ANALISIS KEAMANAN WPA2-PSK DAN RADIUS SERVER PADA JARINGAN NIRKABEL MENGGUNAKAN METODE WIRELESS PENETRATION TESTING

WAHYUDI, ERFAN

Magister Teknik Informatika, Konsentrasi Forensika Digital
Fak. Teknologi Industri Universitas Islam Indonesia, Yogyakarta

Email : erfan.wahyudie@gmail.com

ABSTRAK

Jaringan Nirkabel merupakan salah satu teknologi yang mengalami pertumbuhan yang pesat dan hampir digunakan disetiap penjuru dunia saat ini. Banyaknya perusahaan maupun individu yang mengimplementasikan jaringan nirkabel ini tak lepas dari permasalahan yang paling sering dijumpai dalam telekmounikasi, yaitu masalah keamanan. Banyak orang yang masih ragu dengan keamanan wireless, dan banyak pula yang meyakini bahwa sistem keamanan wireless yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan wireless yang lain. Namun dari hasil studi pustaka yang dilakukan, sistem keamanan wireless yang benar-benar mampu memberikan keamanan yang lebih *secure* adalah dengan menggunakan sistem keamanan *Remote Authentication Dial In User Service* (RADIUS) *server*. Saat ini masih banyak perusahaan yang menggunakan WPA2-PSK sebagai sistem keamanan wireless mereka untuk menghindari kemungkinan penggunaan akses internet secara ilegal oleh orang yang tidak memiliki hak akses. Penelitian yang dilakukan ini bertujuan untuk menganalisa perbandingan kedua sistem keamanan jaringan wireless diatas dan menyimpulkan hasil pengujiannya untuk mengetahui sistem yang mana yang benar- benar aman untuk jaringan wireless. Pengujian dilakukan dengan menggunakan metode wireless penetration testing dengan melakukan beberapa kemungkinan serangan seperti *Brute force, MAC Address Spoofing, Sniffing to Eavesdrop, Man in the Middle Attack, Ping of Death,* dan *Deauthentication Attack.*

Kata kunci: WPA2-PSK, RADIUS, Captive Portal, Penetration Testing

ABSTARCT

The wireless network is one technology that experienced rapid growth and almost used in every corner of the world today. The number of companies and individuals who implement this wireless network cannot be separated from the problems most often encountered in telecommunications is a security problem. Many people are still unsure of wireless security, and many believe that wireless security systems using WPA2-PSK are more secure than other wireless security systems. However, from the results of literature studies conducted, the wireless security system that really can provide more secure security is to use the security system Remote Authentication Dial-In User Service (RADIUS) server. Currently, there are many companies that use WPA2-PSK as their wireless security system to avoid the possibility of unauthorized use of internet access by unauthorized people. This research aims to analyze the comparison of the two wireless network security systems above and conclude the test results to determine which system is really safe for wireless networks. Testing is done using wireless penetration testing method by performing several possible attacks such as Brute force, MAC Address Spoofing, Sniffing to Eavesdrop, Man in the Middle Attack, Ping of Death, and Deauthentication Attack.

Keywords: *WPA2-PSK, RADIUS, Captive Portal, Penetration Testing*

PENDAHULUAN

Informasi dan komunikasi pada saat ini mutlak menjadi suatu kebutuhan pokok yang harus dipenuhi. Bahkan untuk sebagian orang, mereka memerlukan informasi kapan pun dan dimana pun mereka berada. Dan teknologi yang mampu memenuhi kebutuhan tersebut adalah teknologi *wireless.*

Wireless menawarkan beragam kemudahan, kebebasan, mobilitas, dan fleksibilitas yang tinggi. Teknologi wireless memiliki cukup banyak kelebihan dibandingkan teknologi kabel yang sudah ada. Kemudahan-kemudahan yang ditawarkan wireless LAN menjadi data tarik tersendiri bagi para pengguna komputer dalam menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet.

Masalah yang akan dihadapi apabila menerapkan jaringan wireless adalah isu tentang keamanannya. Banyak pihak yang masih mempertanyakan tentang keamanan wireless, dan banyak pula pihak yang meyakini bahwa sistem keamanan wireless yang menggunakan WPA2-PSK lebih aman dibandingkan dengan sistem keamanan wireless yang lain.

