Wireless Lan Network Authentication Captive Portal

Nita Rosa Damayanti
Department of Informatics Management
Universitas Bina Darma
Palembang, Sumatera Selatan
1nita_rosa@gmail.com

Muhammad Sobri
Department of Informatics Management
Universitas Bina Darma
Palembang, Sumatera Selatan
sobri@binadarma.ac.id

***Abstract*—The development of wireless networks is needed to improve security and comfort when using it because of the current management of the hotspot network at PT. Tri Sapta Jaya which uses the old system has many shortcomings because there is no monitoring system and the use of the same password for each user and there are no data restrictions. To overcome these shortcomings, a new system is needed, using the Mikrotik Routerboard-based Captive portal authentication system that can be used to create an account for each different user to log in to the portal that will appear in the browser when connected to the network and the administrator can monitor devices that are connected to the network. hot spot. In research to develop the Captive portal system several stages are carried out using the waterfall system development method, namely analysis, design, implementation, testing and maintenance, in which case the research can produce a security system that runs optimally, safely, comfortably and efficiently.**

Keywords—captive portal, hotspot, proxy, routerboard, waterfall)

I. INTRODUCTION

The development of the internet which was initially accessible using a cable network and continues to develop so that it can be accessed using a wireless network called wireless [1]. The use of wireless networks in information technology is now widely used, because of the advantages gained, Namely, that wireless network no longer uses cable but use radio waves as a medium for sending data for communication needs and access to information from the internet. Wireless networks are actually very vulnerable from cyber crimes committed by hackers to hack or steal data and information, because it can be accessed in general, therefore the development of wireless network security at hotspots is needed to prevent it [2].

PT. Tri Sapta Jaya which is located at Jln. Lt. Gen. Bambang Utoyo Palembang, is a company engaged in the business of distributing pharmaceutical and health products that focuses on expanding the pharmaceutical distribution network in the lower market and also to better reach remote areas. PT. Tri Sapta Jaya applies wireless computer networks as a medium for exchanging data and information. Currently the wireless network at PT. Tri Sapta Jaya has a hotspot facility that uses WPA2-PSK as a security system to authenticate usage in order to access the internet. The use of the WPA2-PSK security system at PT. Try Sapta Jaya itself has been built since 2009 until now. Actually the use of wireless networks in the hotspot area at PT. Tri Sapta Jaya still has various problems that become obstacles in the hotspot security system, namely the lack of management and review of hotspot activities or the absence of a system that monitors the activities in the network as well as open or public hotspots.

The use of WPA2-PSK as a wireless network security system has a loophole namely, the use of the same password to be able to access the internet and can be used by many users who know the password is also prone to hacking of PT. Try Sapta Jaya network systems such as sniffing, arp poisoning, data theft and crime other cyber [3]. Examples of cases that have occurred at PT. Tri Sapta Jaya, which occurred in 2012, has lost data about the supply of medicines that can harm the company.

These problems disrupt hotspot activities that should be stable or smooth to be slow and often occur when accessing hotspots at PT. Tri Sapta Jaya. Systems like this that make using hotspots, less secure.

Wireless network security at PT. Tri Sapta Jaya needs development by replacing the WPA2-PSK security system with a Mikrotik Routerboard based Captive portal security system that allows only registered users to access hotspots where users must pass the authentication process or log in by entering a username and password to access the network and be able to access the network monitoring active users [4] and also what devices are currently connected to the PT. Tri Sapta Jaya.

II. METHODOLOGY

The research method used in this study is the waterfall methodology which is analysis, design, implementation, testing, and maintenance to produce a security system that is targeted to be optimal, safe, comfortable and efficient [5].

A. System analysis

System analysis is an analysis of network security systems that run at PT. Tri Sapta Jaya Palembang, which is currently still very minimal, has not been managed properly, so it makes administrators have to work extra hard to find out a problem that occurs on the network at PT. Tri Sapta Jaya due

to the absence of a monitoring system and also network devices at PT. Tri Sapta Jaya is not configured optimally making network security very weak inside and outside and will have an impact on the confidentiality of data residing in PT. Tri Sapta Jaya Palembang because it uses WPA2-PSK with the same *hotspot password* for each *user*.

