ANALISIS KEAMANAN SISTEM WPA RADIUS

Surahmat[1], Yesi Novaria Kunang[2], Deny Erlansyah[3]

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Bina Darma

Jl. Ahmad Yani no.12 Plaju Palembang

Telp. (0711) 515679 ext.177, Faks. (0711) 515679 ext 124

Email: surahmat.ubd@gmail.com

Abstract **:** Security on computer networks is importance because of the growing computer network technology either through a LAN (Local Area Network) and WLAN (Wireless Local Area Network) . One method commonly used in network security is a RADIUS (Remote Authentication Dial -in User Service) but after meticulous system turns on the RADIUS authentication based on usernames and passwords only so this system can be penetrated by using packet sniffing , session hijacking , and several other techniques . To overcome this security system is used the WAP RADIUS authentication system using the username and password in addition it also use a certificate that is installed on a radius server . So the WPA RADIUS system has a better level of security against attacks such as packet sniffing , session hijacking , SQL injection attacks , and several others , the methods used in this research is Action Research is composed of stages Diagnosing , Action Planning , Action Taking , Evaluating , and Specifying Learning . This method will be generated solution and prevention of security holes found in WPA RADIUS . Because of the importance of an analysis of the security system then prompted the authors to conduct Analysis System Security as proof for WPA RADIUS.

Keywords : RADIUS , RADIUS WPA , Security Analysis

Abstrak **:** Keamanan pada jaringan komputer merupakan hal yang sangat penting dikarenakan semakin berkembangnya jaringan komputer baik itu melalui LAN (Local Area Network) maupun WLAN (Wireless Local Area Network).Salah satu metode keamanan jaringan yang biasa digunakan ialah RADIUS (*Remote Authentication Dial-in User Service*) tetapi setelah di teliti ternyata sistem autentikasi pada RADIUS hanya berdasarkan *username* dan *password*s sehingga sistem ini masih bisa ditembus dengan *menggunakan Sniffing paket, session Hijacking* dan beberapa teknik yang lain. Untuk mengatasi hal tersebut digunakanlah sistem keamanan WAP RADIUS dimana sistem autentikasi selain menggunakan *username* dan *password* juga menggunakan sertifikat yang diinstall pada server radius. Sehingga sistem WPA RADIUS memiliki tingkat keamanan yang lebih baik terhadap serangan seperti *Sniffing paket, session Hijacking, SQL Injection* dan beberapa serangan yang lain, metode yang digunakan dalam penelitin ini ialah *Action Research* yang terdiri dari tahapan *Diagnosing,Action Planning, Action Taking, Evaluating, dan Specifying Learning.* Dengan penggunaan metode ini nantinya akan dihasilkan solusi maupun pencegahan dari lubang-lubang keamanan yang terdapat pada WPA RADIUS. Karena pentingnya sebuah penganalisaan dari sistem keamanan maka mendorong penulis untuk melakukan Analisis Keamanan Sistem WPA RADIUS sebagai pembuktian kehandalah WPA RADIUS.

Kata Kunci : RADIUS, WPA RADIUS, Analisis Keamanan

1. PENDAHULUAN

Keamanan pada jaringan komputer merupakan hal yang sangat penting dikarenakan semakin berkembangya jaringan komputer baik itu melalui LAN (*Local Area Network*) maupun WLAN (*Wireless Local Area Network*). Keamanan komputer betujuan untuk menjaga sistem komputer dari orang yang tidak berhak.

Sistem keamanan komputer semakin dibutuhkan seiring dengan meningkatnya pengguna komputer saat ini (Andi, 1998). Selain itu makin meningkatnya para pengguna yang menghubungkan jaringannya ke *internet*, namun tidak diimbangi dengan adanya SDM atau *administrator* jaringan yang handal sehingga dapat menjaga keamanan data serta infomasi yang ada didalam sistem. Sehingga keamanan data menjadi terancam untuk diakses orang-orang yang tidak berhak. Keamanan komputer menjadi penting karena ini berkaitan dengan *Privacy, Integrity, Autentication, Confidentiality* dan *Availability.* Beberapa ancaman keamanan komputer adalah *virus, worm, trojan, spam* serta tangan-tangan jahil para *Cracker*. Masing-masingnya memiliki cara untuk mencuri data bahkan merusak sistem komputer.