Berdasarkan hasil studi pustaka yang dilakukan, sistem keamanan wireless yang benar-benar mampu memberikan keamanan yang lebih *secure* adalah dengan menggunakan sistem keamanan *Remote Authentication Dial In User Servie* (RADIUS) *server* menggunakan autentikasi Captive Portal. Namun pada saat ini, banyak pihak yang masih menggunakan WPA2-PSK sebagai sistem keamanan *wireless* mereka untuk menghindari kemungkinan penggunaan akses internet secara ilegal oleh orang yang tidak memiliki hak akses. Dari permasalahan tersebut, maka ranah penelitian ini adalah melakukan analisis perbandingan terhadap sistem keamanan jaringan nirkabel yang menggunakan sistem keamanan WPA2-PSK dengan Captive Portal atau RADIUS menggunakan metode *wireless penetration testing.*

DASAR TEORI

Penulis menemukan penelitian terdahulu dengan topik analisa keamanan jaringan wireless menggunakan *radius server*, yang selanjutnya dijadikan sebagai tinjauan pustaka. Penelitian tersebut berjudul "Analisa Keamanan Jaringan Wireless Menggunakan Radius Server Pada Mikrotik (Studi Kasus : Perpustakaan Universitas Gadjah Mada)", oleh Ahmad Arief, tahun 2015.

Penelitian tersebut memaparkan analisis keamanan RADIUS Server pada Perpustakaan Universitas Gadjah Mada untuk mengetahui cara-cara penyerang merusak fasilitas tersebut. Setelah mengetahui kelemahan pada titik tertentu, kemudian dilakukan *penetration testing* pada RADIUS Server untuk memastikan kelemahan yang ditemukan.

Sedangkan penelitian ini bertujuan menganalisa perbandingan kerentanan (*vulnerability*) keamanan pada jaringan wireless yang menggunakan WPA2-PSK dengan RADIUS Server Captive Portal di Divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri. Perbedaan penelitian ini dengan penelitian dalam tinjauan pustaka yang sudah dipaparkan di atas terletak pada objek penelitian, tujuan penelitian, *tools* yang digunakan, dan langkah-langkahnya.

Mengetahui permasalahan berupa ancaman keamanan tersebut, penulis melakukan penelitian dengan objek jaringan *wireless* Divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri. Dari penelitian ini, penulis ingin mengetahui perbandingan kelemahan pada objek dan bagaimana cara menanggulanginya, kemudian memberikan rekomendasi kepada administrator jaringan *wireless* di objek penelitian

1. Captive Portal

Captive portal merupakan suatu teknik autentikasi dan pengamanan data yang membuat user atau pengguna suatu jaringan harus melalui satu halaman web khusus, (biasanya sebagai otentikasi) sebelum dapat mengakses internet. Captive portal sebenarnya merupakan mesin router atau gateway yang memanfaatkan web browser sebagai sarana atau perangkat otentikasi yang aman dan terkendali dalam memproteksi serta mengijinkan adanya trafik hingga user melakukan registrasi.

Hal ini dilakukan untuk mencegah terjadinya pengiriman semua paket berupa data dalam bentuk apapun kepada user yang tidak memiliki izin, sampai user

membuka web browser dan mencoba untuk mengakses internet. Pada saat itulah browser akan diarahkan ke suatu halaman khusus yang telah ditentukan untuk melakukan otentikasi, atau sekedar menampilkan halaman kebijakan yang berlaku dann mengharuskan pengguna untuk menyetujuinya. Captive portal sering kali digunakan pada jaringan nirkabel (wifi, hotspot) dan dapat juga digunakan untuk jaringan kabel.

2. Cara Kerja Captive Portal

Berikut adalah cara kerja Captive Portal:

a. User dengan wireless client diizinkan untuk terhubung ke wireless untuk mendapatkan alamat IP DHCP.
b. Sebelum melakukan otentikasi, semua IP DHCP yang disebarkan oleh server sebelumnya dibelokkan menuju Captive portal (otentikasi berbasis web).
c. User yang terhubung ke dalam jaringan tersebut akan melewati Captive portal.
d. Setelah user selesai melakukan login atau registrasi, barulah user dapat menggunakan jaringan internet yang disediakan oleh server.

