Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Website : jurnal.ummu.ac.id/index.php/J-TIFA

J-TIFA

(Jurnal Teknologi Informatika)

|Teknologi Informasi | Jaringan Komputer | Data Mining |

Simulasi Protokol Authentikasi 802.1x Pada Jaringan Kabel Ummu

Sri Dantris Anhal[a], Junaidi Noh[b], Mustamin Hamid[c]
[abc]Informatika, Universitas Muhammadiyah Maluku Utara, Ternate, Indonesia
Email: dantrissri@gmail.com[a], junski576@gmail.com[b], hamidmustamin@gmail.com[c]

Abstrak

Teknologi yang semakin maju beriringi dengan muncul internet dengan interkoneksi bebasis *wireless* dan berbasis kabel (LAN). Namun dengan teknologi jaringan yang dirasakan sekarang terdapat kelemahan dalam infrastruktur jaringan tersebut. Tujuan yang ingin dicapai, penulis dalam penyusunan penelitian ini adalah mewujudkan keamanan jaringan kabel LAN agar lebih baik dan aman di Kampus UMMU. Hasil dalam penelitian ini adalah agar jaringan pada sistem keamanan di kampus UMMU tidak rentan dibobol dengan pihak-pihak yang tidak berwenang, oleh karena itu pada penelitian ini penulis ingin menerapkan metode protokol keamanan autentikasi 802.1x berbasis radius server. Dengan adanya protokol keamanan tersebut maka setiap pengguna yang terkoneksi ke jaringan kabel pada kampus UMMU melalui proses autentikasi sebelum terkoneksi ke jaringan kabel.

Kata Kunci : IEEE *802.1x, Network Infrastruktur, Keamanan Jaringan*

Abstract

Technology that is increasingly advanced is accompanied by the emergence of the internet with wireless-based and cable-based (LAN) interconnections. However, with today's perceived network technology, there are weaknesses in the network infrastructure. The goal to be achieved, the author in the preparation of this research is to realize the security of the LAN cable network to be better and safer on the UMMU Campus. The results in this study are that the network security system on the UMMU campus is not vulnerable to being breached by unauthorized parties, therefore in this study the author wants to apply the 802.1x authentication protocol method based on radius server. With this security protocol, every user connected to the wired network on the UMMU campus goes through an authentication process before connecting to the wired network..

Keywords: IEEE 802.1x, Network Infrastuctu, Network Security

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020 ISSN: 2654-2617 (Cetak)
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044 ISSN: 2654-2633(Online)

1. Pendahuluan

Di era yang sekarang ini perkembangan teknologi jaringan meningkat begitu pesat, hal ini di lihat pada era tahun 80 an jaringan komputer masi menjadi teka-teki yang ingin di jawab oleh para akademisi, dan pada tahun 1988 jaringan komputer mulai digunakan di universitas, perusahaan, sekarang memasuki era Millenial ini terutama *word wide* internet telah menjadi realitas sehari-hari jutaan manusia dimuka bumi ini. Berdasarkan hasil observasi pada sistem yang sedang berjalan pada kampus Universitas Muhammadiyah Maluku Utara (UMMU) menggunakan satu *internet Service provider* yaitu paket ISP Borero Net dan dua buah raouter serta dua switch terletak di ICT. Sistem yang sedang berjalan di Kampus UMMU menggunakan *Hotspot/Captive Portal*.