Ancaman bagi keamanan sistem komputer ini tidak bisa dihilangkan begitu saja, namun dapat kita kurangi, hal ini adalah dengan menggunakan software keamanan sistem antara lain *antivirus, antispam* dan sebagainya. Selain itu dalam penggunanya sistem keaman pada jaringan khusunya *wireless* menggunakan beberapa sistem keamanan diataranya adalah WEP. WPA, WPA2, dan RADIUS. Masing-masing sistem keamanan ini memiliki keunggulan dan kelemahan nya sendiri.

Pada sistem keamanan RADIUS yang hanya mengandalkan proses autentikasi *username* dan *password* terdapat beberapa masalah antara lain dapat ditembus melalui penetrasi *DoS (Denial of Service)* ke AP, *Sniffingpaket*, *session hijacking* dan*penetrasi user autentikasi*. Disinilah sangat dibutuhkan pengujian sebuah sistem dan jaringan agar hasil dari test penetrasi bisa digunakan untuk perbaikan sistem kedepannya.

2. METODOLOGI PENELITIAN

Adapun tahapan penelitian yang merupakan bagian dari *action research ini*, yaitu.

1. *Diagnosing*, yaitu melakukan diagnosa terhadap sistem keamanan padajaringan *wireless* berbasis WPA RADIUS.
2. *Action Planning*, yaitu melakukan rencana tindakan yang akan dilakukan pada jaringan *wireless* WPA RADIUS dengan membuat perancangan sistem pengujian.
3. *Action Taking*, yaitu mengimpelementasikan rancangan tindakan yang telah dibuat dengan menjalankan tahapan-tahapan mengikuti fase *penetrasi testing* terhadap jaringan *wireless* WPA RADIUS untuk mencari kelemahan sistem jaringan *wireless*.
4. *Evaluating*, yaitu melaksanakan evaluasi hasil dari hasil penetrasi tadi yang menemukan celah keamanan sistem autentikasi *wireless* berbasis WPA RADIUS, dalam tahap ini yang dilihat adalah apakah sistem keamanan jaringan

wireless WPA RADIUS berjalan dengan baik.

5. *Specifying Learning*, yaitu review tahapan-tahapan yang telah berakhir dan mempelajari kriteria celah keamanan dan cara menutup celah keamanan tersebut sehingga penelitian ini memiliki kesimpulan yang diharapkan.

2.1. Keamanan Sistem

(Sarno dan Iffano, 2003) keamanan adalah suatu upaya untuk mengamankan aset atau informasi terhadap ancaman yang mungkin timbul, sedangkan menurut kamus besar bahasa Indonesia keamanan ialah keadaan aman, nyaman sesuai dengan yang diharapkan.

Sistem menurut (Bertalanffy, 2010) adalah sekumpulan komponen yang saling berinteraksi dan bekerja sama untuk mencapai tujuan yang sama. Sedangkan menurut (R. Soemita Adikusumah, 1998) sistem ialah Suatu jaringan atau sejumlah prosedure yang saling berhubungan yang dikembangkan sesuai dengan suatu pola atau rencana untuk melakukan aktivitas utama.

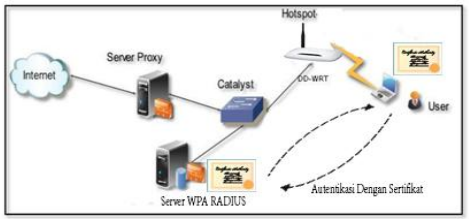
Jadi kemanan sistem dalam penelitian ini ialah upaya yang dilakukan untuk menjaga sesuai kondisi yang diharapkan dengan menggunakan komponen yang salaing berkerja sama dan behubungan untuk mencapai tujuan yang diaharapkan.