B. Data Analysis

Data analysis is an analysis of the data obtained by the author of research conducted at PT. Tri Sapta Jaya was then collected to help facilitate research.

The data collected by the author is the device used, the amount of space and floor at PT. Tri Sapta Jaya.

TABLE I. NUMBER OF DEVICES USED

No.	Device	Total
1.	computer (PC)	20
2.	*Server*	1
3.	*Switch*	2
4.	*Router*	1
5.	*Access Point*	2

TABLE II. TOTAL OF SPACE AND /FLOOR

No.	Floor	Space
1.	1	8
2.	2	6
3.	3	6

C. Procedure Analysis

Procedure analysis is performed by the author to see the comparison of the old system with the system that will be developed by the author by looking at the workings of the two systems.

The figure on the next page will show the differences between the two network security systems by looking at how they work.

• The system that will be developed is Captive portal.

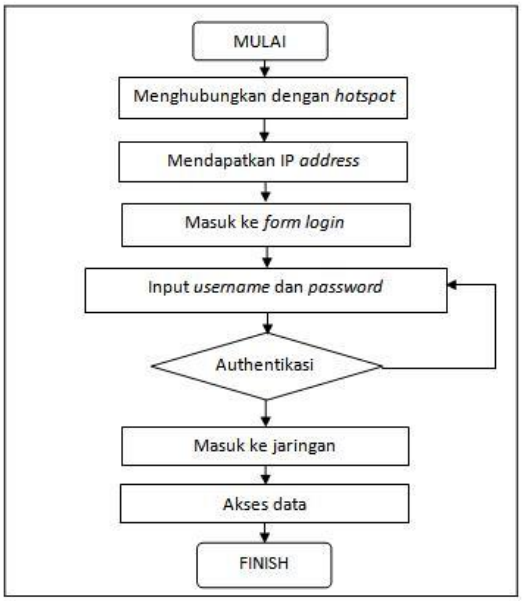

Fig. 1. Procedure Captive portal.

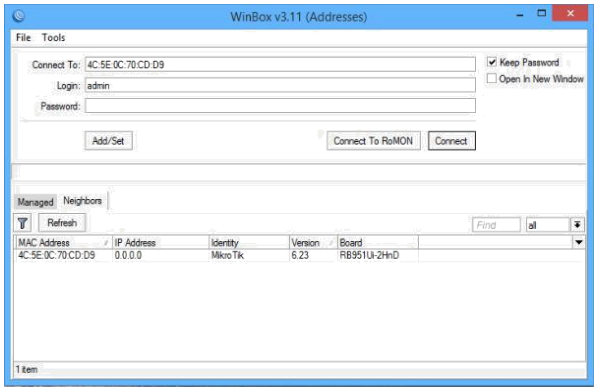

Fig. 2. Procedure WPA2.

D. Network Topology Design

To design network topology and configuration, the writer uses Cisco Packet Tracer 7.0 software or application program. This application is a network simulator application program that is often used as a medium of learning, training, and also in the field of research. This program is made by Cisco Systems. Initial display of Cisco Packet Tracer 7.0. can be seen in Figure 3

