Jurnal Ilmu Komputer dan Sistem Informasi (JIRSI) **e-ISSN 2830-3954**
Volume: 2, Nomor : 3, September 2023 : 206-215 **p-ISSN 2830-6031**
https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Keamanan Jaringan Hotspot Mikrotik Menggunakan Metode Otentikasi Pengguna dengan Captcha dan IP-Binding Untuk Filtering User

Network Security of MikroTik Hotspot Utilizing User Authentication Methods with CAPTCHA and IP-Binding for User Filtering

Muhammad Rayza*[1] , Ari Usman[2], Arif Budiman [3]
[1,2,3] Prodi Teknik Informatika Universitas Harapan Medan, Jl. HM. Joni No. 70 C, Teladan Baru Kota Medan, Sumatera Utara, Indonesia.
E-mail: [1,]muhammadrayza39@gmail.com, [2]ariusman09@gmail.com, [3]ariefdiman13@gmail.com

Abstrak

Salah satu layanan yang paling umum disediakan bagi pengguna internet adalah jaringan hotspot. Hotspot ini berfungsi sebagai area publik yang dilengkapi dengan akses jaringan nirkabel. Banyak lokasi hotspot yang tersedia, bahkan beberapa di antaranya menawarkan akses gratis, memungkinkan semua orang menikmati layanan ini tanpa dikenakan biaya. Namun, masalah keamanan menjadi perhatian penting dalam penggunaan fasilitas hotspot di zona publik karena sifat terbuka tempat tersebut. Selain itu, penggunaan jaringan hotspot juga memiliki kelemahan - adanya kerentanan keamanan akibat kurangnya perhatian administratif. Berdasarkan temuan dari literatur yang ada, pendekatan efektif untuk meningkatkan keamanan nirkabel melibatkan otentikasi pengguna melalui metode CAPTCHA dan IP-binding untuk penyaringan pengguna. Metode otentikasi pengguna ini diharapkan dapat mengoptimalkan keamanan jaringan hotspot, sehingga hanya individu yang diizinkan dan terdaftar yang dapat mengakses layanan tersebut.

Kata kunci : Hotspot, Mikrotik, Captcha , Ip-binding

Abstrct

One of the most common services provided for internet users is a hotspot network. This hotspot functions as a public area equipped with wireless network access. Numerous hotspot locations are available, with some even offering free access, allowing everyone to enjoy this service without any charges. However, security concerns are a significant focus in utilizing hotspot facilities in public zones due to the open nature of these places. Additionally, the use of hotspot networks also has a drawback - the existence of security vulnerabilities due to a lack of administrative attention. Based on findings from existing literature, an effective approach to enhancing wireless security involves user authentication through CAPTCHA and

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

IP-binding methods for user filtration. It is anticipated that this user authentication method can optimize hotspot network security, ensuring that only authorized and registered individuals can access the service.

***Keywords**: Hotspot, Mikrotik, Captcha , Ip-binding*

1. PENDAHULUAN

Mikrotik merupakan sebuah sistem operasi yang di rancang pada sebuah perangkat keras jaringan. Perangkat keras yang digunakan dapat dijadikan sebuah perangkat jaringan yang cukup kuat yang terdiri dari beragam jenis fitur yang dibuat untuk konfigurasi sebuah jaringan komputer baik dalam bentuk *wire* maupun jaringan *wireless*. *Mikrotik* didesain dengan bentuk *portable* dimana memberikan efisiensi tampilan GUI, mudah digunakan dalam keperluan adminstrasi sistem jaringan komputer. Konfigurasi yang dilakukan pada sebuah perangkat *mikrotik* memberikan hak akses konifgurasi seperti modem (DHCP server) dapat dilakukan dengan baik, mentranslasikan penerjemahan IP seperti penggunaan NAT, dimana memanfaatkan ketentuan yang ada seperti perusahaan , Pendidikan , sekolah bahkan *home user* yang digunakan untuk melaukan akses koneksi jaringan internet [1].