METODE

Untuk melakukan *penetration testing*, penulis mengacu pada *Wireless Network Penetration Testing Methodology* seperti ditulis dalam situs www.rapid7.com. Berikut ini penulis paparkan metodologi *penetration testing* yang dimaksud.

a. Intelligence Gathering
Tahap ini merupakan tahap pengumpulan informasi pada jaringan, layanan aplikasi, pencarian informasi tentang objek serangan atau footprinting pada ruang lingkup yang telah ditetapkan. Selama tahap ini, penguji mencoba mengidentifikasi mekanisme perlindungan yang ada pada sistem.
b. Vulnerability Analysis
Pada tahap ini penguji mencari dan menetapkan tingkat keamanan. Analisa terhadap kemungkinan kerentanan yang ditentukan akan memunculkan laporan teknis seperti port yang terbuka, dan lain sebagainya.
c. Threat Modelling
Berdasarkan informasi yang didapatkan dari tahap-tahap sebelumnya, pada tahap ini penguji akan menentukan metode serangan yang efektif.
d. Password Carcking
Pada tahap ini penguji akan langsung melakukan cracking password berdasarkan informasi yang sudah didapatkan dengan menggunakan metode yang ditentukan pada tahap threat modelling.
e. Reporting
Reporting merupakan hasil akhir dari pengujian sistem. Penguji menyampaikan apa saja yang telah dilakukan dan apa saja temuan selama menguji sistem. Kemudian penguji menyampaikan bagaimana pemilik sistem memperbaiki dan menutup kerentanan.

HASIL DAN PEMBAHASAN

1. Observasi Lapangan

Melalui pengamatan langsung yang telah dilakukan penulis, di PT. Yoshugi Putra Mandiri terdapat potensi kerugian akibat masalah keamanan. Jika dilakukan analisis masalah yang ada, maka dapat diketahui potensi kerugiannya seperti pada tabel berikut :

Tabel 1. Identifikasi Masalah dan Potensi Kerugian

No	Identifikasi Masalah	Potensi Kerugian
1	Letak Akses Point berada pada ruang terbuka yaitu ditempelkan di dinding tanpa kotak pengaman	Memungkinkan terjadinya kerusakan alat jaringan apabila perekat terlepas dan terjatuh
2	Sinyal *wireless* dari akses point bisa menjangkau 1 rumah makan disamping kantor, dan kombinasi *password* yang digunakan tergolong lemah	Memungkinkan orang yang iseng untuk melakukan *brute force* terhadap jaringan *wireless* untuk menggunakan akses internet secara ilegal apabila tidak menggunakan

		kombinasi *password* yang kuat
3	Akses untuk masuk ke halaman administrator pada akses point masih menggunakan *username* dan *password* standar pabrik.	Memungkinkan karyawan yang iseng mencoba masuk ke halaman administrator untuk merubah konfigurasi yang ada
4	Tidak ada kamera pengawas atau CCTV di ruangan yang terdapat alat-alat jaringan	Memungkinkan adanya kehilangan inventaris atau pencurian alat yang dilakukan oleh orang yang tidak bertanggungjawab
5	SSID, BSSID, Channel dan Mac address client dapat diketahui dengan melakukan scanning	Memungkinkan *attacker* untuk melakukan serangan *Brute Force Attack* menggunakan *Dictionary File*
6	Mac address client dapat diketahi dengan melakukan scanning	Memungkinkan *attacker* untuk melakukana serangan *Mac Address Spoofing*
7	IP dan Mac Address client dan gateway dapat diketahui	Memungkinkan *attacker* untuk melakukan serangan *Sniffing to Eavesdrop* dan *Man in the Middle Attack*
8	IP gateway dapat diketahui	Memungkinkan *attacker* melakukan serangan Ping of Death
9	Mac address client dan gateway dapat diketahui dengan melakukan scanning	Memungkinkan *attacker* untuk memutuskan koneksi antara client dengan server atau melakukan serangan *Deatuhentication Attack*

Diamati dari sisi penempatan, akses point hanya ditempelkan di dinding dengan perekat dan tidak diberikan kotak sebagai pelindung atau pengaman memungkinkan terjadinya kerusakan pada alat jaringan, misalnya seperti perekat yang sudah tidak kuat menahan beban dari akses point yang memungkinkan akses point akan rusak bila terjatuh. Lokasinya yang cukup rendah juga bisa dijangkau oleh tangan orang dewasa memungkinkan terjadinya kehilangan mengingat akses tamu yang bebas keluar masuk tidak menutup kemungkinan terjadi pencurian alat oleh orang yang tidak bertanggungjawab.

