui seluler yang berada di area hotspot.

Disamping biaya dan instalasi yang mudah, jaringan nirkabel memiliki kelemahan pada jenis konfigurasi fan kelemahan pada enkripsi. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan nirkabel cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan jaringan nirkabel yang masih menggunakan konfigurasi bawaan vendor. Sering ditemukan jaringan nirkabel yang dipasang pada jaringan masih menggunakan konfigurasi standar vendor seperti SSID, IP Address, remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user (password) untuk administrasi jaringan nirkabel tersebut.

WEP (Wired Equivalent Privacy) yang menjadi standar keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia gratis di internet. WPA-PSK dan

LEAP yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode dictionary attack secara offline.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dirumuskan permasalahan pokok dalam penelitian ini adalah "Bagaimana cara mengurangi dan mengatasi celah keamanan jaringan nirkabel".

1.3 Pembatasan Masalah

Agar penelitian ini sesuai dengan yang direncanakan maka perlu diberikan batasan yang meliputi :

1. Analisa yang dilakukan pada celah keamanan jaringan nirkabel (802.11 a/b/g).
2. Perangkat yang diteliti adalah access point.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah menganalisa kelemahan jaringan nirkabel serta mencari solusi untuk mengatasi kelemahan jaringan nirkabel.

2. Landasan Teori

2.1 Jaringan Nirkabel / Wireless Network

Wireless network merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Pada dasarnya wireless dengan LAN merupakan sama-sama jaringan komputer yang saling terhubung antara satu dengan lainnya, yang membedakan antara keduanya adalah media jalur lintas data yang digunakan, jika LAN masih menggunakan kabel sebagai media lintas data, sedangkan wireless menggunakan media gelombang radio/udara. Penerapan dari aplikasi wireless network ini antara lain adalah jaringan nirkabel diperusahaan, atau mobile communication seperti handphone, dan HT.

Adapun pengertian lainnya adalah sekumpulan standar yang digunakan untuk Jaringan Lokal Nirkabel (Wireless Local Area Networks – WLAN) yang didasari pada spesifikasi IEEE 802.11. Terdapat tiga standard tersebut yaitu 802.11b atau dikenal dengan WIFI (Wireless Fidelity),802.11a (WIFI5), dan 802.11. ketiga standard tersebut biasa di singkat 802.11a/b/g. Versi wireless LAN 802.11b memilik kemampuan transfer data kecepatan tinggi hingga 11Mbps pada band frekuensi 2,4 Ghz. Versi berikutnya 802.11a, untuk transfer data kecepatan tinggi hingga 54 Mbps pada frekuensi 5 Ghz. Sedangkan 802.11g berkecepatan 54 Mbps dengan frekuensi 2,4 Ghz.

2.2 Wireless LAN

Wireless Local Area Network pada dasarnya sama dengan jaringan Local Area Network yang biasa kita jumpai. Hanya saja, untuk menghubungkan antara node device antar client menggunakan media wireless, chanel frekuensi serta SSID yang unik untuk menunjukkan identitas dari wireless device.

2.3 Komponen pada WLAN

Untuk bisa mengembangkan sebuah mode WLAN, setidaknya diperlukan empat komponen utama yang harus disediakan, yaitu :

1. Access Point

   Access Point akan menjadi sentral komunikasi antara PC ke ISP, atau dari kantor cabang ke kantor pusat jika jaringan yang dikempangkan milik sebuah korporasi pribadi. Access Point ini berfungsi sebagai konverter sinyal radio yang dikirimkan menjadi sinyal digital yang akan disalurkan melalui perangkat WLAN lainnya untuk kemudian akan dikonversikan kembali menjadi sinyal radio oleh receiver.

2. Wireless LAN Interface

   Alat ini biasanya merupakan alat tambahan yang dipasangkan pada PC atau Laptop.Namun pada beberapa produk laptop tertentu, interface ini biasanya sudah dipasangkan pada saat pembeliannya. Namun interface ini pula bisa diperjual belikan secara bebas dipasaran dengan harga yang beragam. Disebut juga sebagai Wireless LAN Adaptor USB.