Data adalah kumpulan aset terbesar bagi setiap keperluan organisasi bisnis, diperlukan upaya khusus dalam memelihara sebuah data dengan baik yang dimana merupakan perhatian utama setiap organisasi. Pada umumnya dunia IoT digunakan di semua industri untuk penggunaan dan pengelolaan data yang efisien. Organisasi yang ada diharapkan dapat memperkaya data dari penggunaan perangkat yang di-butuhkan untuk meninjau resiko yang ada. Keamanan data menjadi perhatian utama dalam pengelolaan dan pemeliharaan data perusahaan. Kecerdasan bisnis terus berjalan berdasarkan pertahanana data yang digunkaan untuk memilih dan memilah berdasarkan data historis dan saat ini untuk memprediksi dan melakukan perhitungan pada apa yang terjadi di masa depan. Karena masalah keamanan data, data organisasi dapat berisiko karena potensi ancaman, kehilangan data, dan manipulasi data [2].

Hotspot (Wi-Fi) juga menjadi salah satu bentuk eksploitasi teknologi di lokasi ruang publik seperti taman, perpustakaan, restoran, kampus, kantor, dan bahkan bandara. Beberapa di antaranya bahkan dapat diakses tanpa biaya. Biasanya, perangkat *portable* seperti *notebook*, *laptop*, atau PDA dapat digunakan untuk terhubung kedalam jaringan internet melalui jaringan *hotspot*. Konsep *hotspot* (Wi-Fi) pertama kali diusulkan pada tahun 1993 oleh Breet Stewart. Dengan teknologi ini, seorang individu dapat mengakses jaringan *internet*, melalui komputer atau laptop pribadi mereka di lokasi-lokasi di mana *hotspot* (Wi-Fi) tersedia [3].

Sistem otentikasi pengguna pada jaringan *wireless* dilakukan dengan WPA2/PSK yang diperoleh dari security default yang ada pada perangkat *access point*, dalam melakukan pengamanan sederhana dengan memakai kunci *WPA*. *Key* pada *WPA* namun

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

masih memiliki celah keamanan yang signifikan sehingga memerlukan metode verifikasi agar dapat melindungi jaringan hotspot menjadi lebih baik.

CAPTCHA (Publikasi Sepenuhnya Otomatis) merupakan sebuah Tes Turing yang dilakukan untuk membedakan (komputer dari manusia). pada dasarnya captcha ini merupakan program sedikit demi sedikit yang digunakan Kebanyakan manusia bisa melewatinya, tapi komputer tidak bisa melakukan verifikasi CAPTCHA tersebut. captcha digunakan untuk mencegah perangkat lunak otomatis (bot) melakukan tindakan atas nama orang sungguhan. Tujuan utama CAPTCHA adalah untuk memberikan tes yang dapat dijawab dengan mudah oleh manusia tetapi tidak dapat dijawab oleh Komputer [4].

IP *Binding* merupakan sebuah fitur yang terdapat pada perangkat *mikrotik*. kegunaan dari IP *binding* ni digunakan untuk dapat melakukan menajemen akses user pada suatu jaringan *hotspot*. *hotspot* dari IP binding ini dilakukan untuk memberikan IP pada perangkat yang memberikan sinyal *interfaces* seperti *access point* dan pada tiap perangkat *client* yang terhubung kedalam suatu jaringan yang terkonfigurasi kedalam IP *binding* tersebut[5].

Access point merupakan sebuah perangkat yang digunakan untuk menyebarkan suatu jaringan menggunakan moda transportasi wireless. Penempatan acces point yang baik ada pada titik tertentu merupakan salahs atu permasalahan yang ada dalam bidang infrastruktur jaringan. Karena penempatan access point yang baik memerluukan pemikiran dan analisis lengkap sebelum di-implementasikan. Berbagai fakfor tertentu seperti hambatan sinyak yang digunakan untuk dapat mengganggu sinyal yang diterima dari titik akses (mounting) dari perangkat penerima. Lokasi titik tersebut mempengaruhi jangakauan penerima dari sebuah jaringan WI-Fi. Semakin baik lokasi titik akses yang diberikan , maka akan menampilkan titip ases semakin baik. Persiapan tertentu ini disebutkan mempengaruhi kualitas jaringan yang diberikan[6] **.**

