

IMPLEMENTASI *WIRELESS SECURITY* MENGGUNAKAN *RADIUS MEDIA ACCESS CONTROL AUTHENTICATION* PADA SMK NEGERI 3 BENGKALIS

Yuda Irawan¹, Yulisman², Rian Ordila³, Amri Akbar⁴

^{1,2,3}Sistem Informasi, STMIK Hang Tuah Pekanbaru

⁴Teknik Informatika, STMIK Hang Tuah Pekanbaru

Email :yudairawan89@gmail.com¹, yulismanaziera27@gmail.com², rianordila@htp.ac.id³, amriakbarti@gmail.com⁴

Abstrak: Seiring dengan Perkembangan teknologi akses internet telah mencapai tahapan yang lebih mempermudah penggunaannya dengan memanfaatkan media akses jaringan *wireless* atau disebut dengan nirkabel, jaringan komputer *wireless* merupakan teknologi yang sering digunakan diberbagai instansi, perusahaan, cafe, toko, dan lain-lain. Jaringan *wireless* tidak hanya digunakan pada instansi saja, tetapi sebagian rumah tangga juga menggunakannya. Masalah yang perlu diperhatikan pada jaringan *wireless* adalah keamanannya. Apabila keamanan jaringan nirkabel tersebut memiliki celah, maka akan mudah dimanfaatkan celah tersebut oleh orang yang tidak bertanggung jawab. Hal ini dapat merugikan bagi Instansi yang memiliki jaringan nirkabel tersebut. Salah satunya Sekolah Menengah Kejuruan (SMK) Negeri 3 Bengkalis merupakan sebuah sekolah menengah yang bertempat di Bengkalis. Pada saat ini SMK sudah menggunakan layanan jaringan *wireless*. Namun permasalahan yang terjadi di SMK saat ini adalah apabila pengguna ingin mengakses internet harus melakukan *login* terlebih dahulu dan masih bisa membuka situs yang tidak dibenarkan. Hal ini terjadi karena jaringan *wireless* berada di SMK menggunakan keamanan *proxy*. Di karenakan itu perlu menerapkan sistem keamanan *wireless* dengan *Radius MAC Authentication* sehingga pengguna tidak perlu *login* ulang saat berpindah tempat dalam satu area. Dengan adanya keamanan jaringan ini diharapkan dapat mempermudah pengguna jaringan *wireless*. Penelitian ini menghasilkan suatu sistem keamanan jaringan yang telah di konfigurasi dengan mikrotik, Dari beberapa pengujian keamanan *wireless* yang dilakukan jaringan *wireless* hanya bisa digunakan oleh pengguna yang terdaftar dan apabila pengguna berpindah tempat, pengguna tidak perlu *login* ulang.

Kata Kunci: Jaringan, Security, Wireless, Radius MAC Authentication.

Abstract: Along with the development of internet access technology has reached a stage that makes it easier to use by utilizing wireless network access media or called wireless, wireless computer networks are technologies that are often used in various agencies, companies, cafes, shops, and others. Wireless networks are not only used on an instance, but some households also use them. The problem that needs to be considered on a wireless network is security. If the security of a wireless network has a vulnerability, it will be easy to exploit that vulnerability by irresponsible people. This can be detrimental to agencies that have wireless networks. One of them is Bengkalis Vocational High School (SMK) 3 is a secondary school located in Bengkalis. At this time the Vocational School already uses wireless network services. But the problem that occurs at SMK now is if the user wants to access the internet must log in first and still be able to open a site that is not justified. This happens because the wireless network resides in the Vocational School using proxy security. Because it is necessary to implement a wireless security system with Radius MAC Authentication so that users do not need to re-login when moving in one area. With this network security is expected to facilitate wireless network users. This research resulted in a network security system that has been configured with a proxy. From a number of wireless security tests conducted by a wireless network can only be used by registered users and if the user moves places, the user does not need to re-login.

Keywords: Network, Security, Wireless, Radius MAC Authentication.