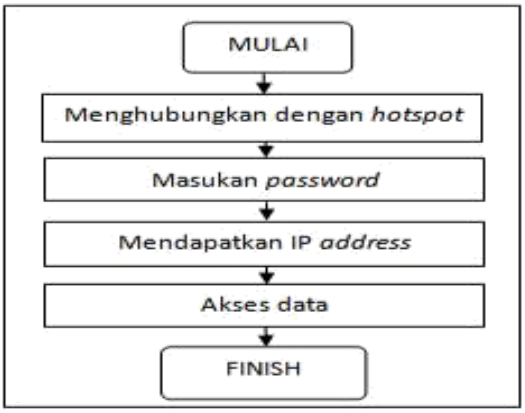

Fig. 3. Aplication Cisco Packet Tracer

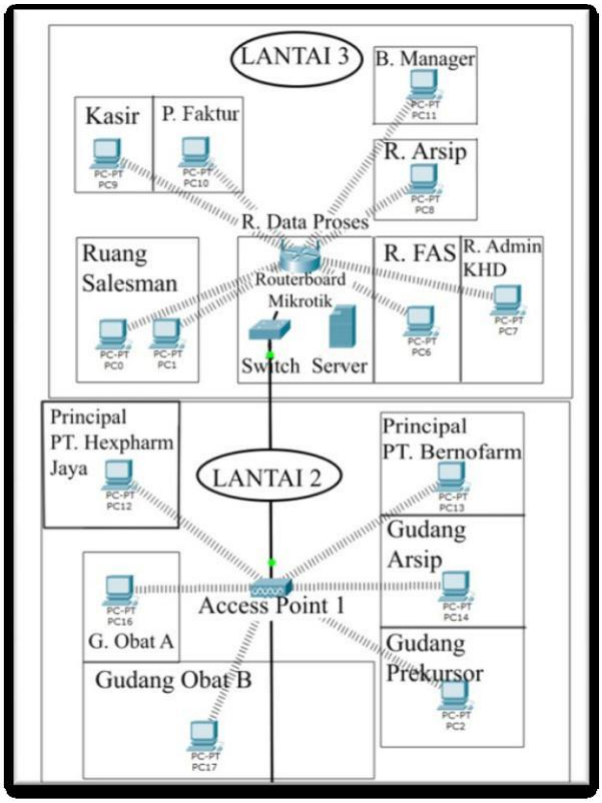

Fig 4. Aplication Cisco Packet Tracer

III. Results and Discussion

A. *Microtic Configuration*

In the research, the authors configure using Winbox v3. 11 software. Configuring a Mirotik routerboard using Winbox software with a GUI interface makes it easy for the writer to configure the Mikrotik routerboard.

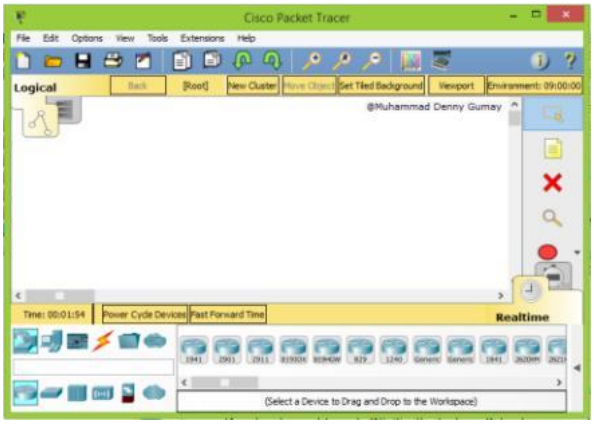

Fig. 5. Display Mikrotik login with winbox

B. *Microtic Internet Configuration*

Connecting Mikrotik routerboard to the internet by doing DHCP Client on Mikrotik so that Mikrotik gets an ip address from the public network by connecting Mikrotik to the modem then select the IP menu - DHCP Client

- Select Add to the Address List
- select Internet - Ok and Mikrotik will get an ip address as in Figure 6 and to ensure that Mikrotik is connected to the internet by pinging Google in Figure 2.3.

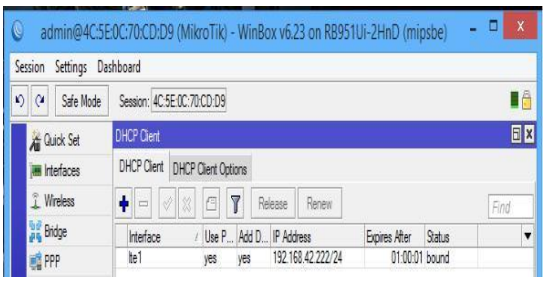

Fig. 6. Display Address List

Fig. 7. Process ping google.com.