2.2.WPA RADIUS (*Wireless protectin Autentication Remote Authentication Dial-In User Service*)

WPA RADIUS merupakan sistem keamanan pada jaringan wireless yang cukup terkenal dan banyak di pakai pada jaringan-jaringan internet untuk menghubungkan client pada jaringan . Pengamanan WPA RADIUS memerlukan minimal 3 (tiga) point yang harus dipenuhi oleh administrator (Arif Dkk, 2007) yaitu .

1. *Server* : Komputer server yang dituju oleh akses point yang akan memberi otontikasi kepada client. Aplikasi yang biasa digunakan antara lain freeRADIUS, openRADIUS.
2. *Port* : Nomor port yang digunakan adalah 1812.
3. *SharedSecret* : Shared Secret adalah kunci yang akan dibagikan ke komputer dan juga kepada client secara transparant.
4. Sertifikat Autentikasi : ialah sertifikan yang dimiliki oleh *client* dan *server* sebagai authentikasi dalam jaringan.

Setelah *server* diinstall aplikasi seperti freeRADIUS, maka adminstrator juga harus membuat serifikat yang kemudian akan dibagikan kepada *client* dan *Server*, agar dapat menangani sistem otentikasi



Gambar 2.1. Jaringan WPA Radius

2.3. Teknologi Pengamanan *Wireless*

2.3.1. WEP (*Wired Wquivalent Privacy*)

Sistem pengamanan pada WEP menggunakan satu kunci enkripsi yang digunakan secara bersama oleh client dalam suatu jaringan hal mengakibatkan sistem keamanan yang kurang begitu baik apabila digunakan pada jaringan hotspot pada tempat-tempat umum. Menurut Agung (2005) Sistem pengamanan WEP memiliki begitu banyak lubang-lubang keamanan sehingga sangat mudah untuk dibobol oleh orang yang tidak berhak sehingga penggunaan WEP sangat tidak disarankan untuk digunakan.

(Jasakom, 2006) menjelaskan Untuk sistem keamanannya WEP menggunakan 2 jenis autentikasi yaitu

1. *Open System Autentication*. Saat level keamanan WEP diaktipkan maka data-data yang dikirimkan akan dienkripsi dengan WEP *key*. Sehingga apabila data client berbeda dengan data yang telah disetting pada WEP maka data tersebut tidak akan dikenali.
2. *Shared Key Autentication*. Berfungsi untuk memaksa client untuk mengetahui terlebih dahulu kode *passphare* sebelum diberikan hak akses terhadap AP.

2.3.2. WPA (*Wi-Fi Protected Access*)

WPA adalah sistem keamanan yang diciptakan untuk menutupi kelemahan dari sistem WEP sehingga memiliki sistem keamanan yang lebih baik dari WEP. Pada sistem WPA user harus terlebih dahulu terhubung ke *wireless* LAN atau internet, untuk sistem autentikasinya bisa menggunakan *username* dan *password* (Kunang, 2009).

Impementasi sistem WPA menggunakan 802.1x dan EAP *(Extensible Autenticatin Protokol*) sistem inilah yang membuat keamanan WPA lebih baik dari WEP. Teknik pengamanan yang menggunakan standar 802.1x dan EAP pada WPA mengharuskan client untuk melakukan proses otentikasi terlebih dahulu sebelum terhubung kedalam jaringan. Sebenarnya sistem autentikasi memiliki banyak cara tetapi pada WPA menggunakan sistem autentikasi pertukaran *key* secara dinamik, sistem pertukaran secara dinamik ini dibuat menggunakan *Extensible Autentication Protokol* (EAP).

3. HASIL

3.1. *Action Taking*

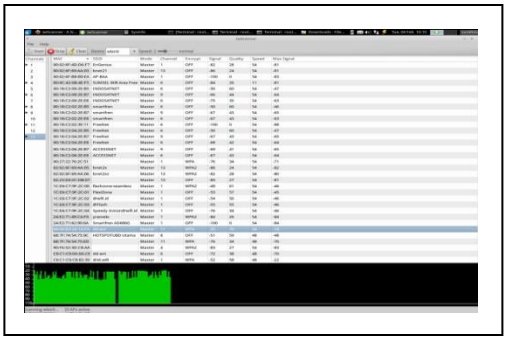
hasil pengujian dari sistem WPA RADIUS dimana pengujian menggunakan metode White box testing dengan berpedoman pada *United States National Institute of Standards and Technology* (UNNIST) yaitu terdiri dari beberapa tahap.