Captive Portal (Wireless) masi menggunakan tingkat keamanan WEP dan WPA, WEP (*Wired Equivalent Privacy*) sebagai *wireless security* nya dimana WEP masih menggunakan satu kunci enkripsi yang digunakan bersama-sama oleh para pengguna *wireless* LAN. Pengguna kunci WEP ini menyulitkan jika pengguna (user) harus berpindah dari satu hotspot ke hotspot lain, user tersebut harus merubah kunci WEP sesuai dengan titik hotspot yang digunakan. Dan karena lubang keamanan yang dimiliki WEP cukup banyak sehingga mudah dibobol oleh pihak ketiga yang tidak berhak, maka penggunaannya tidak disarankan. Sistem keamanan lainya adalah WPA (*WiFi Protected Access*), yang menggeser WEP dan menghasilkan keamanan yang lebih baik dari WEP. WPA bersifat meminta *Network Key* kepada setiap *wireless client* yang ingin melakukan koneksi ke jaringan (Tjaya Budi Santosa, 2008), oleh karena itu diperlukan penanganan dari berbagai serangan pada jaringan, salah satunya yaitu serangan *Mac Clone*. *Mac Clone* merupakan serangan pada mikrotik, dimana satu user dapat digunakan untuk login lebih dari satu user atau biasa di sebut duplikasi. Berdasarkan rujukan pada data yang telah didapat dalam satu bulan bisa terjadi serangan sampai tiga puluh kali bahkan bisa lebih dari itu Sistem keamanan jaringan yang menggunakan *Captive Portal* belum mendukung penanganan *Mac-Clone* oleh karena itu badan IEEE mengeluarkan protocol IEEE 802.1X pada jaringan kabel ataupun *Nirkabel*. 802.1X merupakan implementasi dari standard IEEE 802.1X. Fungsi utama dari protokol ini adalah (Uji Muryanto, 2011) untuk mengaktifkan fungsi *Network Access Control* pada koneksi kabel (*port-based*). Teknologi ini juga bisa disebut sebagai EAP *over* LAN (EAPOL) dan jika menggunakan *wireless* disebut *EAP Over Wlan* (EAPOW), pada implementasinya setiap perangkat yang ingin terkoneksi dengan standard 802.1X akan dibagi kedalam beberapa istilah yaitu *Supplicant*, *Authenticator, Authentication Server* (*Radius Server).*

Seperti yang telah dijelaskan diatas penelitian ini mencoba menggunakan protokol IEEE 802.1X yang dihubungkan dengan RADIUS sehingga diharapkan bisa melakukan konfigurasi dan maintenance *wireless network* dapat lebih aman kedepannya. Administrasi User dan Password juga dilakukan terpusat menggunakan RADIUS Server dan tingkat keamanannya lebih baik dari pada menggunakan WPA *Enterprise* yang ada di protokol IEEE 802.1X. Diharapkan hasil penelitian ini dapat meningkatkan *Quality Of Service* pada system jaringan di Universitas Muhammadiyah Maluku Utara (UMMU).

2. Landasan Teori

2.1. Prinsip Kerja Radius

RADIUS merupakan protocol *security* yang bekerja menggunakan system *clien-server* terdistribusi yang banyak digunakan Bersama AAA untuk mengamankan jaringan pengguna yang tidak berhak. RADIUS melakukan autentikasi *user* melalui serangkaian komunikasi antara *client-server.* Bila *user* berhasil melakukan autentikasi, maka *user* tersebut dapat menggunakan lanyanan yang disediakan oleh jaringan. (Lukman :06)

2.2. Standard Keamanan 802.11

RADIUS (*Remote Access Dial-in User Service*) merupakan suatu protokol *client-server* yang dikembangkan untuk mekanisme akses kontrol yang memeriksa dan mengautentikasi pengguna berdasarkan protokol Autentikasi, Autorisasi,

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Akutansi atau dikenal dengan protokol AAA (Deris Setiawan, 2008).

2.3. Server

Merupakan hati dari jaringan. Server biasanya merupakan computer berkecepatan tinggi dengan kapasitas memori (RAM) dan simpanan yang besar, dan dihubungkan dengan kartu jaringan yang cepat yang berkualitas tinggi. Sehingga server mampu beroprasi terus-menerus untuk melayani permintaan. (Wagito,2007:24).