C. *Configure Wireless Access Point*

Mikrotik wireless AP configuration is done to make Mikrotik an access point transmitter so that it can be used by opening wireless settings in the wireless menu, then activating wlan1 by clicking enable then Setting AP as shown in Figure 8 below.

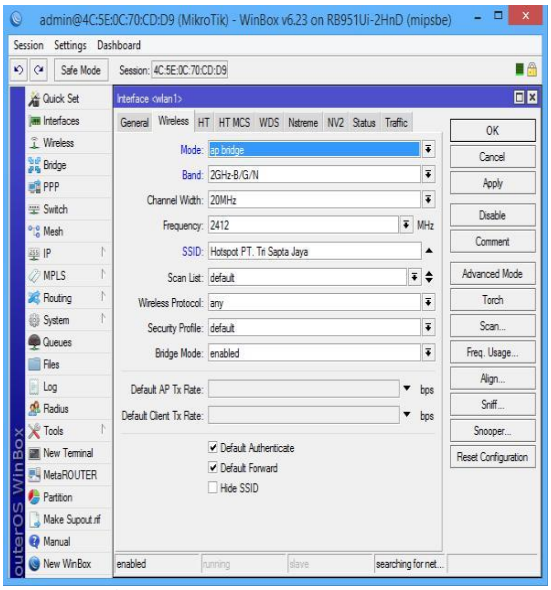

Fig. 8. Display interface wlan1.

D. Configure DHCP Server

This configuration is done so that the client device that is connected to get an IP Address dynamically. The DHCP Server configuration steps are:

- The first step is select the DHCP Server menu then DHCP Setup.

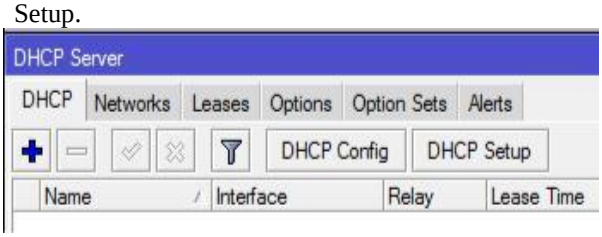

Fig. 9. Menu DHCP Server.

- The second Select the WLAN1 interface

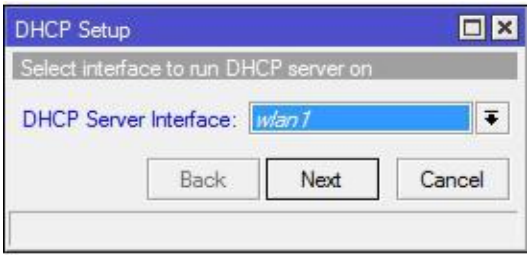

Fig. 10. DHCP Server Interface pada DHCP Setup.

- The third step is Network input used on the wlan1 interface.