1. *Planning*
2. *Discovery*
3. *Attack*
4. *Reporting* (Pembahasan)

3.1.1. *Discovery*

Didapatkan data yang tersembunyi yang didapatakan melalui hasil *scaning* pada *Server*, *Client*, dan *Access Point*.

1. Hasil *Scaning* WiFi di Sekitar Acess Point WPA Radius.



Gambar3.1 . Wifi Di sekitar *Acess Point* WPA-RADIUS

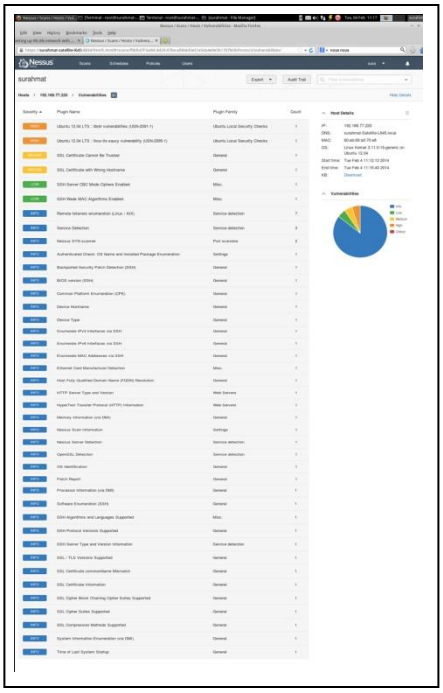
2. Hasil Scaning Nmap

Nmap ialah tool yang digunak untuk mengecek atau melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan *features scanning* lainnya yang berguna untuk proses audit dalam jaringan. Nmap memiliki tampilan GUI yang bernama Zenmap cara penggunanya sama dengan Nmap. Pada penelitian ini penulis melakukan *scaning* standar yaitu dengan perintah :

nmap –T4 –A –v [IP Target]

3. Hasil *Scaning* Nessus

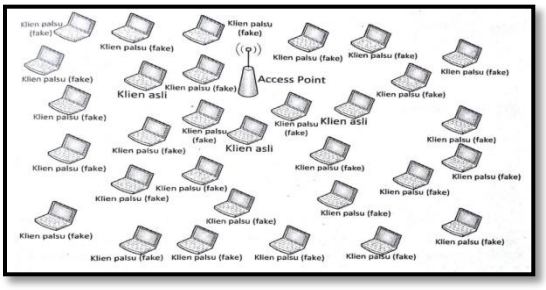
Cara menggunakan nessus relatif mudah hanya dengan memasukkan alamat Host/IP dari target yang dituju dengan terlebih dahulu melakukan seting *policy* pada nessus. *Vulnerability* yang ditampilkan pada nessus akan di kelompokan menjadi High, Medium, Low, dan Info. Sehingga memudahkan hal apa yang harus dilakukan perbaikan nantinya berdasarkan standar prioritas. Hasil dari scaning nessus yang peneliti lakukan dapat dilihat yaitu.



Gambar 3.2. Hasil Scaning Nessus Pada Server

3.1.2. *Attack*

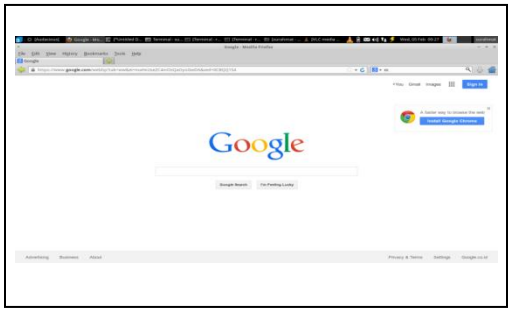
1. DoS (*Denial of Service*) ke *Acces Point*



Gambar 3.3. Simulasi Serangan DoS

Seperti yang terlihat pada gambar bahwa, seolah-olah ada banyak client yang ingin melakukan authentikasi pada access point hingga menimbulkan *overload* sehingga *access point* tidak mampu bekerja lagi. Sehingg jaringan *wireless* menjadi tidak dapat digunakan lagi. Dikarenakan banyak klien yang mengirim paket secara bersamaan.