2. METODOLOGI PENELITIAN

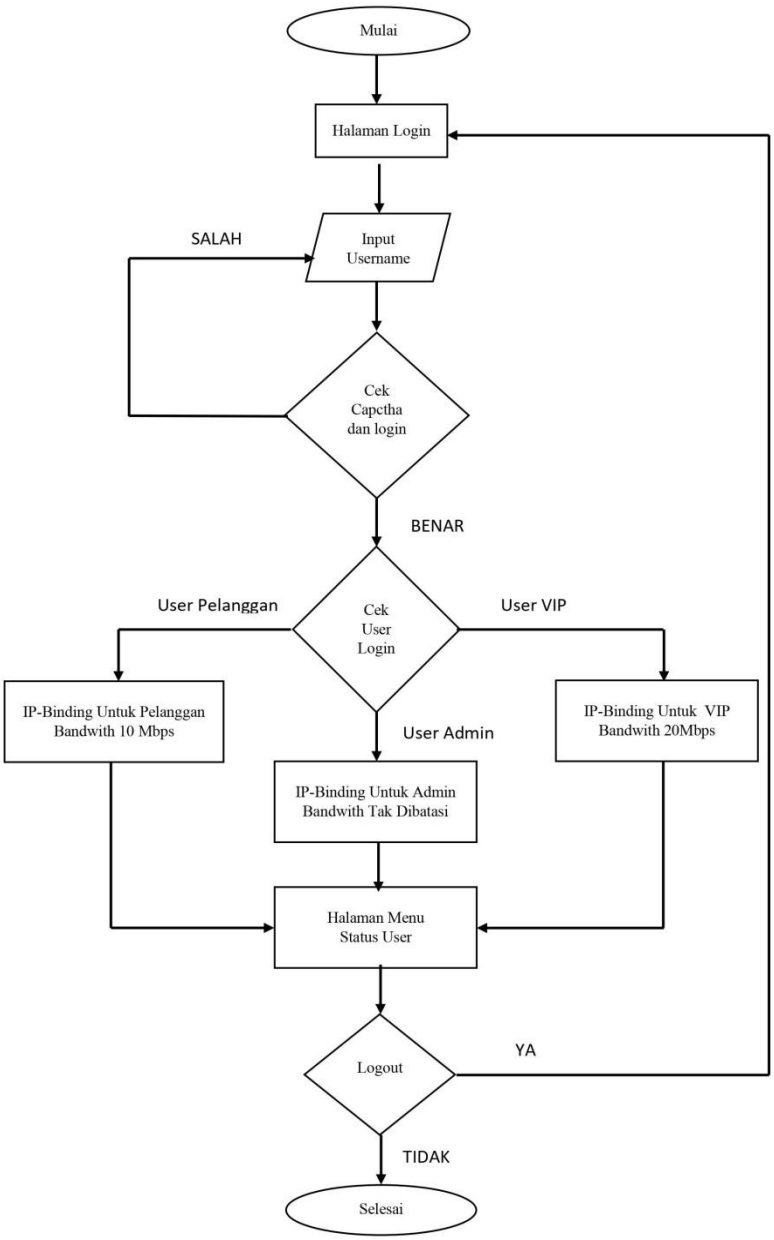
Pada penelitian ini , peneliti mengimplementasikan penggunaan hasil dari metode pengembangan berbasis kualitatif yang digunakan sebagai berikut dibawah ini:

1. Studi Literatur
   Melakukan pencarian teori pendukung dan komponen yang diperlukan dalam pembuatan penelitian ini. Informasi tersebut diperoleh dengan cara membaca pada buku referensi serta mencari sumber ilmiah melalui internet.
2. Analisa Sistem

Pada tahap ini penulis menerapkan sebuah proses tahap awal dari sebuah bentuk dari perancangan *sistem* untuk membangun keamanan jaringan *hotspot* Mikrotik menggunakan metode otentikasi pengguna dengan *Captcha* dan *Ip-Binding.*

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

2.1 Flowchart Sistem



Gambar 1. Flowchart Sistem

Pada gambar 1 diatas, menjelaskan bagaimana sebuah *user* dapat terhubung kedalam suatu sistem jaringan yang dibangun menggunakan perangkat mikrotik. Perpaduan dari sistem menggunakan teknologi kombinasi dari teknologi *captcha* dan IP *binding* menggunakan perangkat *mikrotik*.