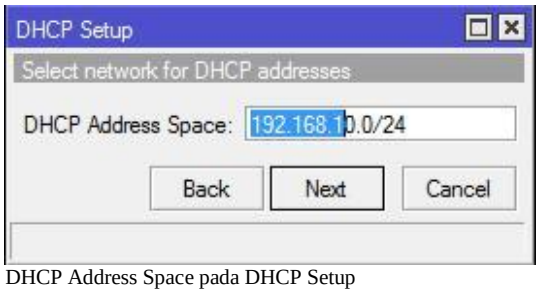

Fig. 11. DHCP Address Space pada DHCP Setup

- The fourth step is to enter the Gateway ip address

Fig. 12. Gateway for DHCP Network pada DHCP Setup

- The fifth step is the contents as below

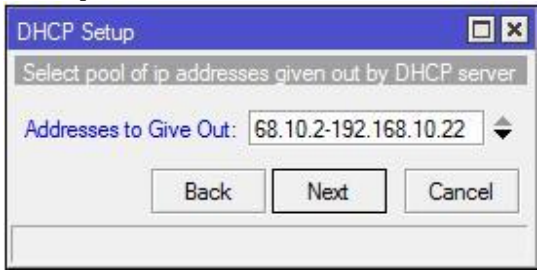

Fig. 13. Address to Give Out pada DHCP Setup

- The sixth step is to enter the DNS Server used

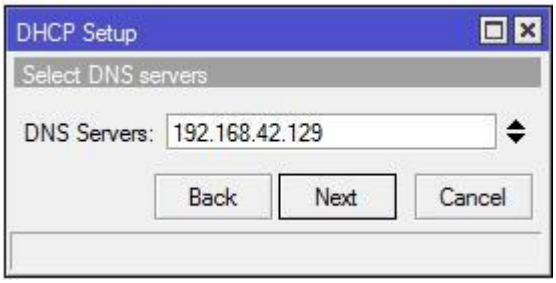

Fig. 14. DHCP Server pada DHCP Setup

- The final step is just next and finished.

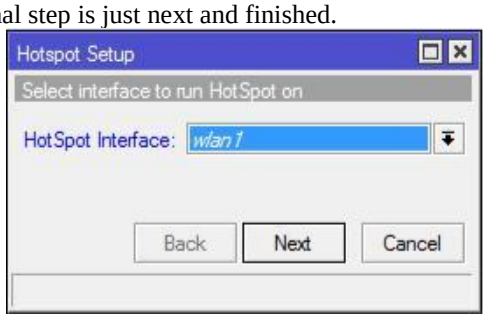

Fig. 15. Lease Time pada DHCP Setup

E. Configure Hotspot

Hotspot setup and configuration is done in a number of steps so that devices connected to the Mikrotik wireless AP will pass the authentication portal using registered users to access the internet and this configuration will be carried out with the steps below:

- The first step is select the wlan1 hotspot interface

Fig. 16. Hotspot interface on Hotspot Setup

- Next contents *Local of Network, next.*

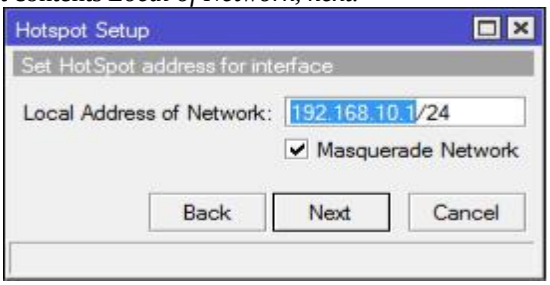

Fig. 2.13. Display Local of Network.

- Then fill in the Address Pool of Network, next.

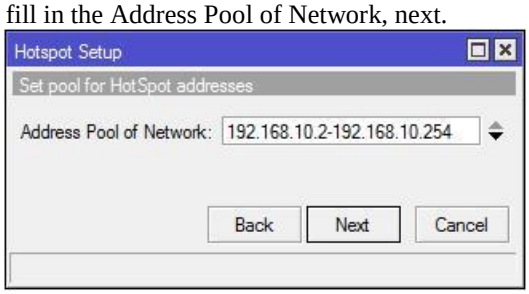

Fig. 17. Display Address Pool of Network

- Fill in the Domain name server in accordance with the modem being used, next.

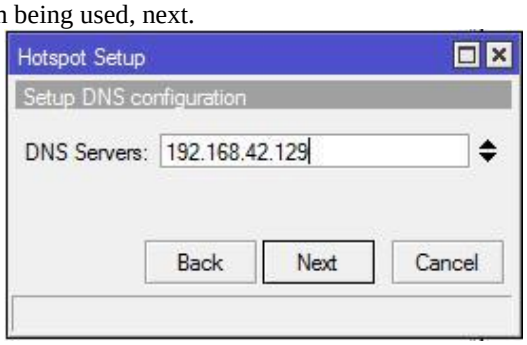

Fig. 18. Display DNS Servers pada Hotspot Setup

- Fill in the DNS Name that will be used, next.