Untuk melihat perbedanya penulis melakukan serangan DoS terhadap *Access Point* dengan menggunakan *tools* mdk3 pada ssid 64:66:B3:2A:1A:FA di *channel* 11 yaitu dd-wrt dengan sistem keamanan WPA RADIUS.



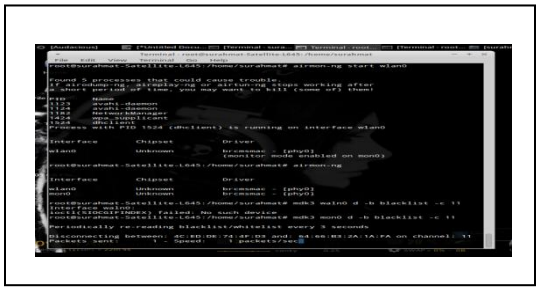
Gambar 3.4. *C*lient sebelum dilakukan serangan Dos

Serangan DoS dilakukan dengan menggunakan perintah.

#airmon-ng start Wlan0

#mdk3 mon0 d –b blacklist –c Target_Channel

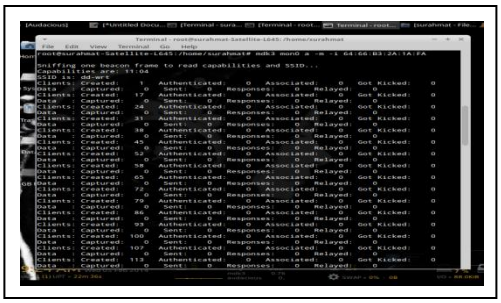
#mdk3 mon0 a –m –I Target_Address



Gambar 3.5. Menjalankan Serangan Dos

Lalu pada perintah terakhir membuat sebuah pengelompokan *blacklist* taget yang akan

di serang sehingga client yang tidak akan bisa melakukan koneksi ke acces point.



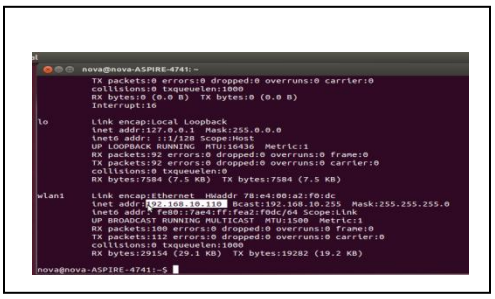
Gambar 3.6. Serangan DoS Pada *Acces Point*

Saat dilakukan serangn DoS pada access point web browser yang digunakan client serta sinyal autentikasi terhadap acces point menjadi terputus seperti terlihat pada gambar 4.6.

Gambar 3.7. Serangan DoS Berhasil

2. TuxCut ke *Client* WPA Radius

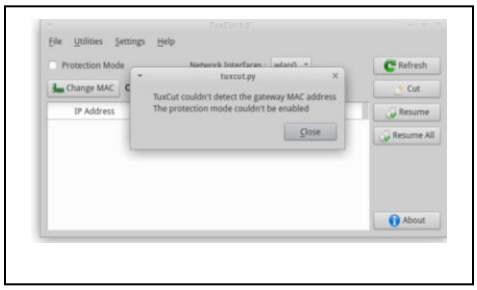
Peneliti melakukan pemutusan jaringan dari client ke internet. Untuk melakukan pemutusan jaringan ini peneliti menggunakan *Aplikasi* TuxCut. Cara kerja TuxCut dalam teknik ini ialah dengan menjadikan laptop atau komputernya yang peneliti gunakan sebagai gateway. Sehingga memungkinkan mengatur siapa yang dapat terkoneksi pada jaringan, dan siapa yang diputuskan koneksinya terhadap jaringan. Untuk melakukan teknik ini seorang penyerang membutuhkan koneksi terlebih dahulu ke *access point* dan mendapatkan IP dari dari *acess point.* Untuk mengetahui ip client yang ingin diputuskan koneksinya bisa menggunakan perintah *ifconfig* pada terminal client.