2.2 Perancangan Dasar Sistem

Tahap ini perlu dilakukan dengan memanfaatkan alur flowchart yang telah dibuat sebelumnya, peracangan sistem dapat membuat keamanan jaringan *hotspot* Mikrotik

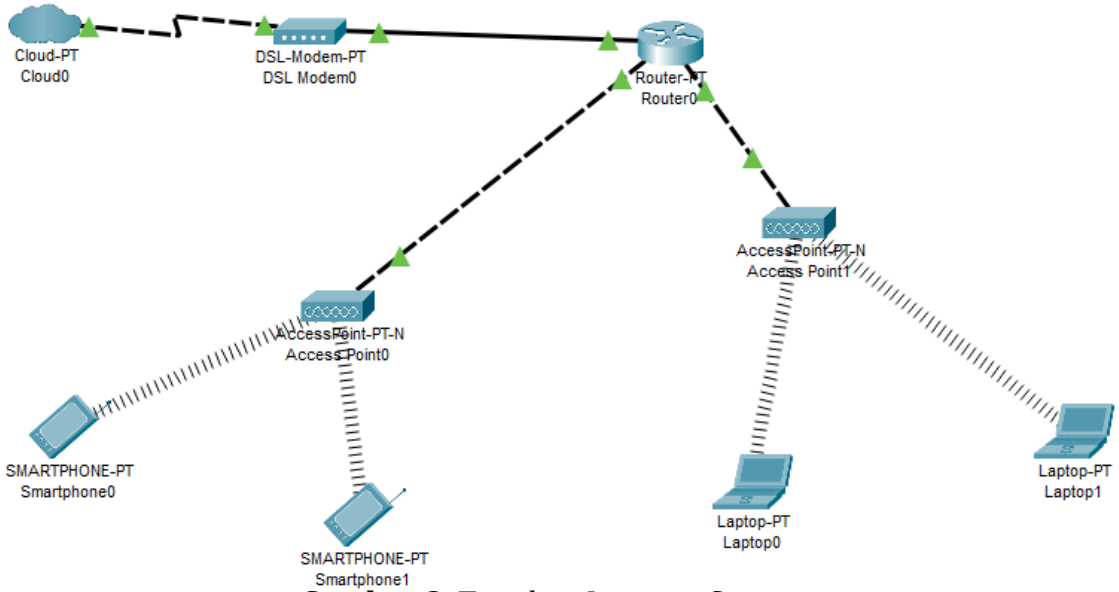
© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

menggunakan metode otentikasi pengguna dengan memanfaatkan tekonologi *Captcha* dan IP-*Binding* untuk *filtering user* agar jaringan *hotspot* hanya dan bisa dapat dibuka oleh pengguna yang telah terdaftar atau telah diberi izin dan *login* menggunakan otentikasi *Captcha* agar terhindarnya dari *spam* atau *login bruteforce spammer*. Detail dari perancangan system ini dapat dilihat pada tabel 1 yang memperlihatkan detail penggunaan alat yang ada.

Tabel 1 Alat yang digunakan untuk melakukan perancangan sistem

No	Nama Barang	Jumlah
1	Modem	1 Unit
2	Router Mikrotik	1 Unit
3	Access Point	1 Unit
4	Laptop	1 Unit
5	Kabel UTP	1 Rol
6	RJ 45	1 Kotak

2.3 Topologi Sistem Jaringan Yang Digunakan



Gambar 2. Topologi Jaringan Sistem

Pada gambar 2 topologi diatas menjelaskan kaitan antara tiap tiap perangkat jaringan dapat saling terkoneksi kedalam jaringan *internet* yang dikonfigurasi menggunakan perangkat mikrotik sebagai sistem yang mengatur jalannya hak akses pemberikan jaringan internet