- Finally create a user for the Administrator, Done.

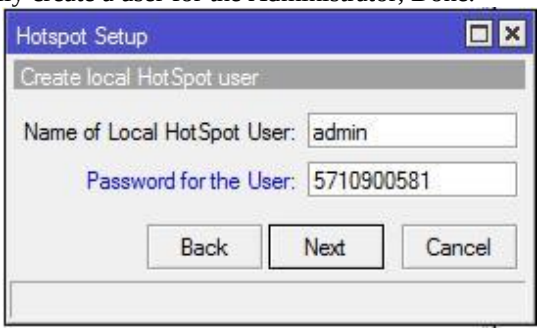

Fig. 19. User administrator pada Hotspot Setup

F. Configure Firewall NAT

This configuration aims to allow connected devices to access the internet or browse. The configuration is:

- The first step into the Firewall menu is then select NAT and add the following rule.

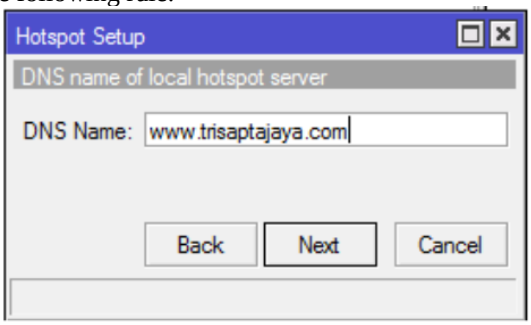

Fig. 20. Menu General NAT Rule

- The final step is enter the Action menu and select masquerade

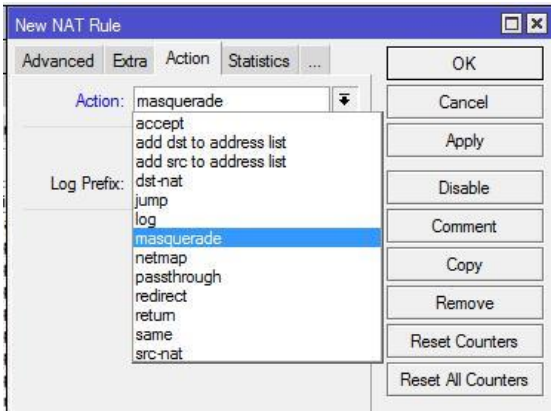

Fig. 21.. Menu Action NAT Rule

G. Configure DNS Server

This configuration is only done to add a check mark on the Allow Remote Request DNS Settings menu and there is no other configuration because the DHCP Client Mikrotik has already obtained DNS dynamically.

H. Hotspot Template Installation Configuration

Replacing the hoyspot template display by uploading the design file that has been created by selecting the files list menu and deleting the old hotspot folder then we upload the webpage file, the file list can be seen in Figure 22.

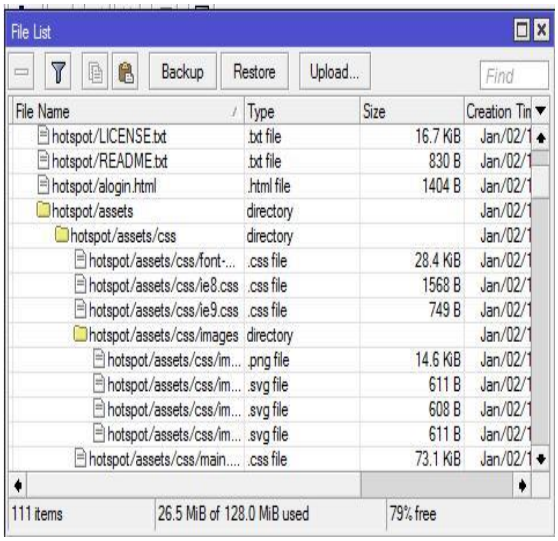

Fig. 22. Display File List.