Gambar 3.8. Ip dari komputer *client*

Langkah selanjutnya penyerang akan menjalankan aplikasi TuxCut dengan cara mengetikan perintah tuxcut pada terminal dengan terlebih dulu masuk sebagai *root* sehingga memiliki *access* penuh terhadap penggunaan *resources* yang ada pada komputer atau labtop *attacker*.

Gambar 3.9. Ip dari komputer *Attaker*



Gambar 3.10. Serangan Menggunakan TuxCut

Pada tahapan ini bisa dilihat bahwa penyerang gagal melakukan serangan ke jaringan client sistem WPA Radius dikarenakan telah ada sistem proteksi pada gate way pada sistem yaitu IP 192.169.10.1. sehingga attacker tidak dapat memutuskan jaringan client pada sistem WPA Radius.

Gambar 3.11. Koneksi *client* Tidak terganggu

3.1.3. Reporting

sistem WPA Radius hanya memiliki sedikit celah keamanan dan yang paling siknifikan ialah berupa konfigurasi dari Administrator jaringan itu sendiri. Dan sistem ini jelas lebih baik dari sistem-sistem sebelumnya seperti EAP, WPA/WPA2, dan RADIUS. Seperti tergambardalam tabel berikut:

No	Serangan	Tools	Keterangan	Hasil
1	Penetrasi Pada Acces Point	Mdk3	Pengujian Tanpa Utentikasi terlebih dahulu	Berhasil melumpuhkan Acces Point
2	Penetrasi Pada client	Nmap , Tux Cut, Etterc ap. Wires hark, fireshe ep	Pengujian dengan melakukan Authentikasi terlebih dahulu	Nmap berhasil mengetahui port, serta sistem operasi yang client gunakan TuxCut tidak berhasil memutus koneksi client . Ettercap ,wireshark, fireship tidak berhasil menangkap data clent.
3.	Penetrasi Sistem Authentikasi	SQL Injection	Serangan Tanpa Authentikasi terlebih dahulu	Tidak berhasil karena sistem authentikasi WPA Radius tidak menggunakan portal authentikasi terlebih dahulu.
4.	Penetrasi ke server WPA Radius	Nmap, DoS.	Serangan dengan melakukan authentikasi terlebih dahulu	Tergantung konfigurasi Sistem WPA Radius

Tabel 3.1. Hasil Pengujian WPA RADIUS

Seperti dilihat saat penulis melakukan pengujian menggunakan tuxcut penulis tidak dapat mendapatkan ip dari client yang berada di jaringan WPA Radius sedangkan pada pengujian menggunakan wireshark paket yangditangkap ialah paket dengan protokol LLC (*Logical Link Control*) yakni protokol yang berkerja pada OSI layer 2 yang menandakan bahwa paket yang ada di jaringan WPA Radius Terenkripsi sehingga tidak menampilkan data yang sebenarnya. Sehingga client yang terkoneksi pada jaringan WPA Radius hanya akan mendapatkan paket-

paket data yang dibutuhkannya saja sedangkan paket data yang bukan miliknya tidak akan terdeteksi pada komputer *attacker*.

Dalam penelitian berjudul "*Session Hijacking on Android Devices*" dijelaskan bahwa dengan penggunaan sertifikant authentikasi maka semua data di bawah OSI layer 3 tidak dapat diekstraksi dari jaringan ini berarti Hanya komunikasi 2 arah yang dapat saling berhubungan web server dan klien yang ter authentikasi yang mampu membaca data HTTP sedangkan *cookie* dari data tetap rahasia. (Koch:2011).

3.1.3.1. *Specifying Learning*

Pada tahapan ini penulis akan mengevalusi hasil dari penelitian yang telah dialkuakan kelemahan yang paling utama ialah terhadap serangan DoS ini bukan disebabkan sistem WPA Radius tapi kelemahan dari hardware yang digunakan seperti acces point dan server yang dipakai. Untuk mengatasi serangan DoS bisa dengan melakukan beberapa konfigurasi seperti dibawah ini .

