Jurnal Ilmiah Sistem Informasi dan Teknik Informatika (JISTI) p-**ISSN: 2620 – 5327**
Volume 6 Nomor 1, April 2023 **e-ISSN: 2715 – 5501**
DOI : 10.57093/jisti.v6i1.144

Analisis Sistem Keamanan Jaringan *Hotspot* Pada SMA Negeri 1 Bajo Kabupaten Luwu

Hasbi
Teknologi Informasi, STMIK Kreatindo Manokwari
Jl. Kali Bambu Reremi Puncak Manokwari Barat, Manokwari, Papua Barat, Indonesia
abhyalhasbi48@gmail.com*1

Abstrak

Hotspot pada SMA Negeri 1 Bajo Kabupaten Luwu dapat diakses pada dua area, seperti pada ruangan guru, dan area ruangan Laboratorium, jumlah *user* yang mengakses jaringan *wireless* di sekolah SMA Negeri 1 Bajo Kabupaten Luwu berkisar antara 1 sampai dengan 4 0 *user*, namun didalam jaringan yang tidak mempunyai server yang bertindak sebagai *authentication, authorization, and* a*ccounting* membuat administrator tidak bisa mengetahui identitas yang jelas dari *user*. Dengan sistem keamanan yang menggunakan WEP (*Wired Equivalent Privacy*) dimana WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* untuk dapat beriternet pada jaringan *wireless* di sekolah SMA Negeri 1 Bajo Kabupaten Luwu, seorang *user* juga harus meminta key kepada seorang *administrator*, dan setiap *user* yang ingin berpindah ke *hotspot* yang lain, *user* pun di minta untuk kembali memasukan key, karena setiap titik mempunyai *network* key yang berbeda, tentunya cara yang seperti ini sangat menyulitkan baik bagi *user* maupun *administrator*. Dengan diimplementasikannya sistem keamanan jaringan dapat memberikan pelayanan akses internet yang baik dan aman pada SMA Negeri 1 Bajo Kabupaten Luwu.

Kata Kunci : Jaringan *Hotspot*, Sistem Keamanan, *Wired Equivalent Privacy*.

Abstract

Hotspots at SMA Negeri 1 Bajo Luwu Regency can be accessed in two areas, such as the teacher's room and the laboratory room area, the number of users accessing the wireless network at SMA Negeri 1 Bajo Luwu Regency ranges from 1 to 40 users, but in a network that not having a server that acts as authentication, authorization, and accounting makes the administrator unable to find out the clear identity of the user. With a security system that uses WEP (Wired Equivalent Privacy) where WEP uses one encryption key that is shared by wireless users to be able to surf the internet on a wireless network at SMA Negeri 1 Bajo, Luwu Regency, a user must also ask a key from a administrator, and every user who wants to move to another hotspot, the user is also asked to re-enter the key, because each point has a different network key, of course this method is very difficult for both users and administrators. With the implementation of a network security system, it can provide good and safe internet access services at SMA Negeri 1 Bajo, Luwu Regency.

Keywords: Hotspot Network, Security System, Wired Equivalent Privacy.

PENDAHULUAN

Salah satu perubahan utama di bidang telekomunikasi adalah penggunaan teknologi jaringan *wireless*. Dimana Jaringan *wireless* atau sering disebut *hotspot* ini menjadi daya tarik tersendiri bagi para pengguna komputer yang menggunakan teknologi ini untuk mengakses suatu jaringan komputer atau internet, dikarenakan kemudahan-kemudahan yang ditawarkan oleh teknologi jaringan *wireless*. Pada beberapa tahun terakhir ini pengguna jaringan *wireless* mengalami peningkatan yang pesat. Peningkatan dari pengguna teknologi ini juga diimbangi dengan peningkatan jumlah *hotspot* di tempat-tempat umum, seperti pusat perbelanjaan, Kafe, Bandara, di perkantoran, di Kampus bahkan juga di Sekolah-sekolah. Dengan menggunakan teknologi *wireless* (*hotspot)* kita dapat menikmati akses internet dimanapun kita berada selama di area *hotspot* tanpa harus menggunakan kabel.