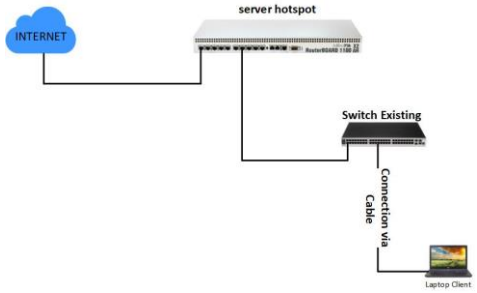
2.4. Protokol IEEE 802.1x

Keamanan merupakan hal yang sangat penting dalam jaringan wireless. Pada network *wireless*, IEEE mendukung standar 802.1X untuk meningkatkan keamanan transmisi data. *Portbased network access control* mengijinkan seorang *administrator network* untuk membatasi penggunaan IEEE 802 Lan *service access points* (ports) untuk mengamankan komunikasi antara peralatan yang sudah di otentikasi dan di otorisasi IEEE Std 802.1X menentukan suatu arsitektur, elemen fungsional dan protokol yang mendukung *mutual authentication* antar *client* yang menggunakan port yang terpasang pada LAN yang sama dan mengamankan komunikasi antar ports (Ichsan Wirata,2019)

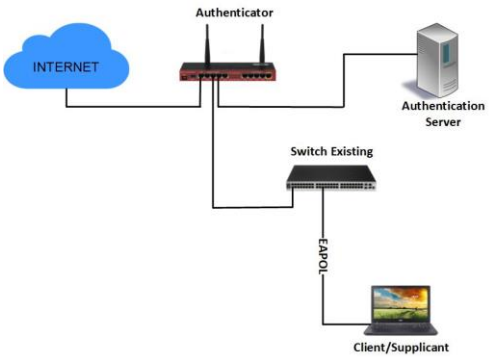
3. Analisis Dan Perancangan Sistem

Objek penelitian dari penulisan penelitian ini adalah pengembangan sistem keamanan jaringan kabel di Universitas Muhammadiyah Maluku Utara (UMMU) dengan menerapkan protokol otentikasi 802.1x diserver UMMU tepatnya di ICT. saat ini keamanan jaringan kabel Kampus UMMU masih menggunakan *Captive Portal,* dengan adanya protocol 802.1x memungkinkan proses otentikasi dilakukan secara terpusat.

Sistem Yang sedang berjalan pada Kampus UMMU dapat dilihat pada gambar 2. Pada Desain topologi, ada beberapa komponen yang di gunakan yaitu, ISP (Internet Service Provider), Router MikroTik, *Access Point, Switch*, dan *Client* yang terhubung melalui kabel. *Router* di sini digunakan sebagai server hotspot dan Juga sebagai koneksi internet melalui kabel, *Access point* digunakan sebagai pemancar signal *wireless* yang akan digunakan oleh *client*. Sedangkan switch digunakan sebagai koneksi via kabel oleh *client*.



Gambar 1 Sistem yang sedang berjalan saat ini



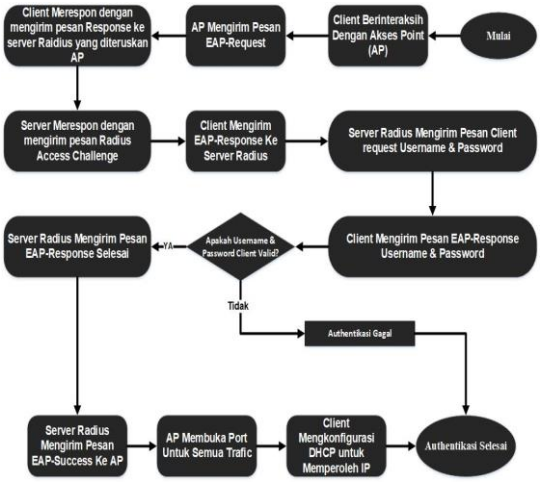
Gambar 2 Sistem yang diusulkan oleh penelitian ini.