1. PENDAHULUAN

Perkembangan teknologi akses internet telah mencapai tahapan yang lebih mudah penggunaannya dengan memanfaatkan media akses jaringan *wireless* atau disebut dengan nirkabel. Menurut Setiawan (2013), jaringan komputer *wireless* merupakan teknologi yang sering digunakan diberbagai instansi, perusahaan, cafe, toko, dan lain-lain. Jaringan *wireless* tidak hanya digunakan pada instansi saja, tetapi sebagian rumah tangga juga menggunakannya.

Masalah yang perlu diperhatikan pada jaringan *wireless* adalah keamanannya. Riyasa dkk (2013), Apabila keamanan jaringan nirkabel tersebut memiliki celah, maka akan mudah dimanfaatkan celah tersebut oleh orang yang tidak bertanggung jawab. Hal ini dapat merugikan bagi Instansi yang memiliki jaringan nirkabel tersebut.

Sekolah Menengah Kejuruan (SMK) Negeri 3 Bengkalis merupakan sebuah sekolah menengah yang bertempat di Bengkalis. Pada saat ini SMK sudah menggunakan layanan jaringan *wireless*. Namun permasalahan yang terjadi di SMK saat ini adalah apabila pengguna ingin mengakses internet harus melakukan *login* terlebih dahulu dan masih bisa membuka situs yang tidak dibenarkan. Hal ini terjadi karena jaringan *wireless* berada di SMK menggunakan keamanan *proxy*. Dari masalah tersebut dibutuhkan juga keamanan jaringan dengan menggunakan *radius mac authentication* agar pengguna jaringan *wireless* tidak perlu melakukan *login* dan apabila membuka situs yang tidak dibenarkan maka akan diblokir.

Setiawan (2013), *Radius mac* merupakan keamanan jaringan yang bekerja dengan memberikan autentikasi dengan *MAC address*. Berdasarkan uraian diatas maka diperlukan perancangan *wireless security* menggunakan *radius mac autentikasi* di SMK. Jaringan *wireless* yang dibangun dapat digunakan untuk pengguna yang sudah mendaftar kepada *administrator*

Dengan menggunakan *wireless security* pengguna jaringan di SMK Negeri 3 Bengkalis dapat langsung terhubung tanpa harus memasukan *login* dan *password* apabila berpindah tempat di area SMK Negeri 3 Bengkalis. Apabila pengguna yang terdaftar membuka situs yang tidak dibenarkan akan terblokir secara otomatis dan pengguna yang ingin menggunakannya kembali harus mendaftarkan *MAC addressnya* kembali dengan *administrator*.

Media Access Control adalah sebuah metode untuk mentransmisikan sinyal yang dimiliki oleh node-node atau disebut satu titik sambungan yang terhubung ke jaringan tanpa terjadi konflik.

Berdasarkan masalah-masalah yang dipaparkan, penulis akan merancang sebuah “Implementasi *Wireless Security* Menggunakan *Radius Media Access Control Authentication* Pada SMK Negeri 3 Bengkalis” yang dapat mengatasi masalah-masalah tersebut. Keamanan jaringan ini adalah sebuah keamanan yang akan menangani masalah *login* kepada pengguna agar tidak berulang ulang kali *login* dan situs yang tidak dibenarkan terbuka.

2. METODE PENELITIAN

Pada penelitian ini digunakan metode penyelesaian masalah sebagai pengembangan perangkat, adapapun metode dapat dilihat pada gambar 3.1 di bawah ini