Di lingkungan sekolah SMA Negeri 1 Bajo Kabupaten Luwu saat ini juga sudah menyediakan layanan internet yang berbasis *wireless (hotspot)*. Layanan Telkom Speedy yang berkecepatan hingga 2 Mbps pun digunakan untuk membuat jaringan *wireless (hotspot)* di sekolah SMA Negeri 1 Bajo Kabupaten Luwu, dan terdapat dua buah *access point* TP-LINK, sehingga *hotspot* pada SMA Negeri 1 Bajo Kabupaten Luwu dapat diakses pada dua area, seperti pada ruangan guru, dan area ruangan Laboratorium, jumlah *user* yang mengakses jaringan *wireless* di sekolah SMA Negeri 1 Bajo Kabupaten Luwu berkisar antara 1 sampai dengan 40 *user*, namun didalam jaringan yang tidak mempunyai server yang bertindak sebagai *authentication*, *authorization*, *and* a*ccounting* membuat administrator tidak bisa mengetahui identitas yang jelas dari *user*.

Dengan sistem keamanan yang menggunakan WEP (*Wired Equivalent Privacy*) dimana WEP ini menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* untuk dapat beriternet pada jaringan *wireless* di sekolah SMA Negeri 1 Bajo Kabupaten Luwu, seorang *user* juga harus meminta key kepada seorang *administrator*, dan setiap *user* yang ingin berpindah ke *hotspot* yang lain, *user* pun di minta untuk kembali memasukan key, karena setiap titik mempunyai *network* key yang berbeda, tentunya cara yang seperti ini sangat menyulitkan baik bagi *user* maupun *administrator*.

Untuk dapat membuat autentikasi pengguna jaringan *wireless (hotspot)* serta meningkatkan keamanan jaringan hotspot sekolah SMA Negeri 1 Bajo Kabupaten Luwu, dan memberi kenyamanan terhadap pada pengguna jaringan *wireless*, maka dapat dilakukan penelitian tentang Analisis Sistem Keamanan Jaringan Hot-spot pada SMA Negeri 1 Bajo Kabupaten Luwu.

KAJIAN PUSTAKA

1. RADIUS Server

Remote Access Dial-in User Service (RADIUS), merupakan suatu mekanisme akses kontrol yang mengecek dan mengautentikasi (*authentication*) *user* atau pengguna berdasarkan pada mekanisme authentikasi yang sudah banyak digunakan sebelumnya, yaitu menggunakan metode *challenge / response*. *Remote Access Dial In User Service* (RADIUS) dikembangkan di pertengahan tahun 1990 oleh *Livingstone Enterprise* (sekarang *Lucent Technologies*). Yang pada awalnya perkembangan RADIUS menggunakan *port* 1645 yang namun bentrok dengan layanan *datametrics*. Dan sekarang *port* yang dipakai RADIUS adalah *port* 1812 yang format standarnya ditetapakan pada *Request for Command* (RFC) 2138. Server RADIUS menyediakan mekanisme keamanan dengan menangani autentikasi dan autorisasi koneksi yang dilakukan pengguna. Pada saat computer *client* akan menghubungkan diri dengan jaringan maka server RADIUS akan meminta identitas pengguna (*username* dan *password*) untuk

kemudian dicocokkan dengan data yang ada dalam *database server* RADIUS untuk kemudian ditentukan apakah pengguna diijinkan untuk menggunakan layanan dalam jaringan komputer. Jika proses autentikasi dan autorisasi berhasil maka proses pelaporan dilakukan, yakni dengan mencatat semua aktivitas koneksi pengguna, menghitung durasi waktu dan jumlah transfer data yang dilakukan oleh pengguna. Proses pelaporan yang dilakukan server RADIUS bisa dalam bentuk waktu (detik, menit, jam) maupun dalam bentuk besar transfer data (*Byte, KByte, Mbyte*).

2. *Chilli Spot*

ChilliSpot, merupakan *open source captive portal* atau *Wireless LAN access point controller*. Digunakan untuk mengautentikasi *user* dari sebuah jaringan *Wireless LAN*. Mensupport login berbasis web yang merupakan standar untuk public *hotspot* dewasa ini. ChilliSpot juga dapat sebagai media autentikasi, autorisasi dan *accounting* (AAA) yang merupakan framework atau arsitektur kerja dari sebuah RADIUS server.