3.1.3.2. Mengaktifkan Firewall

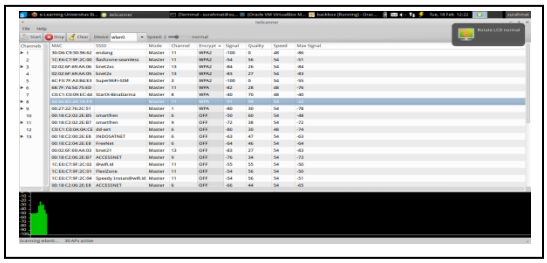
Pada accespoint yang digunakan oleh penulis firewall sudah terdapat pada accespoit tersebut dengan jenis SPI (*Stateful Packet Inspection*) yang merupakan proses inspeksi paket yang tidak hanya dilakukan dengan menggunakan struktur pakettetapi juga dengan data yang terkandung dalam paket tersebut.

Pengaturan ini dapat mencegah serangan Nmap, paket *flooding*, serta *ping of death* yang dilakukan oleh attacker.

Gambar 3.12. seting firewall enable

3.1.3.3. Menyembunyikan SSID

SSID berguna sebagai penanda atau nama acces point pada penelitin ini penulis menggunakan nama standar yaitu dd-wrt

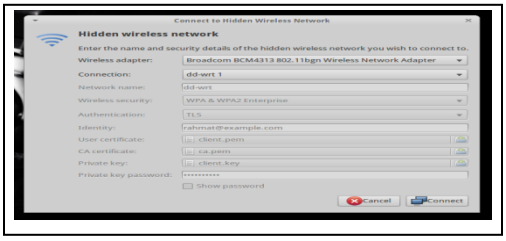


Gambar 3.13. SSID acces point terhidden

Dengan menghiden ssid mampu mencegah attacker untuk melakukan penyerangan misalnya DOS *(Denial of Service*) dan juga akan menyulitkan atau mengecoh attacker dikarenakan nama dari acces point yang penulis gunakan tidak bisa ditampilkan.

Gambar 3.14. SSID Disable

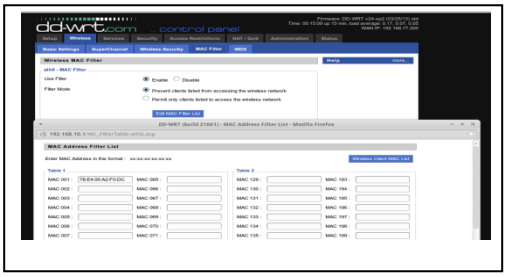
Untuk melakukan koneksi client dapat menggunakan connet to hidden wireless dengan terlebih dahulu memasukan semua konfigurasi yang di butuhkan untuk melakukan koneksi



Gambar 3.15. Konesi hidden wireless

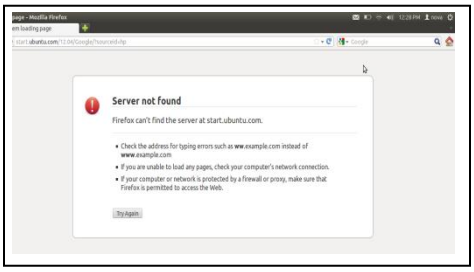
3.1.3.4. Melakukan MAC *Filtering*

Dengan menggunkan MAC *filtering* akan memberlakukan pengaturan bahwa hanya client yang sudah diketahui MAC nya saja yang bisa melakukan koneksi atau tidak bisa melakukan koneksi. Sehingga dapat meminimalisir potensi atau ancaman dari user yang tidak berhak untuk terkoneksi di jaringan WPA Radius.



Gambar 3.16. MAC *Filltering*

Pada MAC Filetring terdapat 2 tabel yang berisikan 128 field untuk memfilter user di dalam MAC filtering sehingga client bisa atau tidak terkoneksi



Gambar 3.17. Client yang telah difilter

4. SIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya, dalam penelitian yang berjudul Analisis Keamanan Sistem WPA Radius, penulis dapat menyimpulkan beberapa hal berupa.