Gambar 2.1 Alur Perancangan *Wireless Security*

1. Identifikasi Masalah
Pada tahap ini yaitu menentukan permasalahan yang ingin diangkat untuk dilakukan penelitian. Masalah saat ini adalah keamanan jaringan wireless, untuk menggunakan jaringan di SMK Negeri 3 Bengkulu pengguna harus login terus menerus untuk mengakses jaringan internet.
2. Studi Literatur
Penelitian yang dilakukan untuk mendapatkan bahan rujukan berupa referensi yang bersifat teoritis dari buku-buku, jurnal, dan sumber bacaan lain yang mendukung topik.
3. Observasi
Observasi dilakukan untuk mengetahui secara langsung masalah di lapangan. Observasi merupakan suatu teknik pengumpulan data yang mempelajari sistem, dengan cara mengamati langsung objek penelitian SMK Negeri 3 Bengkulu termasuk tempat dan jumlah siswa.
4. Analisa Sistem
Tahapan Analisa sistem ini meliputi analisa dari sistem yang ada dan analisa sistem yang diusulkan.
5. Perancangan Jaringan
Pada tahapan ini dilakukan untuk membuat struktur jaringan yang digunakan untuk merancang *security wireless* menggunakan *radius mac authentication*
6. Implementasi Sistem
Pada tahap ini, sistem pertama kali dikembangkan di program kecil yang disebut *unit*, yang terintegrasi dalam tahap selanjutnya. Setiap unit dikembangkan dan diuji untuk fungsionalitas yang disebut sebagai *unit testing*.
7. Pengujian Sistem
Tahapan ini merupakan mengujian serta melakukan perbaikan terhadap rancangan apabila ditemukan kekurangan atau kesalahan.

Pengumpulan data dalam penelitian ini akan menggunakan teknik observasi, wawancara, dan studi Literatur. Metode ini bertujuan untuk memperoleh data-data yang berhubungan dengan penelitian mengenai Perancangan *Wireless Security* Menggunakan *Radius Media Access Control Authentication* di SMK Negeri 3 Bengkulu.

1. Observasi

Observasi merupakan suatu teknik pengumpulan data yang mempelajari sistem, dengan cara mengamati langsung objek penelitian SMK Negeri 3 Bengkulu termasuk tempat dan jumlah siswa.

2. Wawancara

Wawancara merupakan pertanyaan langsung yang di tanyakan oleh pihak terkait khususnya Tim jaringan / guru jaringan, yang di lakukan adalah dengan Tim jaringan / guru jaringan tersebut menanyakan jaringan yang sedang berjalan untuk menunjang penelitian yang di buat.

4. Studi Literatur

Studi Literatur yaitu pengumpulan data dengan membaca, mempelajari dan menganalisa beberapa buku, jurnal, dan website yang berkaitan dengan masalah penelitian ini.

Landasan teori merupakan penjabaran dari teori - teori pendukung, karena dalam Implementasi *Wireless Security Menggunakan Radius Media Access Control Authentication* Pada Smk Negeri 3 Bengkulu diperlukan teori - teori pendukung untuk menjabarkan bagaimana suatu jaringan dibuat. Teori - teori yang mendukung pembangunan jaringan ini adalah sebagai berikut:

1. Jaringan

Jaringan komputer adalah sebuah kumpulan komputer, printer dan peralatan lain yang terhubung. Informasi dan data bergerak melalui kabel-kabel sehingga memungkinkan pengguna jaringan komputer dapat saling bertukar dokumen dan data. Mencetak pada printer yang sama dan bersama sama menggunakan *software/hardware* yang terhubung dengan jaringan (Basten, 2019)

2. Router

Router adalah salah satu komponen pada jaringan komputer yang mampu melewatkan data melalui sebuah jaringan atau internet menuju sarannya, melalui sebuah proses yang dikenal sebagai *routing*. Proses *routing* dapat dilakukan dengan memasukkan informasi suatu alamat jaringan secara manual kedalam tabel *routing* ataupun dengan bantuan protokol *routing* (Sumarianta, 2011).

3. Radius Server

Radius server merupakan suatu mekanisme kontrol yang mengecek dan mengautentifikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme *autentifikasi* dengan menggunakan metode *challenge/response remote acces dial in user service (radius)* merupakan *protokol connectionless* berbasis UDP yang tidak menggunakan koneksi langsung (Jonatan, 2012).

4. Wireless LAN

Jaringan *wireless* LAN merupakan suatu sistem komunikasi data tanpa kabel yang merupakan solusi alternatif dari jaringan komputer yang menggunakan kabel (*Wireless* LAN). merupakan salah satu pengembangan media transmisi dari teknologi jaringan komputer dengan menggunakan perangkat radio komunikasi data yang dapat menghubungkan sebuah komputer ke jaringan *local Area Network* (LAN). Jaringan *Wireless* LAN dapat dipasang didalam sebuah gedung, maupu diluar gedung (Najoan,2019).