3. Autentikasi

autentikasi adalah proses pengesahan identitas pengguna (*end user*) untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, *username, password, pin,* sidik jari oleh pengguna kepada server. Di sisi server, sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database* server. Jika hasilnya sama, maka server akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka server akan mengirimkan pesan kegagalan dan menolak hak akses pengguna. Tujuan standar 802.1x IEEE adalah untuk menghasilkan kontrol akses, autentikasi, dan manajemen kunci untuk *wireless* LANs. Standar ini berdasarkan pada *Internet Engineering Task Force* (IETF) *Extensible Authentication Protocol* (EAP), yang ditetapkan dalam RFC 2284. Standar 802.1x IEEE juga mendukung beberapa metode autentikasi, seperti *smart cards, password* yang hanya bisa digunakan oleh satu pengguna pada satu waktu, dan yang lebih baik lagi adalah *biometrics*. 802.1x terdiri dari tiga bagian, yaitu *wireless node* (*supplicant*), *access point* (autentikator), autentikasi server. Autentikasi server yang digunakan adalah *Remote Authentication Dial-In Service* (RADIUS) server dan digunakan untuk autentikasi pengguna yang akan mengakses *wireless* LAN. EAP adalah *protocol*.

4. Jaringan *Wireless*

Sinyal *Wireless* merupakan sinyal gelombang elektromagnetis yang dapat berjalan tanpa media tetapi melalui ruang hampa atau media seperti udara. Karena tidak dibutuhkan media fisik sebagai perantara, maka hal ini akan sangat menguntungkan pada saat membangun jaringan pada daerah atau area yang luas. WI-FI (*Wireless Fidelity*) atau jaringan tanpa kabel, yang sering, maka disebut degan jaringan 802.11 karena standar yang biasanya digunakan adalah IEEE 802.11. Keuntungan menggunakan jenis jaringan seperti ini adalah tanpa menggunakan medium seperti kabel,kita sudah dapat membangun atau melakukan koneksi ke jaringan. Penggunaan angka 802.11 *(standard wireless network)* dibuat oleh IEEE *(Institute of Electrical and Electronics Engineers).* Penggunaan notasi a,b,dan g, adalah menunjukan versi yang berbeda dalam standar 802.11. versi yang pertama diluncurkan adalah 802.11b beroperasi pada 2,4GHz dan kecepatan 11 Mbps. Kemudian dilanjutkan dengan versi 802.11a dengan beroperasi pada 5GHz dan kecepatan 54Mbps. Versi yang terakhir adalah 802.11g adalah campuran dari kedua versi sebelumnya, beroperasi pada 2,4 GHz dan kecepatan 54Mbps.

METODE PENELITIAN

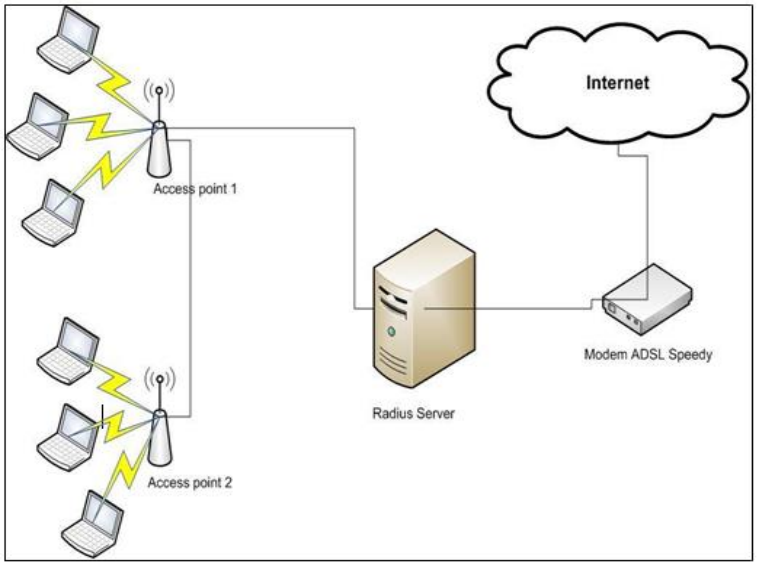
1. Teknik Pengumpulan Data

a) Studi Literatur, yaitu mengumpulkan data dari berbagai Kajian kepustakaan, yaitu pengumpulan data dengan cara membaca buku-buku studi melalui literatur yang ada hubungannya dengan penelitian yang dilakukan, selain itu mengumpulkan bahan dengan cara men*download* dari internet.