Sedangkan dari pengamatan terhadap akses ke halaman administrator melalui browser pada akses point masih menggunakan username dan password default dari pabrik untuk login ke halaman admin. Hal ini memungkinkan karyawan yang iseng untuk melakukan percobaan login ke halaman admin dan merubah konfigurasi atau pengaturan-pengaturan keamanan yang diterapkan saat ini, hal ini tentunya akan mengganggu kelancaran akses internet yang ada.

Kekuatan jangkauan sinyal wireless yang cukup kuat bisa menjangkau 1 rumah makan di samping kantor memungkinkan orang-orang yang tidak memiliki izin akses akan melakukan serangan terhadap jaringan wireless dengan metode brute force untuk mendapatkan password wifi guna mendapatkan akses internet gratis secara ilegal apabila kombinasi password yang digunakan tergolong lemah atau bukan kombinasi password yang kuat.

Adapun serangan secara logical yang meliputi kemungkinan serangan terhadap sistem seperti serangan Brute force attack, MAC address spoofing, Sniffing to Eavesdrop, Man in the Middle Attack, Ping of Death dan Deauthentication Attack akan ditindaklanjuti pada tahap berikutnya.

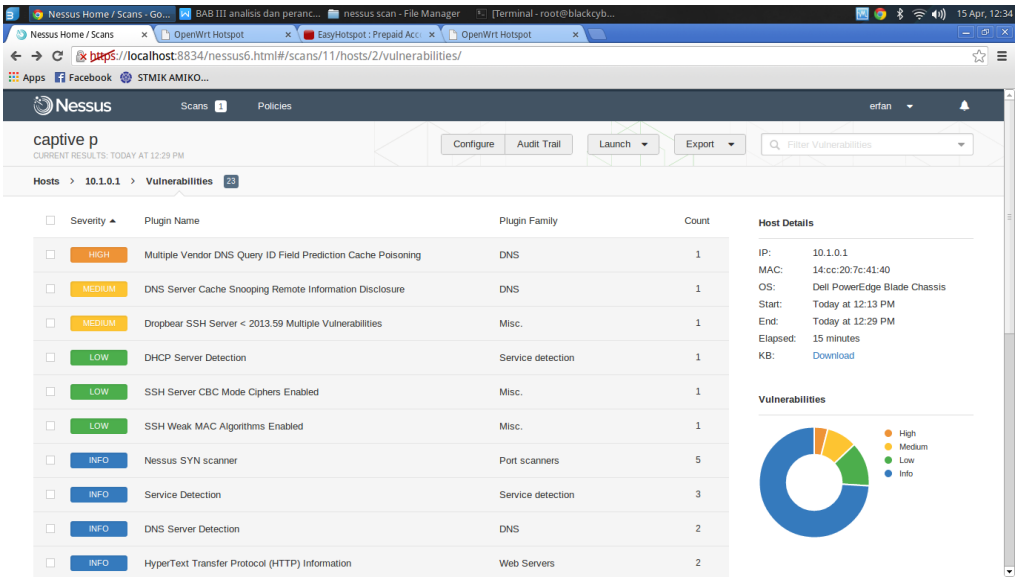
2. Vulnerability Analysis Captive Portal

Untuk menentukan titik kerentanan pada Captive Portal, penulis menggunakan bantuan tool Nessus Scanner versi 6 pada BackBox Linux. Setelah melakukan scanning, penulis menemukan beberapa vulnerability yang

terdeteksi pada server Captive Portal setelah scanning selesai dilakukan yaitu:

a. *Vulnerability* dengan resiko *high* 1 buah
b. *Vulnerability* dengan resiko *medium* 2 buah
c. *Vulnerability* dengan resiko *low* 3 buah

Dari reports dibawah yang terlihat, bisa diketahui secara detail informasi dari vulnerability tersebut, yang meliputi keterangan dan deskripsinya. Bila beruntung akan ada juga beberapa solusi yang dapat dicoba untuk menutup celah tersebut.