3. Mobile/Desktop PC

Perangkat akses untuk pengguna (user) yang harus sudah terpasang media Wireless LAN interface baik dalam bentuk PCI maupun USB.

4. Antena External, digunakan untuk memperkuat daya pancar. Antena ini bisa dirakit sendiri oleh client (user), misal : antena kaleng.

2.4 Enkripsi (*Encryption*)

Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet e-commerce, jaringan Telepon bergerak dan ATM pada bank.

Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, Message Authentication Code (MAC) atau digital signature. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer.

3. Analisa dan Pembahasan

3.1 Masalah Keamanan Jaringan Nirkabel

Beberapa hal yang mempengaruhi aspek keamanan dari sistem wireless antara lain:

1. Perangkat pengakses informasi yang menggunakan sistem nirkabel biasanya berukuran kecil sehingga mudah dicuri. Seperti notebook, PDA, handphone, dan sejenisnya sangat mudah dicuri. Jika tercuri maka informasi yang ada di dalamnya (atau kunci pengakses informasi) bisa jatuh ke tangan orang yang tidak berhak.
2. Penyadapan pada jalur komunikasi (*man in the middle attack*) dapat dilakukan lebih mudah karena tidak perlu mencari jalur kabel untuk melakukan hubungan. Sistem yang tidak menggunakan pengamanan enkripsi dan otentikasi, atau menggunakan enkripsi yang mudah dipecahkan akan mudah ditangkap.
3. Perangkat wireless yang kecil membatasi kemampuan perangkat dari sisi CPU, RAM, kecepatan komunikasi, catudaya. Akibatnya sistem pengamanan, misalnya enkripsi yang digunakan harus memperhatikan batasan ini. Saat ini tidak memungkinkan untuk menggunakan sistem enkripsi yang canggih membutuhkan CPU cycle yang cukup tinggi sehingga memperlambat transfer data.
4. Pengguna tidak dapat membuat sistem pengaman sendiri (membuat enkripsi sendiri) dan hanya bergantung kepada vendor (pembuat perangkat) tersebut. Namun mulai muncul perangkat handphone yang dapat diprogram oleh pengguna. Begitu juga saat ini notebook sudah menggunakan pengaman otentikasi akses dengan sistem biometric.
5. Adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas. DoS attack dapat dilakukan dengan menginjeksikan traffic palsu.
6. Saat ini fokus dari sistem wireless adalah untuk mengirimkan data secepat mungkin. Adanya enkripsi akan memperlambat proses pengiriman data sehingga penggunaan enkripsi masih belum mendapat prioritas. Setelah kecepatan pengiriman data sudah memadai dan harganya menjadimurah, barulah akan melihat perkembangan disisi pengamanan dengan menggunakan enkripsi.

3.2 Kelemahan Pada Lapisan Jaringan Nirkabel

Pada setiap lapisan proses komunikasi data melalui media nirkabel terdapat celah-celah yang menunggu untuk dimasuki. Maka itu, keamanan jaringan nirkabel menjadi begitu lemah dan perlu dicermati dengan ekstra teliti. Lapisan-lapisan beserta kelemahannya tersebut adalah sebagai berikut:

1. *Physical Layer*. Seperti diketahui, Lapisan fisik dari komunikasi data akan banyak berbicara seputar media pembawa data itu sendiri. Di dalam sistem komunikasi data nirkabel, yang menjadi media perantaranya tidak lain adalah udara bebas. Di dalam udara bebas tersebut, data yang berwujud sinyal-sinyal radio dalam frekuensi tertentu lalu-lalang dengan bebasnya. Tentu sudah bisa dibayangkan bagaimana rentannya keamanan data tersebut karena lalu-lalang di alam bebas. Siapa saja mungkin bisa menangkapnya, menyadapnya, bahkan langsung membacanya tanpa sepengetahuan. Jika hanya untuk penggunaan pribadi yang sekadar iseng-iseng saja, disadap atau dibaca oleh orang lain tentu tidak akan terlalu berbahaya meskipun agak menjengkelkan juga. Namun, bagaimana jika kelemahan- kelemahan ini terdapat pada jaringan nirkabel perusahaan yang didalamnya terdapat berbagai transaksi bisnis, proyek- proyek perusahaan, info-info rahasia, rahasia

keuangan, dan banyak lagi informasi sensitif di dalamnya. Tentu penyadapan tidak dapat ditoleransi lagi kalau tidak mau perusahaan menjadi bulan-bulanan orang.