b) Wawancara (interview) yaitu mengadakan tanya jawab Wawancara adalah salah satu teknik pengumpulan data dalam penelitian dengan mengajukan pertanyaan-pertanyaan seputar keamanan jaringan. Waktu untuk melaksanakan wawancara direncanakan minggu kedua bulan Oktober tahun 2022 yang dilaksanakan di SMA Negeri 1 Bajo Kabupaten Luwu. Adapun selaku narasumber pada wawancara tersebut adalah user yang selama ini menggunakan jaringan hotspot di kampus. Wawancara ini bertujuan untuk mendapatkan data berdasarkan jawaban-jawaban atas pertanyaan yang berhubungan topik penelitian.

2. Perancangan Arsitektur Jaringan

Langkah-langkah yang dilakukan pada perancangan sistem ini adalah membuat usulan pemecahan masalah secara logikal dan usulan-usulan lainya. Berikut ini adalah perancangan arsitektur keamanan jaringan hotspot di SMA Negeri 1 Bajo Kabupaten Luwu.



Gambar 1. Rancangan Arsitektur Jaringan

HASIL PENELITIAN

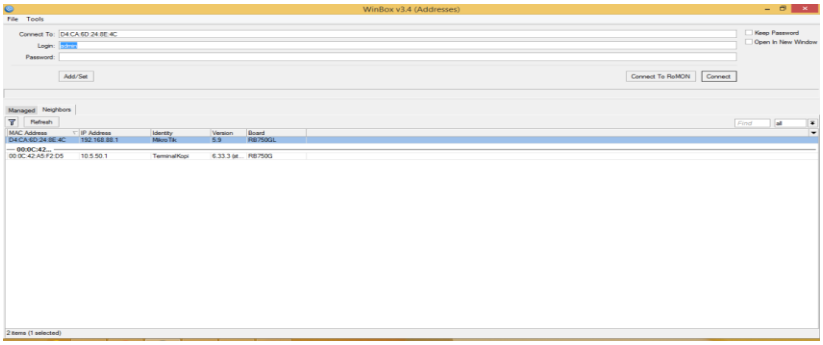
1. Implementasi Sistem

Sistem Keamanan Jaringan Hot-spot pada SMA Negeri 1 Bajo Kabupaten Luwu dibangun dengan menggunakan alat mikrotik dan access point. Berikut hasil implementasi keamanan jaringan:

a) Client Login Mikrotik

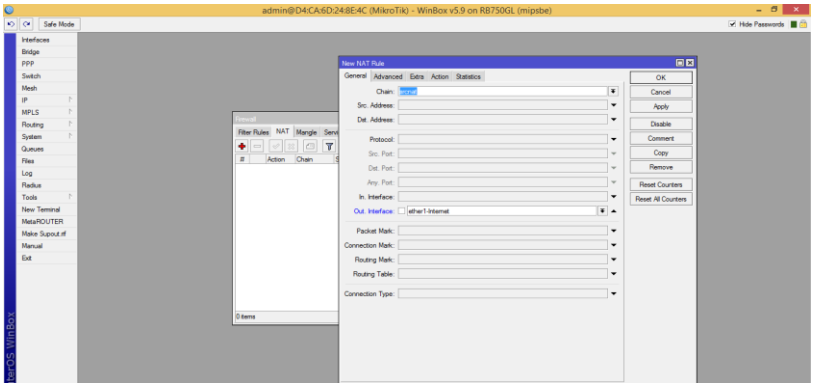
Client login dengan winbox adalah tampilan dimana user setting konfigurasi untuk memberikan alamat IP. Berikut gambar konfigurasi mikrotik Client login dengan winbox