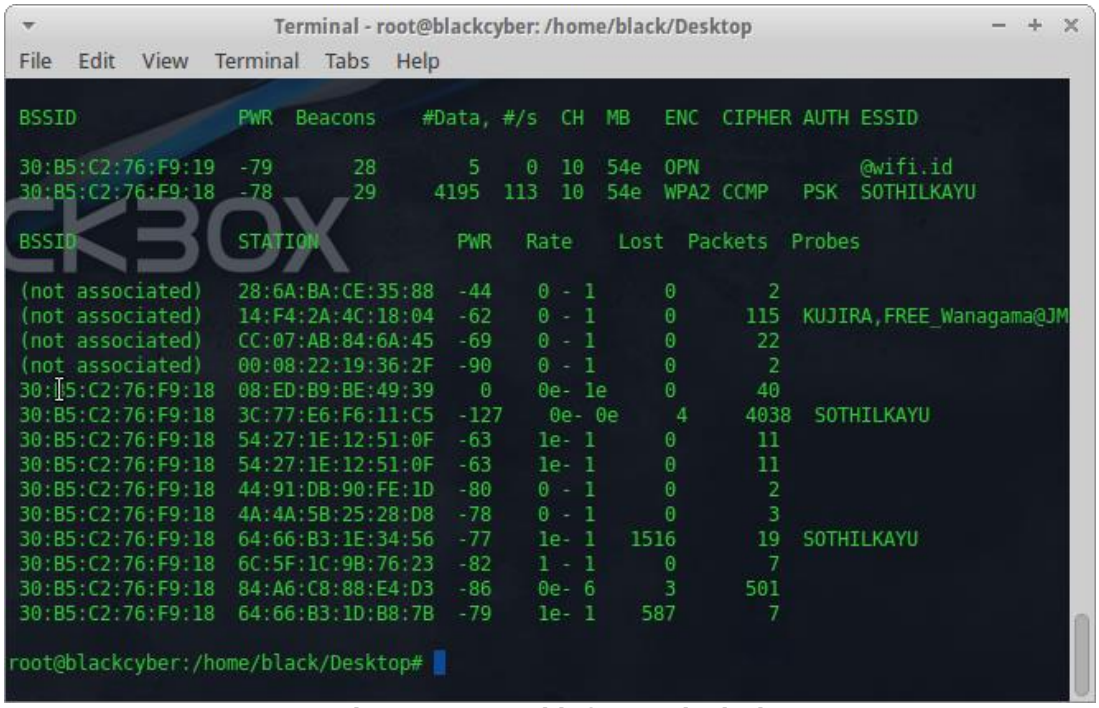
Gambar 1. List Vulnerability Captive Portal

Dari gambar diatas terlihat ada beberapa vulnerability yang ditemukan, ada yang bernilai low, medium, dan high. Vulnerability yang berwarna orange (high) ada 1 buah, warna kuning (medium) ada 2 buah, dan hijau (low) 3 buah. Untuk mengetahui detail dari vulnerability tersebut double klik pada vulnerability yang ingin dibuka, maka akan muncul tampilan yang menampilkan rekomendasi dari permasalahan yang ada.

3. Vulnerability Analysis WPA2-PSK

Untuk mencari vulnerability pada jaringan wireless yang menggunakan sistem keamanan WPA2-PSK, penulis menggunakan perangkat lunak aircrack-ng. Aircrack-ng akan digunakan untuk mencari informasi dari jaringan *wireless*, informasi yang dicari berupa jenis keamanan yang digunakan, SSID target, *MAC Address* akses point, *MAC address* host yang terkoneksi ke jaringan *wireless* target.

Untuk melakukan *scanning* terhadap jaringan *wireless* target dengan menggunakan aircrack-ng, langkah awal adalah mengubah interface wlan menjadi mode monitoring dengan perintah *airmon-ng start wlan0*, dan kemudian menjalankan pemindaian jaringan *wireless* dengan metode *passive scanning* dengan perintah *airodump-ng mon0* maka hasilnya akan terlihat seperti pada gambar dibawah.



Gambar 2. Mencari informasi wireless

Pada gambar diatas dapat kita lihat bahwa target yang akan diuji menggunakan sistem keamanan WPA2-PSK dan SSIDnya ditampilkan atau tidak di hiden, pada gambar terlihat SSID target adalah SOTHILKAYU dan terletak pada channel 10. MAC address dari akses point target adalah 30:B5:C2:76:F9:18 dan terdapat 2 host yang terkoneksi ke jaringan tersebut dengan MAC address masing-masing 3C:77:E6:F6:11:C5 dan 64:66:B3:1E:34:56.

4. Identifikasi Masalah

Dari hasil *vulnerability assasement* pada Captive Portal dengan bantuan Nessus, diketahui terdapat 23 kerentanan secara sistem di Radius server Captive portal OpenWRT namun tidak seluruhnya mempunyai faktor resiko yang berbahaya terhadap radius server.