2. *Network Layer*, biasanya akan banyak berbicara seputar perangkat-perangkat yang memiliki kemampuan untuk menciptakan sebuah jaringan komunikasi yang disertai juga dengan sistem pengalamatannya. Pada jaringan komunikasi nirkabel, perangkat yang biasa digunakan sering disebut dengan istilah AccessPoint atau disingkat AP. Sistem pengalamatan IP tentu akan banyak ditemukan pada perangkat ini. Karena melayani komunikasi menggunakan media bebas yang terbuka, maka AP-AP tersebut juga dapat dikatakan sebagai perangkat yang terbuka bebas. Perangkat jaringan yang tidak diverifikasi dan dikontrol dengan baik akan dapat menjadi sebuah pintu masuk bagi para pengacau. Mulai dari hanya sekadar dilihat-lihat isinya, diubah sedikit-sedikit, sampai dibajak penuhpun sangat mungkin dialami oleh sebuah AP. Untuk itu, perlu diperhatikan juga keamanan AP-AP pada jaringan nirkabel yang ada. Selain itu, komunikasi antar-AP juga harus dicermati dan perhatikan keamanannya.
3. *User Layer*. Selain keamanan perangkat jaringan yang perlu diperhatikan, juga perlu diperhatikan dan dicermati siapa-siapa saja yang mengakses jaringan nirkabel yang ada. Jaringan nirkabel memang menggunakan media publik untuk lalu-lintas datanya, namun jika jaringan yang ada bukan merupakan jaringan publik yang dapat diakses oleh siapa saja, tentu harus ada batasan-batasan pengaksesnya.Tidak sulit bagi para pengguna yang tidak berhak untuk dapat mengakses sebuah jaringan wireless. Jika sembarangan pengguna dapat menggunakan jaringan yang ada, tentu hal ini akan sangat merugikan para pengguna lain yang memang berhak. Sebuah jaringan wireless yang baik harus memiliki kepastian bahwa hanya para pengguna yang dikenal, yang dipercaya, dan yang memang berhak dapat mengakses jaringan tersebut. Perangkat-perangkat jaringan yang biasa bergabung dalam jaringan nirkabel tersebut juga harus dapat di-track dan dimonitor dengan benar, karena hal ini akan sangat berguna untuk kepentingan monitoring, accounting,untuk mengetahui tren-tren yang terjadi dalam jaringan yang ada,danbanyak lagi.
4. *Application Layer,* jaringan yang menggunakan media kabel saja dapat membuka celah-celah yang ada pada aplikasi dengan cukup lebar, apalagi jaringan nirkabel yang memang rentan di seluruh layer-nya. Aplikasi-aplikasi bisnis yang penggunaannya lalu-lalang melalui media wireless tentu sangat rentan keamanannya, baik sekadar disusupi maupun di DoS (*denial of service*). Untuk itu, jaringan nirkabel yang baik harus juga dapat melindungi aplikasi-aplikasi yang berjalan di dalamnya agar tidak dengan mudahdikacaukan.

3.3 Celah Lapisan Jaringan Nirkabel

Berikut ini adalah beberapa celah yang sangat umum terdapat di dalam sebuah jaringan wireless mulai dari layer yang paling bawah:

1. Physical layer

- Bleeding Coverage Area. Seperti diketahui, sinyal radio yang dipancarkan oleh Access Point (AP) berpropagasi dalam berbentuk tiga dimensi, memiliki panjang jangkauan, lebar jangkauan, dan tinggi jangkauan. Sinyal radio cukup sulit untuk diketahui dan diprediksi area-area mana saja yang dapat dijangkaunya. Melihat hal ini, sangatlah mungkin bagi sebuah jaringan wireless untuk dapat melebarkan jangkauannya di luar dari batasan-batasan fisik yang dibutuhkan. Misalnya, memasang sebuah AP di ruangan kantor untuk meng-cover seluruh ruangan kantor, namun kenyataannya kantor tetangga yang berada tepat disebelah, juga masih dapat menggunakan jaringan nirkabel ini. Inilah yang disebut dengan bleeding coverage area. Dengan adanya coverage area yang tidak diinginkan ini, Resource- resource sensitif perusahaan akan sangat berpotensial untuk dieksploitasi oleh orang-orang luar dengan perangkat wireless-nya. Bahkan ada juga beberapa orang yang dengan sengaja mencari-cari bleeding coverage area ini untuk digunakan dan dieksploitasi. Apayang dilakukan oleho rang-orang ini sering disebut dengan istilah *war driving*.
- AP External Pengacau. Para pengguna yang memiliki perangkat wireless di PC, notebook, PDA, ponsel, dan banyak lagi memiliki kemungkinan untuk berasosiasi dengan AP manapun selama AP tersebut memang meng-cover lokasi dimana perangkat tersebut berada dan juga memberikan izin. Jika berada di dalam jaringan wireless yang dipancarkan oleh AP kantor, tentunya harus terkoneksi ke kantor tersebut. Namun, apa jadinya jika ada sebuah AP milik orang lain yang area coverage-nya juga menjangkau perangkat yang ada. Kemudian perangkat yang ada tersebut tanpa

atau dengan disadari berasosiasi dengan external AP tersebut. Apa yang akan terjadi? Tentunya akan terkoneksi kedalam jaringan external tersebut yang tidak ketahui ada apa dibalik jaringan tersebut. Dari segi keamanan, hal ini sangat berbahaya karena mungkin tanpa disadari memberikan data sensitif, misalnya password-password otentikasi yang sebenarnya harus diketikkan di dalam jaringan wireless yang sesungguhnya. Atau mungkin saja ketika sudah terkoneksi kedalam jaringan wireless external tersebut, perangkat yang ada akan segera dieksploitasi dan data dicuri. Atau mungkin juga jaringan tersebut memberikan koneksi internet untuk digunakan, namun dengan dilengkapi packet sniffer dan penyadap-penyadap canggih lainnya sehingga semua transaksi internet dapat diketahui oleh oranglain. Jika sudah berada dalam kondisi ini, sudah dapat dikatakan sebagai korban pencurian yang tanpa disadari masuk sendiri ke dalam sarang pencuri atau mungkin juga jaringan tersebut memberikan koneksi internet untuk digunakan dengan dilengkapi packet sniffer dan penyadap-penyadap canggih lainnya sehingga semua transaksi internet dapat diketahui oleh orang lain. Selain itu,adanyaAP external yang area coverage-nya masuk kedalam area tentu juga dapat menyebabkan interferensi terhadap sinyal-sinyal komunikasi jaringan yang ada. Interferensi ini tentu akan sangat mempengaruhi performa dan kelangsungan jaringan nirkabel ini.

2. *Network layer*

- Rogue AP merupakan kumpulan beberapa AP-AP yang tidak diketahui atau tidak terdaftar keberadaannya oleh para administrator sebuah jaringan wireless. Atau mungkin bisa juga disebut dengan istilah AP liar. AP-AP liar ini sangat berbahaya sekali bagi keamanan jaringan nirkabel karena AP-AP ini memang tidak pernah diinginkan keberadaannya. Selain mengganggu keamanan, tentu juga bisa mengganggu sinyal-sinyal pembawa data pada frekuensi tertentu. Biasanya keberadaan AP liar ini cukup sulit untuk dicegah karena ketidakpastian area yang dijangkau oleh sebuah jaringan wireless, apalagi untuk yang berskala besar. Secara umum, ada dua sumber yang dapat membuat rogue AP muncul di dalam jaringan wireless yang ada:

  1. Operator atau karyawan yang tidak melakukan operasi secara prosedural. Untuk alasan memudahkan pekerjaannya atau untuk penggunaan pribadi, seringkali terjadi dimana seorang karyawan diam-diam memasang sebuah AP untuk dapat terkoneksi ke dalam jaringan internal. Sehingga ia bisa mendapatkan koneksi ke dalam jaringan dari mana saja di sekitarnya. Kebanyakan AP yang digunakan oleh perorangan ini merupakan AP kelas konsumer di mana fitur-fitur sekuritinya tidak lengkap atau bahkan tidak ada. Bisa juga jika memang ada, Tidak di setting dengan benar atau tidak sesuai dengan standar karena ketidaktahuannya. Padahal seluruh AP sudah diamankan oleh para administrator dengan standar-standar yang berlaku diperusahaan tersebut. Dengan adanya AP "bandel" ini, maka terbukalah sebuah gerbang di mana orang-orang dari luar dapat masuk ke dalam jaringan dengan begitu mudahnya. Mereka memiliki hak akses dan kemampuan yang sama dalam memanfaatkan sumber- sumber di dalam jaringan.

  2. *Hacker*. Selain karyawan, para hacker yang dengan sengaja meninggalkan perangkat APnya di dalam jaringan kantor juga bisa terjadi. Jika dikantor memang disediakan port-port ethernet yang dapat digunakan untuk umum, maka ini juga perlu diwaspadai karena mungkin saja para hacker diam- diam menancapkan AP-nya dan kemudian menyembunyikannya, sehingga ia masih dapat mengakses jaringan nirkabel meskipun secara fisik ia sudah meninggalkan ruangan.

- *Fake* AP. Arti secara harafiahnya AP palsu, merupakan sebuah teknik pencurian hak akses oleh sebuah AP untuk dapat tergabung ke dalam sebuah jaringan wireless dan ikut melayani para penggunanya. Tidak hanya melayani penggunanya, AP-AP lain juga mungkin akan berasosiasi dengan AP ini. Hal ini disebabkan karena mungkin pemilik AP palsu tersebut berhasil mendapatkan SSID dari jaringan wireless tersebut dan menggunakan AP-nya untuk mem- broadcast SSID itu. Sehingga pengguna akan melihat SSID yang sama baik dari AP yang sebenarnya maupun dari AP yang palsu. Jika pengguna tersebut

tergabung dalam jaringan AP yang palsu, maka datanya akan dengan mudah dapat dicuri. Lebih parahnya lagi, jika AP ini juga memiliki kemampuan memalsukan alamat MAC dari sebuah AP sebenarnya yang ada di dalam jaringan tersebut. Dengan alamat MAC yang disamakan dengan MAC dari AP sebenarnya, AP palsu akan dikenal sebagai AP yang memang telah diotorisasi di dalam jaringan tersebut. Akibatnya AP palsu tersebut dapat juga berasosiasi dengan AP-AP lain dan diperlakukan seperti halnya AP yang sebenarnya. Ini akan sangat berbahaya karena informasi login, otentikasi, dan banyak lagi dapat diambil oleh penggunaAP palsu ini. Bahkan jika bisa berasosiasi dengan AP lainnya, lebih banyak lagi yang dapat dilakukan.

3.4 Model Solusi

Dengan adanya kelemahan dan celah keamanan seperti di atas, beberapa kegiatan dan aktifitas yang dapat dilakukan untuk mengamankan jaringan nirkabel sebagai berikut:

1. Menyembunyikan SSID. Dengan menyembunyikan *Services Set Id* (SSID) jaringan nirkabel 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 nirkabel, maka client akan tetap mengirimkan SSID dalam bentuk plain text (meskipun menggunakan enkripsi), sehingga jika bermaksud menyadapnya, dapat dengan mudah menemukan informasi tersebut. Beberapa tools yang dapat digunakan untuk mendapatkan ssid yang disembunyikan antara lain, kismet (kisMAC), ssid_jack (airjack), aircrack, void11 dan masih banyak lagi.
2. Menggunakan kunci WEP. WEP merupakan standart keamanan dan enkripsi pertama yang digunakan pada jaringan nirkabel, WEP memiliki berbagai kelemahan antara lain:

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

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- coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika *pass phrase* yang digunakan wireless tersebut memang terapat pada kamus kata yang digunakan si *hacker*. Untuk mencegahnya menggunakan WPA-PSK, gunakanlah *pass phrase* yang cukup panjang (satu kalimat).
4. Memanfaatkan Fasilitas MAC Filtering. Hampir setiap AP maupun router difasilitasi dengan keamanan MAC Filtering. Hal ini sebenarnya tidak banyak membantu dalam mengamankan komunikasi wireless, karena MAC address sangat mudah dispoofing atau bahkan dirubah. Tools ifconfig pada OSLinux/Unix atau beragam tool ssptnetwork utilitis, regedit, smac, machange pada OS windows dengan mudah digunakan untuk spoofing atau mengganti MAC address. Masih sering ditemukan wifi diperkantoran dan bahkan ISP (yang biasanya digunakan oleh warnet-warnet) yang hanya menggunakan proteksi MAC Filtering. Dengan menggunakan aplikasi war driving seperti kismet/kisMAC atau aircracktools, dapat diperoleh informasi MACaddress tiap client yang sedang terhubung ke sebuah AP. Setelah mendapatkan informasi tersebut, dapat terhubung ke AP 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/otentikasi
6. Memakai Enkripsi. Enkripsi adalah ukuran security yang pertama, tetapi banyak *wireless access points* (WAPs) tidak menggunakan enkripsi sebagai defaultnya. Meskipun banyak WAP telah memiliki *Wired Equivalent Privacy*(WEP) protocol, tetapi secara default tidak diaktifkan. WEP memang mempunyai beberapa lubang di securitynya, dan seorang hacker yang berpengalaman pasti dapat membukanya, tetapi itu masih tetap lebih baik daripada tidak ada enkripsi sama sekali.

Pastikan untuk men-set metode WEP authentication dengan "shared key" daripada "open system". Untuk "open system", tidak meng-encrypt data, tetapi hanya melakukan otentifikasi client. Ubah WEP key sesering mungkin, dan pakai 128-bit WEP dibandingkan dengan yang 40-bit.