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

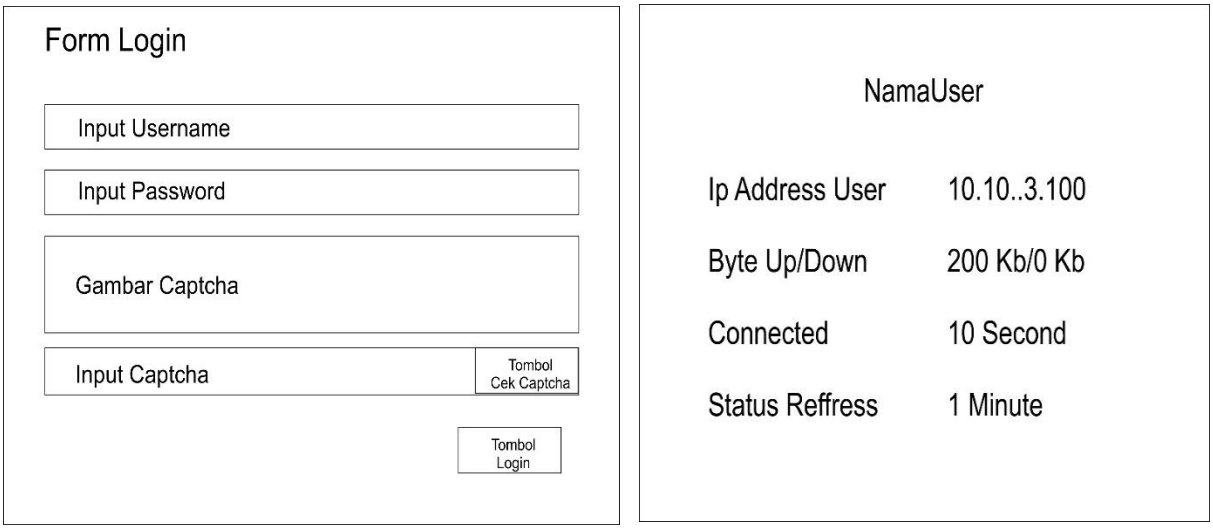
2.4 Pembagian IP Address Pada Lingkup Jaringan

Pada tahap ini dilakukan pembagian *routing* IP *address* untuk memberikan identitas agar terarah dan terstruktur pada suatu jaringan ataupun perangkat *client* yang membutukan sautu koneksi jaringan. Adapun pembagian dari IP address tersebut dapat dilihat pada tabel 2 dibawah berikut ini :

Tabel 2 Pembagian IP address

No	Nama Perangkat	IP Address	Subnet Mask	Gateway
1	Modem (Source Internet)	192.168.0.1	255.255.255.0	-
2	Router Mikrotik ether 1	192.168.0.254	255.255.255.0	192.168.0.1
3	Router Mikrotik ether 2	10.10.2.254	255.0.0.0	-
4	Router Mikrotik ether 3	10.10.3.254	255.0.0.0	-
5	Access Point 1	10.10.2.1	255.0.0.0	10.10.2.254
6	Access Point 2	10.10.3.1	255.0.0.0	10.10.3.254
7	Client	DHCP	255.0.0.0	DHCP

2.5 Perancangan Tampilan Aplikasi



Gambar 3. Rancangan Tampilan Login

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

Perancangan yang dilakukan pada gambar 3 diatas merupakan sebuah sketsa dasar yang digunakan yang terdiri dari 2 betuk *form* yaitu *form login* dan *form* nama *user* yang terkonekesi kedalam jaringan *internet*.

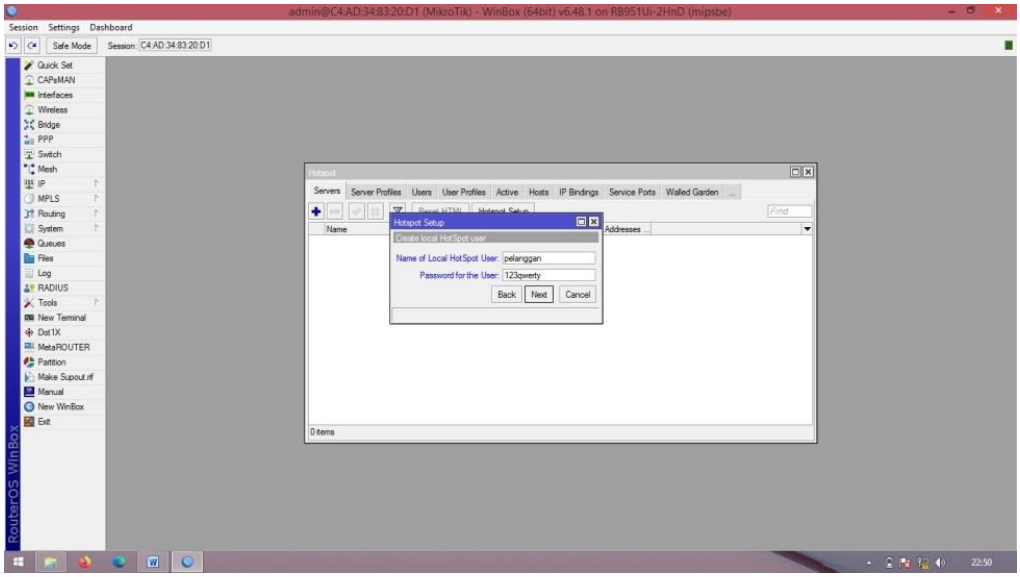
3. Perancangan Sistem

Perancangan sistem diperlukan untuk melakukan konfigurasi terhadap tiap tiap perangkat pengujian yang ada, perangkat tersebut nantinya akan memberikan hasil *output* berupa tiap pengujian yang dapat dilihat pada point 4.