Sedangkan dari hasil *vulnerability assasement* pada jaringan wireless di PT. Yoshugi Putra Mandiri dengan bantuan aircrack-ng, dapat diketahui bahwa SSID AP tidak disembunyikan dan dapat diketahui sistem keamanan yang digunakan adalah WPA2-PSK. Dari hasil scanning juga didapatkan MAC address AP dan client yang nantinya berguna untuk proses pengujian menggunakan teknik serangan *brute force*.

Dari semua kerentanan yang telah ditemukan, tidak semuanya akan ditindaklanjuti, namun ada beberapa yang akan ditindaklanjuti oleh penulis untuk mengetahui lebih lanjut kerentanan tersebut dan membandingkannya dengan sistem keamanan yang menggunakan Captive Portal (RADIUS) serta mendapatkan solusi untuk menutupi kerentanan yang ada.

Variabel-variabel yang ada sebagai hipotesis atau kesimpulan awal sebuah masalah. Berikut penulis simpulkan masalah yang ditemukan.

a. Masalah yang terjadi di jaringan wireless PT. Yoshugi Putra Mandiri meliputi kerentanan pada sistem.
b. Masalah secara sistem yang ada di jaringan wireless PT. Yoshugi Putra Mandiri adalah kemungkinan serangan *brute force, MAC address spoofing, Sniffing to eavesdrop, Man in the Middle Attack, Ping of Death,* dan *Deauthentication attack*.
c. Berdasarkan hasil pemindaian menggunakan *Nessus Scanner* pada jaringan wireless yang menggunakan Radius Server atau captive portal, ada beberapa kemungkinan serangan yang bisa terjadi pada jaringan tersebut, yaitu serangan *brute force, MAC*

address spoofing, Sniffing to eavesdrop, Man in the Middle Attack, Ping of Death, dan *Deauthentication attack*.

5. Hasil Pengujian WPA2 & Captive Portal

Disini penulis melakukan *Vulnerability assesment* dilakukan untuk menilai kerentanan jaringan komputer nikrabel untuk menilai dan mengukur tingkat keamanan yang digunakan pada suatu jaringan. *Test* yang dilakukan pada jaringan simulasi ini menggunakan metode *penetration testing* untuk mengetahui celah keamanan yang ada pada jaringan nikrabel.

Tabel 2. Laporan perbandingan hasil pengujian

Jenis Serangan	Informasi yang di dapatkan	Status Serangan	
		WPA2-PSK	Captive Portal
Brute Force Menggunakan Dictionary File	SSID, BSSID akses point, dan list MAC address *user* yang terkoneksi ke dalam jaringan	Sukses	Gagal
MAC Address Spoofing	List MAC address *user* yang terkoneksi kedalam jaringan	Sukses	Sukses
Sniffing to Eavesdrop	IP dan MAC address *user* serta paket data yang dikirimkan	Sukses	Gagal
Man in the Middle Attack	Port yang terbuka pada server, IP dan MAC address gateway dan *user* yang terkoneksi ke dalam jaringan	Sukses	Gagal
Ping of Death	IP gateway	Sukses	Sukses
Deauthentication Attack	SSID, BSSID akses point, dan list MAC address *user* yang terkoneksi ke dalam jaringan	Sukses	Sukses

Pada tabel diatas menunjukkan bahwa serangan brute force, sniffing to eavesdrop dan man in the middle attack gagal terjadi pada jaringan yang menggunakan RADIUS server dengan otentikasi Captive Portal. Dari serangan-serangan yang telah dilakaukan dengan metode wireless penetration testing, dapat dihasilkan suatu analisa bahwa dengan menggunakan RADIUS server dengan otentikasi Captive Portal sebagai sistem keamanan jaringan wireless dapat mencegah user yang tidak memiliki hak untuk bergabung ke dalam jaringan.