7. Gunakan Enkripsi yang kuat. Karena kelemahan-kelemahan yang ada di WEP, maka dianjurkan untuk menggunakan *Wi-Fi* Protected *Access*(WPA) juga. Untuk memakai WPA, WAP harus mendukungnya. Sisi *client* juga harus dapat men-support WPA tsb.
8. Ganti password admin standar. Kebanyakan pabrik menggunakan password admin yang sama untuk semua WAP produk mereka. Default password tersebut umumnya sudah diketahui oleh para hacker, yang nantinya dapat menggunakannya untuk merubah setting di WAP. Hal pertama yang harus dilakukan dalam konfigurasi WAP adalah mengganti password default. Gunakan paling tidak 8 karakter, kombinasi antara huruf dan angka, dan tidak menggunakan kata-kata yang ada dalam kamus.
9. Matikan SSID Broad casting. Service Set Identifier (SSID) adalah nama dari wireless network. Secara default, SSID dari WAP akan di broadcast. Hal ini akan membuat user mudah untuk menemukan nya, karena SSID akan muncul dalam daftar available networks yang ada pada wireless client. Jika SSID dimatikan, user harus mengetahui lebih dahulu SSID-nya agak dapat terkoneksi dengan jaringan tersebut.
10. Matikan WAP saat tidak dipakai. Cara yang satu ini kelihatannya sangat simpel, tetapi beberapa perusahaan atau individual melakukannya. Jika mempunyai user yang hanya terkoneksi pada saat saat tertentu saja, tidak ada alasan untuk menjalankan wireless network setiap saat dan menyediakan kesempatan bagi hacker untuk melaksanakan niat jahatnya. AP (*Access Point*) dapat dimatikan pada saat tidak dipakai.
11. Ubah default SSID. Kegunaan dari mematikan broadcast SSID adalah untuk mencegah orang lain tahu nama dari network, tetapi jika masih memakai default SSID, tidak akan sulit untuk menerka SSID dari network.
12. Memakai MAC Filtering. Kebanyakan WAP (bukan yang murah-murah tentunya) akan memperbolehkan memakai filter media access control(MAC). Ini artinya dapat membuat "white list" dari client yang boleh mengakses wireless network, berdasarkan dari MAC atau alamat fisik yang ada di network card masing masing client. Koneksi dari MAC yang tidak ada dalam list akan ditolak. Metode ini tidak selamanya aman, karena masih mungkin bagi seorang hacker melakukan sniffing paket yang transmit via wireless network dan mendapatkan MAC address yang valid dari salah satu user, dan kemudian menggunakannya untuk melakukan spoof. Tetapi MAC filtering akan membuat kesulitan seorang hacker.
13. Mengisolasi Wireless Network dari LAN. Untuk memproteksi internal network dari ancaman yang datang dari wireless network, perlu kiranya dibuat wireless DMZ atau parameter network yang mengisolasi dari LAN. Artinya adalah memasang firewall antara wireless network dan LAN. Dan untuk wireless client yang membutuhkan akses ke internal network, dia haruslah melakukan otentifikasi dahulu dengan RAS server atau menggunakan VPN. Hal ini menyediakan extra layer untuk proteksi.
14. Mengontrol Signal Wireless. 802.11b WAP memancarkan gelombang sampai dengan kira-kira 300 feet. Tetapi jarak ini dapat ditambahkan dengan cara mengganti antenna dengan yang lebih bagus. Dengan memakai high gain antena, bisa mendapatkan jarak yang lebih jauh. Directional antenna akan memancarkan sinyal ke arah tertentu, dan pancarannya tidak melingkar seperti yang terjadi di antenna omni directional yang biasanya terdapat pada paket WAP standard. Selain itu, dengan memilih antenna yang sesuai, dapat mengontrol jarak sinyal dan arahnya untuk melindungi diri dari hakcer. Sebagai tambahan, ada beberapa WAP yang bisa disetting kekuatan sinyal dan arahnya melalui config WAP tersebut.
15. Memancarkan Gelombang pada frekuensi yang berbeda. Salah satu cara untuk bersembunyi dari hacker yang biasanya memakai teknologi 802.11b/g yang lebih popular adalah dengan memakai 802.11a, karena 802.11a bekerja pada frekwensi yang berbeda (yaitu difrekwensi 5GHz), NIC yang didesain untuk bekerja pada teknologi yang popular tidak akan dapat menangkap sinyal tersebut.

Jaringan nirkabel merupakan salah satu bentuk jaringan yang proses komunikasi datanya menggunakan frekuensi dengan bantuan udara. Teknologi yang digunakan dalam jaringan nirkabel adalah 802.11a/b/g dan yang terbaru adalah n, dimana teknologi tersebut memiliki frekuensi dan coverage area berbeda.

Dalam penelitian ini teknologi yang digunakan 802.11 a/b/g dimana terdapat beberapa celah dan kelemahan dari keamanan jaringan pada tiap layer komunikasi data yaitu physical layer, network layer, user layer, dan application layer.

Dari beberapa kelemahan tiap-tiap layer bisa diatasi dengan menggunakan enkripsi yang handal, mengganti password default admin, mematikan SSID broadcasting, mengganti default SSID, menggunakan MAC filtering, mengisolasi wireless network dari LAN, menggunakan gelombang pada frekuensi yang berbeda.

DAFTAR PUSTAKA

[1] William, Stalings, 1999, *Cryptography and Network Security : Principles and Practice*, 2nd Eddition, PrenticeHall, Inc.

[2] Edney,Jon and William A. Arbaugh E.2004. *Real8002.11 Security:WiFi Protrcted Access and 802.11i.* Boston: Addison Wesley

[3] http://hamdan-fr.blogspot.com/2012/12/analisis-kelemahan-keamanan-pada.html

[4] http://maulanagilbert.blogspot.com/2013/10/jurnal-analisis-kelemahan-teknologi.html

[5] http://id.wikipedia.net