5. Keamanan Wireless

Kelemahan *wireless* dapat dibagi menjadi 2 jenis, yaitu kelemahan pada konfigurasi dan pada jenis enkripsi yang digunakan. Secara umum, celah pada jaringan wireless terbentang diatas empat layer dimana keempat lapis (layer) sebenarnya merupakan proses terjadinya komunikasi data pada media wireless. Keempat lapis tersebut yaitu lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi. Model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi wireless tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2- PSK, implementasi fasilitas MAC filtering, pemasangan infrastruktur captive portal dan lain sebagainya (Supriyono dan Riadi, 2013).

6. Best Effort Wireless Security

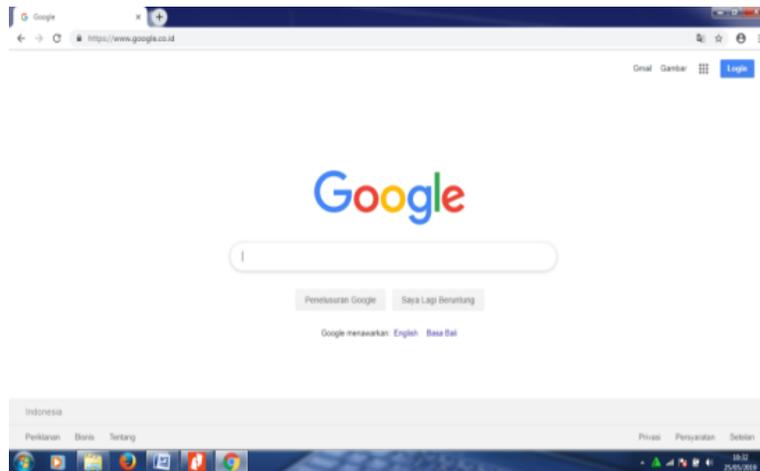
Untuk penggunaan *wireless security* saat ini yang *reliable* adalah WPA/WPA2 dimana *enkripsi* yang digunakan sudah mendukung keutuhan dan kerahasiaan data lebih tinggi. Tentu ingin menerapkan sebuah metode keamanan yang tinggi untuk menjaga jalur koneksi *wireless* agar tetap aman. Akan tetapi perlu diketahui bahwa tidak semua perangkat *wireless support* untuk penerapan metode *wireless security*. Dalam membangun jaringan *wireless*, sebagai *administrator* jaringan kita harus mengetahui detail spesifikasi perangkat *wireless* yang akan digunakan, termasuk dukungan metode *wireless security* yang bisa diterapkan. Dua buah perangkat *wireless* dengan dukungan dan penerapan metode *wireless security* yang berbeda tidak akan bisa terkoneksi (Wijaya, 2015).

3. HASIL DAN PEMBAHASAN

Pengujian adalah bagian penting dalam membangun keamanan jaringan di SMK Negeri 3 Bengkulu, pengujian dilakukan untuk menjamin kualitas dan juga mengetahui kelemahan dari perangkat keamanan jaringan, tujuan dalam memiliki kualitas yang baik sesuai dengan analisis dan perancangan sistem serta konfigurasi pada sistem yang dibangun tersebut sehingga sistem tersebut berfungsi sesuai kegunaannya.

1. Hasil Pengujian *MAC Address* Sudah Terdaftar

Hasil pengujian setelah *MAC Address* pengguna di *Server* oleh *Administrator*, maka akan langsung keluar tampilan salah satu *website* yaitu *google*, dan dimanapun pengguna berpindah tempat dalam satu area maka tidak perlu menghubungkan ke jaringan disekitarnya untuk dapat mengakses internet. Seperti pada gambar 5.24.