3.1 Konfigurasi Hotspot

Pada tahap ini dilakukan konfigurasi *Hotspot Mikrotik* yang dapat dilihat pada tahapan sebagai berikut.

1. Langkah konfigurasi *Hotspot* Mikrotik *Ether2*
   IP → *Hotspot* → pilih tab ***Servers*** → *Hotpot Setup* → Isi *Hotspot Interface = Ether2* → *Next,*
2. Isi *Local Address Of Network = 10.10.2.254/24* → *Next.*
3. Isi *Address Pool Of Network = 10.10.2.2 – 10.10.2.253* dan *select certificate = none* → *Next,*
4. Isi *Address Of SMTP Server = 10.10.2.254* → *Next,*
5. Isi *DNS Servers = 8.8.8.8 dan 8.8.4.4* → *Next,*
6. Isi *DNS Name = loginvip.com* → *Next,*
7. Isi *Name Hotspot Use = vip* dan *Password* = 123qwerty → *Next,*

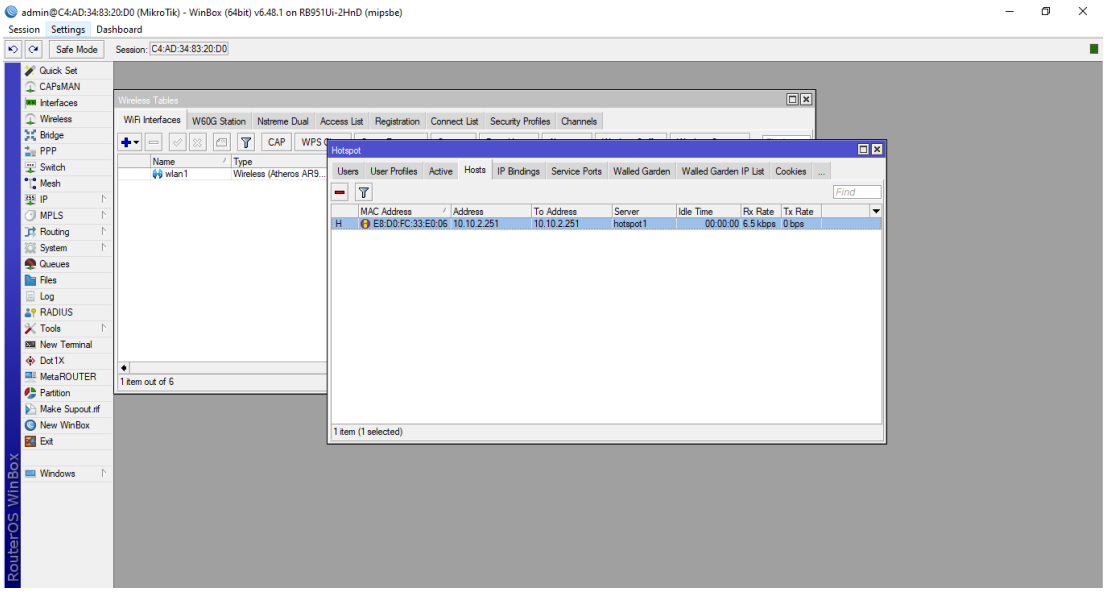


Gambar 4. Konfigurasi Hotspot

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

3.2 Konfigurasi IP - Binding

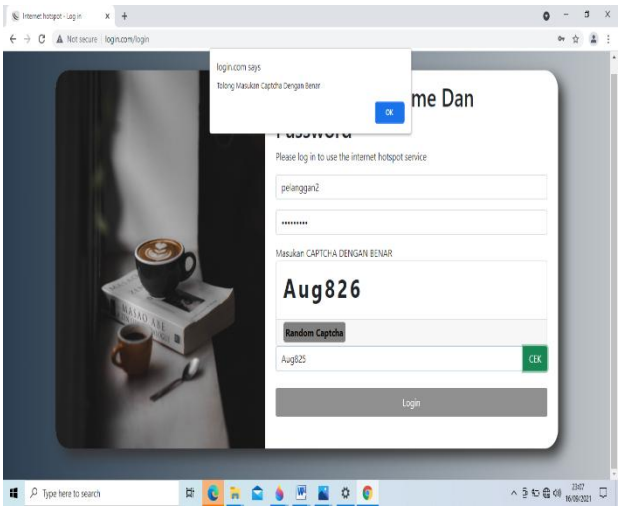
Digunakan untuk memanagament akses *user* pada suatu jaringan *hotspot* tesebut, maksud dari *management* disini yaitu sebuah ketentuan boleh tidaknya *user* tersebut terhubung kedalam suatu jaringan *hotspot*.

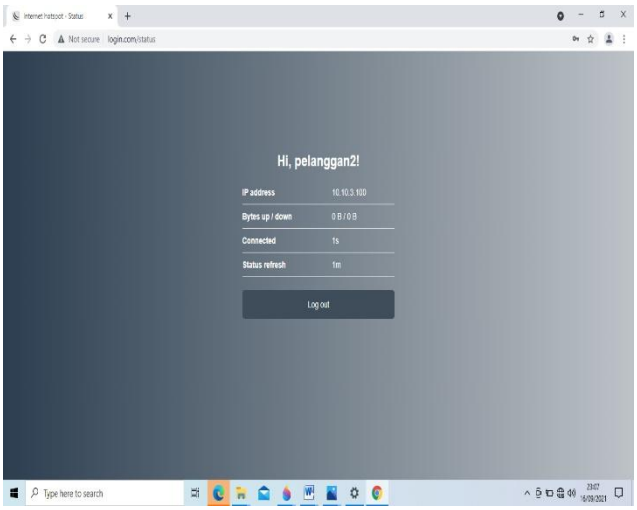


4. Hasil Dan Pembahasan