I. User Management Configuration

User management is used to create and store user usernames and passwords that clients will later use to log in to access the internet. Making these users is made in the hotspot menu.

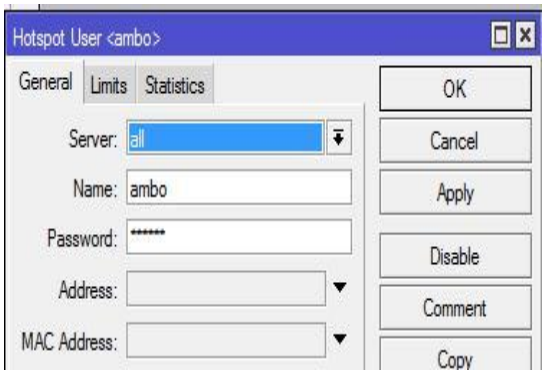

Fig. 23. User Creation

J. Testing the Hotspot and User Login Pages

User testing that has been made by the author to find out the results obtained from the configuration of the user is done with:

- Connect the client PC with PT. Tri Sapta Jaya then open the browser and a PT Hotspot Home Menu will appear. Tri Sapta Jaya as shown in Figure 24, then select information.
- After that PT. Tri Sapta Jaya as shown in Figure 25, then click enter.

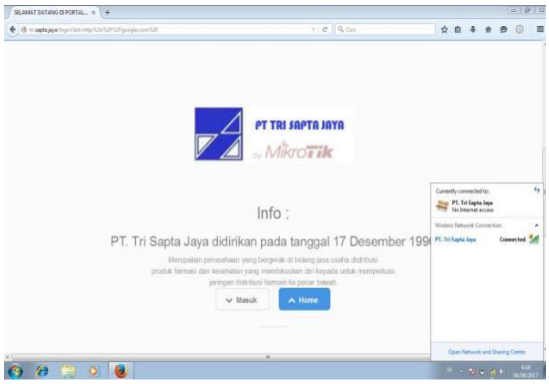

Fig. 24. Information page

Next, fill in with one of the users created by filling in your username and password, then click log in as shown in Figure 26.

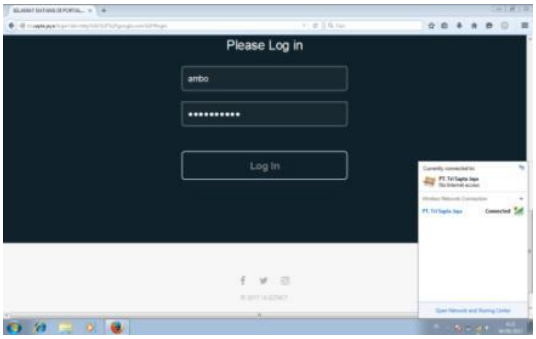

Fig. 25. Login page.

- If successful, it will appear as in Figure 27 below

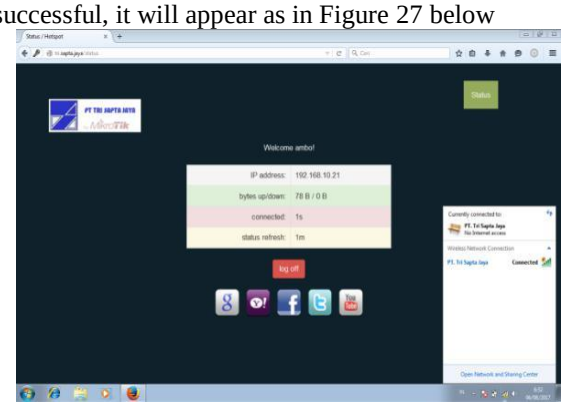

Fig. 26. Display successful login

- After successfully logging in, the user can access the internet

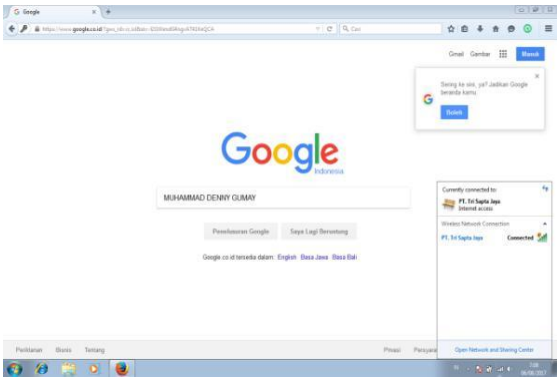

Fig. 27. Internet access.