1. Teknik pengujian dalam Sistem WPA Radius masih begitu banyak yang belum dicobakan oleh penulis sehingga memungkinkan akan ditemukan lebih

banyak kelemahan apabila dilakukan penelitian lebih lanjut.

2. Untuk mengamankan dari serangan atau menutup celah keaman yang terdapat pada sistem WPA Radius penulis menggunakan firewall, hidden SSID, MAC filtering dan IDS sehingga dapat meminimalisir celah keamanan yang penulis temukan.
3. Sistem Keamanan WPA Radius memiliki tingkat keamanan yang lebih baik dikarenakan dari beberapa percobaan yang penulis lakukan mengalami kegagalan.
4. Dengan sistem keamanan yang berlapis yang dimiliki oleh sistem WPA Radius mulai dari *username* , *password*, serta *sertifikat* WPA Radius lebih baik dari sistem EAP, WPA/WPA2, dan Radius dalam segi keamanan data.

5. SARAN

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penelitian yang penulis lakukan mengenai Analisis Sistem Keamanan WPA Radius, hal ini salah satunya disebabkan oleh terbatasnya waktu untuk pengerjaan penululisan skripsi ini. Kemudian saya sebagai penulis menyarankan agar kekurangan-kekurangan yang ada pada saat penulis melakukan penelitian ini dapat diperbaiki pada pengembangan yang lebih lanjut. Saran penulis ialah berupa.

1. Mengawasi atau memonitor jaringan sangat diperlukan agar ancaman-ancaman baik dari luar dan dalam bisa diketahui dari dini, kemudian dapat dilakukan pencegahan.
2. Karena sistem WPA Radius yang penulis gunakan masih tahap development dalam arti masaih bisa di tambah konfigurasinya agar keamanan bisa di tingkatkan. Misalnya dengan menambahkan snort, honyport, sistem proxy, serta penambahan agar dapat dilakukan manajemen waktu maupun kuota untuk *clien*.
3. Selain itu penulis juga menyarankan agar terdapat distribusi sertifikat yang benar misalnya adanya pergantian sertifikat karena pada sistem WPA Radius terdapat menagem sertifikat misalnya berapa lama sertifikat itu dapat digunakan, sehingga apabila diterapkan untuk sebuah institusi hanya orang yang memiliki hak akses dan sudah tervalidasi saja yang bisa menggunakan fasilitas internet, sedangkan untuk validasinya sendiri administrator bisa menggunakan sebuah web misalnya e-learning untuk tempat mendownload sertifikat.dengan menerapkan syarat client yang bisa mendownload sertifikat hanya client yang telah tervalidasi oleh administrator.

DAFTAR RUJUKAN

Arifin, Zaenal. (2008). Sistem Pengamanan Jaringan *Wireless* LAN Berbasis Protokol 802.1x dan Sertifikat.

Deris Setiawan, Dian Palupi Rini, " Analisis perbandingan sistem keamanan WEP/WPA/RADIUS pada jaringan public *wireless* hotspot" jurnal ilmiah seminar nasional electrical, informatics, and it's educations 2009.

Kementrian Komunikasi dan Informatika Republik Indonesia. (2012). E-Book: Panduan Keamanan Web Server.

Nasir, Moh Ph.D. (2003). Metode Penelitian. Jakarta: Ghalia Indonesia.

Penerbit ANDI. (2012). *Network Hacking* dengan *Linux BackTrack*. Semarang: Wahana Komputer.

Sugiyono. (2005). Metode Penelitian Bisnis. Bandung: ALFABETA.

Supriyanto, Aji. (2006). Jurnal: Analisis Kelemahan Keamanan pada Jaringan Wireless. Universitas Stikubank Semarang.

Suryo Guritno**,** Sudaryono**,** Untung Rahardja, 2009, *IT Research*, Penerbit Andi Offset: Yogyakarta.

Y.N. Kunang, Takrim Ibadi, Suryayusra, "Celah keamanan sistem autentikasi berbasis radius", Jurnal ilmiah Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013, 15 Juni 2013.

Zam, Efvy. (2012). Buku Sakti Hacker. Jakarta Selatan:Mediakita.