Pada tahap ini dilakukan pengujian sistem yang dibangun akan menampilkan hasil yang sudah dirancang pada tahap perancangan maupun sebelum dirancang yaitu implementasi sistem Keamanan Jaringan *Hotspot* Mikrotik Menggunakan *Metode* Otentikasi Pengguna Dengan *Captcha* Dan *IP-Binding* Untuk Filtering *User.*

4.1 Tampilan Login Hotspot Mikrotik





© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

Pada halaman *login hotspot mikrotik* Masukan *username* dan *password* yang telah diberikan, contoh :

Username = pelanggan2

Password = 123qwerty

Dan masukan *Captcha* sesuai yang tertulis. Lalu klik tombol *login* untuk menggunakan *internet.*

4.2 Bandwith User Connection

Untuk pelanggan dikategorikan kedalam dua jenis pelanggan yaitu : keperluan *bandwith* pelanggan dan *bandwith* VIP diberikan *bandwith download* sebesar 10Mbps Dan *Upload* 5Mbps. Hasil penugjian dapat dilihat pada tabel 3 dibawah berikut.

Table 3. Pengujian *Bandwith User* Pelanggan

Pengujian	Download	Upload
Pengujian ke-1	9.7 *Mbps*	4.8 *Mbps*
Pengujian ke-2	9.5 *Mbps*	4.5 *Mbps*
Pengujian ke-3	9.8 *Mbps*	4.8 *Mbps*
Pengujian ke-4	9.6 *Mbps*	4.4 *Mbps*
Pengujian ke-5	9.7 *Mbps*	4.9 *Mbps*
Pengujian ke-6	9.8 *Mbps*	4.5 *Mbps*
Pengujian ke-7	9.6 *Mbps*	4.8 *Mbps*
Pengujian ke-8	9.9 *Mbps*	4.7 *Mbps*
Pengujian ke-9	9.6 *Mpbs*	4.5 *Mbps*
Pengujian ke-10	9.7 *Mbps*	4.8 *Mbps*