K. Monitoring Testing

Monitoring is carried out to see what devices (hosts) are connected to the network and valid users of staff employees who are accessing PT. Tri Sapta Jaya is to see whether there is a suspicious device connected to the company network or not.

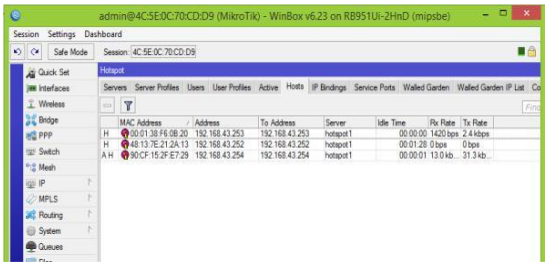

Fig. 28. Host menu on Mikrotik Hotspot

Figure 29 shows several hosts or devices connected to the PT. Tri Sapta Jaya. Connected devices either have logged in or cannot be monitored on this host menu.

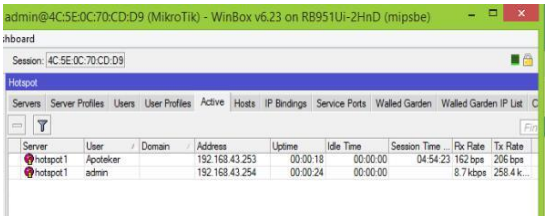

Fig. 29. Active menu on Mikrotik Hotspot

Figure 29 shows that there are 2 users who are currently connected to the hotspot, they are an admin and pharmacist, and also on this menu we can see the session time too.

IV. CONCLUSIONS

Based on research conducted by researchers, it can be concluded that:

- The use of Authentication using the Mikrotik Routerboard-based Captive portal on PT. Tri Sapta Jaya provides more effective and efficient access by:

- Every Staff and Employee at PT. Tri Sapta Jaya has their respective Username and Password.

- Restrictions on the use of hotspots can be set and adjusted according to usage.

- Use of the Mikrotik Routerboard-based Captive portal on the Wireless LAN Network at PT. Tri Sapta Jaya can make it easier for administrators to manage and monitor users or clients who are connected to the network.

REFERENCES

[1] M. Ulfa, M. Sobri, and I. Seprina, "Analisis perbandingan ipv4 dan ipv6 dalam membangun sebuah jaringan," Snit, pp. 342–346, 2014.

[2] S. Rumalutur, "Analisis Keamanan Jaringan Wireless LAN (WLAN) Pada PT. PLN (Persero) Wilayah P2B Area Sorong Sonny Rumalutur," J. Teknol. dan Rekayasa, vol. 19, no. 3, pp. 48–60, 2014.

[3] A. Tsitroulis, D. Lampoudis, and E. Tsekleves, "Exposing WPA2 security protocol vulnerabilities," Int. J. Inf. Comput. Secur., vol. 6, no. 1, pp. 93–107, 2014.

[4] F. L. Aryeh, M. Asante, and A. E. Y. Danso, "Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT *," Ghana J. Technol., vol. 1, no. 1, pp. 40–45, 2016.

[5] brave a. sugiarso rahmat h.labatjo, arie s.m. lumenta, "Rancang Bangun Sistem Pengolahan Data Barang Berbasis Web Pada TokoFitber," E-Journal Tek. Elektro Dan Komput., vol. 4, no. 6, pp. 16–24, 2015.