Adapun alasan mengapa serangan brute force, sniffing to eavesdrop dan man in the middle attack gagal terjadi pada jaringan yang menggunakan RADIUS server dengan otentikasi Captive Portal adalah sebagai berikut:

a. Serangan *brute force* yang dilakukan dengan *dictinoary file* gagal dilakukan pada captive portal karena paket *aircrack-ng* hanya bisa digunakan pada jaringan wireless yang menggunakan enkripsi keamanan seperti WEP, WPA, dan WPA2. Sedangkan Captive Portal tidak menggunakan salah satu dari ketiga enkripsi keamanan tersebut, tetapi bersifat *Open Network* dan menggunakan otentikasi melalui *web browser.*
b. Serangan *sniffing to eavesdrop* dan *man in the middle attack* dengan teknik

ARP spoofing gagal dilakukan pada captive portal dikarenakan cara kerjanya yang berbeda dengan WPA2-PSK, dimana captive portal menggunakan sistem remote yang harus melalui 3 metode yaitu AAA untuk bisa terhubung ke internet. Jadi sebelum *user* terhubung ke jaringan *eksternal*, *user* akan melewati autentikasi pada jaringan *internal* RADIUS terlebih dahulu.

SIMPULAN DAN SARAN

1. SIMPULAN

Dari hasil penelitian yang dilakukan pada divisi *Networking & IT Solution* PT. Yoshugi Putra Mandiri dan Captive Portal OpenWrt, dapat disimpulkan sebagai berikut:

a. Dengan adanya sistem keamanan RADIUS *server* yang menggunakan otentikasi captive portal, hanya *user* yang terdaftar saja yang bisa terkoneksi ke jaringan *wireless*.
b. Terdapat permasalahan yang berhasil ditemukan pada jaringan *wireless* seperti pencurian *password* dan *username*, akses ilegal, serta man in the middle *attack*.
c. Teknik MAC *filtering* pun bisa dikelabui dnegan mudah, karena MAC *address* dapat diubah secara *virtual* menggunakan *tool macchanger*.
d. WPA2-PSK memiliki enkripsi yang cukup kuat, namun apabila menggunakan *passphrase* yang lemah masih memungkinkan untuk dilakukan proses *cracking password* menggunakan *dictionary attack*.
e. Sistem keamanan RADIUS *server* dengan *captive portal* menggunakan OpenWRT ini menawarkan alternatif keamanan pada jaringan *wireless* LAN yang kuat, dan juga manajemen *user* yang terkontrol. Dari hasil pengujian menunjukkan bahwa sistem ini sangat sulit untuk dijebol menggunakan teknik serangan ARP *Spoofing*, *brute force* dan *sniffing to eavesdrop.*
f. Keamanan data pada WPA2-PSK masih tergolong rendah karena data sensitif seperti *username* dan *password* dapat di ketahui dengan melakukan sniffing pada jaringan. Sedangkan pada captive portal keamanan data terjamin karena berdasarkan hasil pengujian *sniffing* gagal dilakukan pada captive portal.

2. SARAN

Apabila masih menggunakan enkripsi WPA2-PSK, sebaiknya gunakan passphrase yang tidak ada di dalam dictionary file. Sebagai contoh gunakan passphrase 5t|_|d10A1 atau $3cU12eP45$w0rD. Penggunaan passphrase yang kuat merupakan jaminan keamanan untuk sebuah jaringan wireless, karena satu-satunya cara yang paling gampang yang sering digunakan oleh hacker untuk mendapatkan WPA2-PSK key adalah dengan melakukan serangan brute force menggunakan dictionary file, karena itu hindari menggunakan passphrase yang ada di dalam dictionary file bahasa manapun.

Untuk mendapatkan jaringan wireless yang lebih aman, gunakan RADIUS server dengan otentikasi Captive Portal yang bisa mengurangi resiko-resiko yang tidak diinginkan

DAFTAR PUSTAKA

Stallings, W. 2011. Network Security Essentials: Application and Standard Fourt Edition. Prentice Hall.

Hassell, Jonathan. 2002. RADIUS. O'Reilly & Associates, Inc. United States of America.

Interlink Networks. 2004. Securing Hotspots with RADIUS. Interlink networks, Inc.

Wagito. 2007. Jaringan Komputer, Teori dan Implementasi Berbasis Linux. Gava Media Yogyakarta.

Sto. 2014. Kali Linux 200% Attack. Jasakom.

Sto. 2014. Wireless Kung Fu, Networking & Hacking. Jasakom.

Abas, A.P., 2008. Menjadi Administrator Jaringan Nirkabel. Andi Yogyakarta.*)*

Quiet H. 2016. How To Secure Network With RADIUS Server. http://hackforsecurity.net/2016/05/secure-network-radius-server/ (diakses tanggal 10 Oktober 2017)