p-**ISSN: 2620 – 5327**
e-ISSN: 2715 – 5501



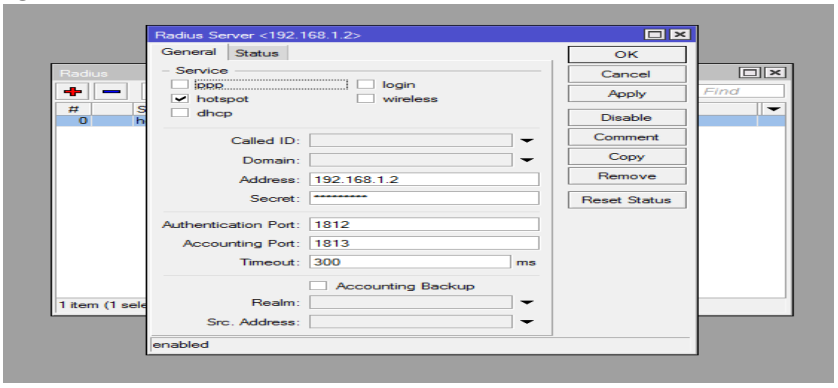
Gambar 2. Login Mikrotik Winbox

b) Setting NAT + Firewall



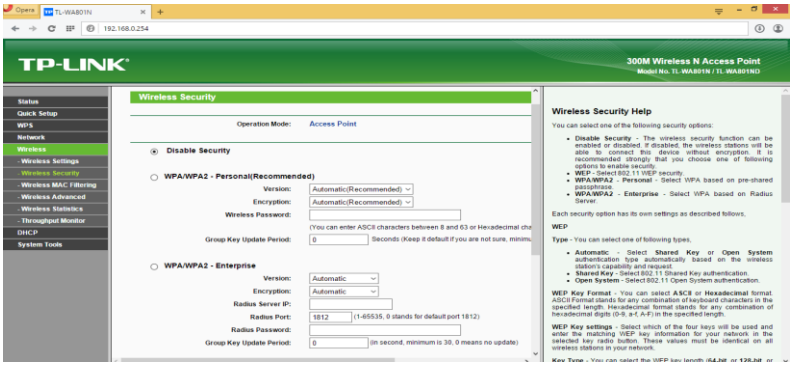
Gambar 3. Tampilan Setting NAT Firewall

c) Setting Radius Server



Gambar 4. Tampilan Setting Radius Server

d) Tampilan Setting *Hotspot Security*



Gambar 5. Tampilan Setting *Hotspot Security*

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan tentang Analisis Sistem Keamanan Jaringan Hot-spot pada SMA Negeri 1 Bajo Kabupaten Luwu, maka dapat ditarik kesimpulan Dengan diimplementasikannya sistem keamanan jaringan dapat memberikan pelayanan akses internet yang baik dan aman pada SMA Negeri 1 Bajo Kabupaten Luwu.

DAFTAR PUSTAKA

Agung S (2014).“*Remote Authentication Dial In User Service (RADIUS) untuk Autentikasi Pengguna Wireless LAN*”, Laporan Akhir EC-5010 Institut Teknologi Bandung.

Febyatmoko, dkk. (2011). *Otentikasi, Otorisasi & Pelaporan Koneksi UserWirelessChillispot Dan Server RADIUS.*

Kunang,Yesi Novaria dan Zuhri,YadiIlman.*”Autentikasi Pengguna Wireless Lan Berbasis Radius Server (Studi Kasus WLAN Universitas Bina Darma)”,*

Sudiarta,Pande Ketut, *“Implementasi Sistem Autentikasi Jaringan Hotspot Universitas Udayana Dengan Menggunakan Open Source Freeradius”*.

Utomo,Eko Priyo.(2012).*Membangun Jaringan Komputer dan Server Internet,* Yokyakarta : MediaKom.

Yunus,Amak *“Implementasi Sistem Otentikasi Pada Pengguna Jaringan Hotspot Di Universitas Kanjuruhan Malang Guna Meningkatkan Keamanan Jaringan Komputer”*.

C. Rigney, S. Willens, A. Rubens, W. Simpson, “*Remote Authentication DialIn UserService*(RADIUS)”,RFC 2138