Table 4. Pengujian *Bandwith User* VIP

Pengujian	Download	Upload
Pengujian ke-1	28.7 *Mbps*	14.8 *Mbps*
Pengujian ke-2	28.5 *Mbps*	14.5 *Mbps*
Pengujian ke-3	29.8 *Mbps*	14.9 *Mbps*
Pengujian ke-4	28.8 *Mbps*	14.4 *Mbps*
Pengujian ke-5	27.9 *Mbps*	14.9 *Mbps*
Pengujian ke-6	28.5 *Mbps*	14.5 *Mbps*
Pengujian ke-7	28.6 *Mbps*	14.8 *Mbps*
Pengujian ke-8	29.5 *Mbps*	14.7 *Mbps*
Pengujian ke-9	28.9 *Mpbs*	14.5 *Mbps*
Pengujian ke-10	29.7 *Mbps*	14.8 *Mbps*

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)

5. Kesimpulan

Berdasarkan penjelasan dan uraian pada bab sebelumnya ditarik beberapa kesimpulan dalam penelitian ini yakni sebagai berikut :

1. Penelitian ini telah berhasil membuat keamanan Mikrotik menggunakan fitur *hotspot* dengan otentikasi pengguna menggunakan *captcha* dan *filtering user* menggunakan *Ip-Binding* yang membuat jaringan *wireless* menjadi susah di bobol oleh orang yang tidak bertanggung jawab baik itu dengan menggunakan *bot* yang dibuat khusus untuk membobol jaringan.
2. Penelitian ini juga telah berhasil merubah tampilan *login hotspot* yang sesuai dengan tampilan yang diinginkan.serta pada penelitian ini juga telah berhasil membuat tampilan *login hotspot Mikrotik* menggunakan *Captcha* yang dibuat menggunakan bahasa pemrograman *html,css* dan *javascript*.
3. *IP Binding* adalah sebuah fitur yang terdapat pada *hostpot Mikrotik* yang dapat di gunakan untuk memanagament akses *user* pada jaringan *hotspot* tesebut, Pada penelitian ini penulis berhasil *memanagement user* untuk mem-*filter user* yang boleh mengakses *hotspot* tanpa *username* dan *password* maupun yang harus *login* menggunakan *hotspot* dengan *username* dan *password*.
4. Metode *simple queue* digunakan untuk memberi *limit bandwidth* pada tiap user dimana kecepatan *bandwidth* pada *modem* yaitu 100 *Mbps* dan dibagi rata pada tiap *client* sesuai dengan jumlah *client* yang terhubung sehingga membuat kecepatan *internet* pada menjadi lebih stabil.

DAFTAR PUSTAKA

[1] T. Rahman, B. Ibrahim, H. Nurdin, and M. Qomaruddin, "Hierarchical Token Bucket (Htb) Pada Quality of Service Pt. Eka Bogainti," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 82–91, 2023, doi: 10.36341/rabit.v8i1.2963.

[2] N. I. Putri, R. Komalasari, and Z. Munawar, "Pentingnya Keamanan Data Dalam Intelijen Bisnis," *J. Sist. Inf.*, vol. 1, no. 2, pp. 41–49, 2020.

[3] M. Gustiawan, R. J. Yudianto, J. Pratama, and A. Fauzi, "Implementasi Jaringan Hotspot Di Perkantoran Guna Meningkatkan Keamanan Jaringan Komputer," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 4, pp. 244–247, 2021, doi: 10.32672/jnkti.v4i4.3098.

[4] D. Rusmana, "Rancang Bangun Pengaman Sistem Login Menggunakan Metode Captcha," *Incomtech*, vol. 10, no. 1, pp. 46–52, 2021, [Online]. Available: https://ejournal.istn.ac.id/index.php/incomtech/article/view/1061%0Ahttps://ejournal.istn.ac.id/index.php/incomtech/article/download/1061/729

[5] H. S. Syahputra and R. WIjaya, "Pembangunan Jaringan Hotspot Berbasis Mikrotik pada Kampung Tematik di Kecamatan Padang Utara," *Maj. Ilm. UPI YPTK*, vol. 29, no. 1, pp. 60–66, 2022, doi: 10.35134/jmi.v29i1.108.

[6] A. Wanto, J. T. Hardinata, H. F. Silaban, and W. Saputra, "Pada Jaringan Wi-Fi Menggunakan Metode Simulate Annealing," *J. Sains Komput. Inform. (J-SAKTI*, no. 1, pp. 134–143, 2017, [Online]. Available: http://ejurnal.tunasbangsa.ac.id/index.php/jsakti

© 2023 The Author(s). Published by UNITY ACADEMY . This is an open access article under the CC BY-SA license (http://creativecommons.org/licenses/by-sa/4.0/)