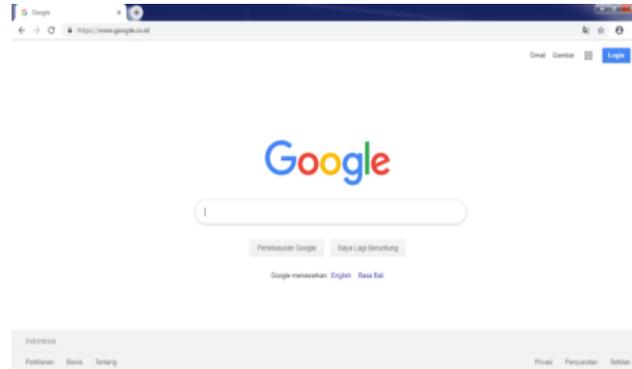
Gambar 3.1 Hasil setelah MAC Address sudah terdaftar

2. Hasil Pengujian Login Akun

Hasil pengujian setelah akun login yang sudah mendaftar pengguna di *Server* oleh *Administrator*, maka akan langsung keluar tampilan login di browser pengguna, dimanapun pengguna diminta untuk masuk username dan password.



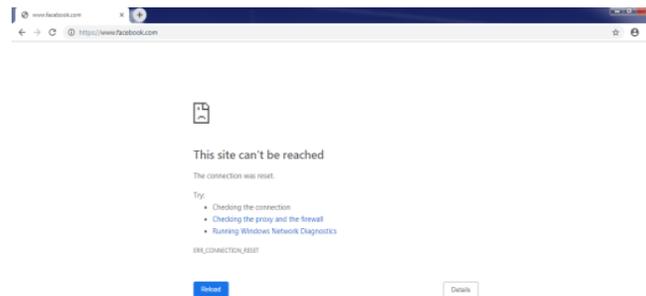
Gambar 3.2 Login Akun Pengguna



Gambar 3.3 Hasil Setelah Login

3. Hasil Pengujian Pemblokiran Situs

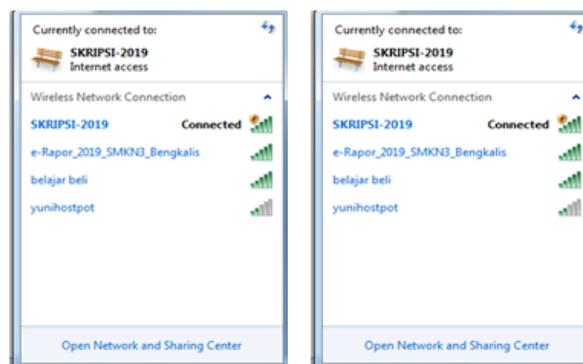
Hasil pengujian pada keamanan jaringan menggunakan *Radius MAC Authentication* didapatkan bahwa bagi pengguna yang ingin membuka situs www.facebook.com maka situs itu tidak akan terbuka Unlimited. Seperti pada gambar 5.27.



Gambar 3.4 Pengujian Sistem Mac Address

4. Pengujian Perpindahan *Hotspot*

Pada hasil pengujian menggunakan sistem Radius MAC Authentication hasil pengujian menunjukkan perpindahan dari *hotspot* yang satu ke yang satunya dapat dilihat pada gambar 5.28



Gambar 3.5 Perpindahan Hotspot

5. Pengujian

Berikut ini table yang menggambarkan metode pengujian *black-box* pada keamanan jaringan di SMK Negeri 3 Bengkulu.

Tabel 5.1 Metode Pengujian *Blackbox*

Interface	Test Case	Input	Output	Kesimpulan
Tampilan Mac Address Terdaftar	Gambar 5.24	Username : 5C:AC:4C:05:37:6F Password : 5C:AC:4C:05:37:6F	Login Menggunakan MAC Address	Valid
		Username : 1C:87:2C:81:DD:19 Password : 1C:87:2C:81:DD:19		Valid
Form Login Menggunakan Akun	Gambar 5.25	Username : amri Password : 12345	Login Menggunakan Akun	Valid
		Username : akbar Password : 12345		Valid
Tampilan Pemblokiran Situs	Gambar 5.26	Situs Yang DiBlokir	Situs Tidak Dapat Dikunjungi	Valid
Tampilan Perpindahan Hotspot	Gambar 5.27	Hotspot Yang Tersedia	Berpindah Hotspot	Valid

4. KESIMPULAN DAN SARAN

Berdasarkan pengujian yang dilakukan keamanan jaringan dengan menggunakan *Radius MAC Authentication* dapat disimpulkan sebagai berikut:

1. Apabila pengguna yang telah mendaftarkan *MAC address*nya ke *administrator* maka pengguna bisa mengakses internet yang terhubung ke *wireless* di satu area.
2. Apabila *wireless* yang satunya mati maka akan langsung terhubung ke *wireless* dua tanpa menggunakan login ulang.
3. Dengan adanya *wireless security* menggunakan *radius media access control authentication*, pengguna tidak berulang-ulang untuk login mengakses internet.
4. Dengan adanya *wireless security* menggunakan *radius media access control authentication*, dapat mengoptimalkan jaringan *wireless*.
5. Dengan adanya *wireless security* menggunakan *radius media access control authentication*, membatasi situs yang tidak diinginkan terbuka.

Dengan segala keterbatasan tentang sistem keamanan jaringan *wireless* menggunakan *Radius MAC Authentication* yang masih sangat sederhana terutama dalam performa kerja. Saran terhadap tahap pengembangan sistem keamanan jaringan ini kedepannya agar lebih baik lagi yaitu :

Untuk kedepannya diharapkan mengembangkan lagi ke tahap yang lebih sempurna dengan menggunakan *Radius MAC Authentication* yang lebih mengandalkan keamanannya sampai ke tahap apabila ada pengguna yang membuka situs atau mencoba *hacking* akan terdeteksi oleh administrator.

5. TERIMA KASIH

Penulis mengucapkan terimakasih yang sebesar-besarnya kepada semua pihak yang banyak membantu didalam proses penyelesaian skripsi ini, terutama kepada:

1. Bapak Yulisman, S.Kom, M.Kom, Selaku pembimbing utama yang telah membantu penulis untuk menyelesaikan Skripsi ini.
2. Rian Ordila, S.Kom, M.Kom, Selaku pembimbing pendamping yang telah membantu penulis untuk menyelesaikan Skripsi ini.
3. Staf dan Karyawan STMIK Hang Tuah Pekanbaru yang mendukung dalam Skripsi ini.

4. Kepala SMK Negeri 3 Bengkulu beserta Guru dan staff yang telah memberi kesempatan kepada kami untuk melaksanakan Skripsi.
5. Orang Tua dan keluarga yang selalu memberi semangat selama kuliah.

DAFTAR PUSTAKA

- [1.] Basten, 2019, Analisa Manejemen Hotspot dengan Captive Portal, *Skripsi*, Program Pasca Sarjana Universitas Negeri Semarang, Unpublished
- [2.] Najoan, 2019, Analisis Dan Implementasi Sistem Redundant hot Standby Network Security Menggunakan Metode Intrusion Preventi Sistem (IPS), *Bianglala Informatika*, Vol. 2 No 2, Hal. 112-119
- [3.] Riyasa,S., Mulyadi,A., dan Purwanto,Y., 2013, Analisa Dan Implementasi Sistem Redundasi Hot Standby Network Security Menggunakan Metode Intrusion Prevention System (IPS) Dan Captive Portal Pada Jaringan Nirkabel, *Jurnal Teknik Komputer*, No. 1 Vol.10
- [4.] .
- [5.] Setiawan,H, 2013, Rancangan Bangun Captive Portal Untuk Jaringan Wireless Berbasis open Source pada CV. Gempar production Palembang, *Jurnal Teknologi Informasi*, Vol. 7 No. 1, Hal. 36-44.
- [6.] Sumarianta, 2011, Instalasi dan Konfigurasi Jaringan Komputer, Pustaka Setia, Bandung
- [7.] Suprianto,A., Riadi,I., 2013, Rancang Bangun Sistem Hotspot Menggunakan Captive Portal, *Jurnal Sarjana Teknik Informatika*, Vol. 1 Nomor 1, hal 172-180, E-ISSN: 2338-5197
- [8.] Wijaya,I.H., 2015, Analisis Dan Implementasi Proxy Server Sebagai Web Caching, Blocking Situs, Dan Monitoring Menggunakan Centos 6 Di Smkn Ganesha Tama Boyolali, *Jurnal Teknologi Informasi & Pendidikan*, Vol. 3 No 1