Sedangkan Gambar 2 adalah sistem yang diusulkan pada penelitian ini. Sistem yang berjalan ini akan dilakukan simulasi pada Lab Networking Prodi Informatika. Adapun perangkat yang digunakan adalah Router MikroTik sebagai *Authenticator*, Komputer yang digunakan sebagai *Authentication Server*, *Access Point* (AP) Sebagai *Supplicant, Switch* Sebagai *Supplicant*, HP dan Laptop Sebagai *Supplicant*. Selanjutnya pada penelitian ini menggunakan skenario pengujian yang dapat dilihat pada gambar 3, jika *client* ingin terkoneksi dengan internet maka client akan ditahan

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

oleh AP dan berinteraksi terlebih dahulu, setelah itu AP akan mengirim pesan *EAP-Request* dan client akan merespon dengan mengirim pesan *response*/identitas AP dan AP akan meneruskan ke *Server Authentication*, setelah itu server akan merespon balik dengan memberikan pesan *RADIUS-Access-Challage*, jika *client* menerima maka *client* akan mengirim *EAP-Response Passtrought* ke server maka server mengirim pesan ke *client EAP-Request username* dan *password*, *client* mengirim pesan *EAP-Response* ke server username dan password, server akan cek di database jika username dan password tidak valid maka selesai, jika username dan password valid maka server mengirim pesan ke *EAP-Response Passtrought* Selesai, server mengirim pesan ke AP *EAP-Success*, Maka AP akan membuka Port untuk semua *traffic* dan *Client* akan Mendapatkan IP DHCP, Auhentikasipun selesai.



Gambar 3. Skenario Pengujian

Selanjunya beberapa kebutuhan perangkat yang digunakan pada penelitian ini berupa software Free Radius dan winbox sedangakan untuk hardware dapat dilihat pada table 1.

Tabel 1 Daftar Hardware

No	Hardware	Spesifikasi/Tipe	Jumlah
1	Authentikasi Server	• Enter Gaming E-Sports PRO • INTEL I5-10400F X AMD G • 16GB (2x8GB) Memori • Ethernet Gigabyte	1
2	Authentikator	• Router Board RB2011	1
3	Accsess Point	• Unifi AP AC Lite	1
4	Supplicant	• Smart Phone • Notebook	2

4. Implementasi Simulasi Protokol Aunthentifikasi 802.1X pada Jaringan Nirkabel

Pada penelitian ini akan dilakukan dilab networking dengan menjalankan radius server (*authentikasi server)* di lab jaringan dan router mikrotik yang akan menjadi bertugas sebagai *Authenticator* dan ada juga sebuah *client* (*Supplicant)* yang akan digunakan untuk menguji. Berikut tahapan-tahapan implementasi penelitian ini.

4.1. Instalasi Dan Konfigurasi FreeRadius

Tahap pertama yang harus dilakukan dalam server baru yaitu dengan memperbarui indeks paket server dan meningkatkan ke paket yang terbaru dengan perintah berikut.

```
$sudo apt update
$sudo apt upgrade
```

Setelah itu yang harus dilakukan berikutnya adalah melakukan instalasi LAMP Stack dengan menginstal apache terlebih dahulu dengan perintah berikut.

```
$sudo apt -y install apache2
```

Jika suda maka selanjutnya lakukan booting pada apache. Dan tahap berikutnya lakukan beberapa hal dibawah ini:

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

1. Melakukan Instalasi Modul tambahan pada apache yang diperlukan untuk freeradius
2. Pengecekan versi php, yang selanjutnya dilakuakn penginstalan mariadb yang akan digunakan sebagai dataset pada freeradius. Pada database lakukan penganturan kata sandi.
3. Melakukan konfigurasi freeradius dan mariadb dengan melakukan penginstalan freedius dan model tambahan freeradius.

```
$sudo apt -y install freeradius freeradius-mysql freeradius-utils –y
```

4. Membuat debug mode, dengan menggunakan perintah *$sudo freeradius-X*. jika sukses maka akan ditampilkan perintah sebagai berikut:

```
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
```

4.2. Instalasi dan Konfigurasi Daloradius

Daloradius adalah manajemen web radius, yang sudah di dukung dengan GUI agar lebih memudahkan administrator memanajemen pengguna. Berikut adalah proses instalasi DaloRadius dan mengintegrasi antara DaloRadius dan FreeRadius. Tahap pertama yang dilakukan adalah dengan menginstall **wget** dikarenakan tidak dinstall secara default setelah diinstall maka unzip file DaloRadius.

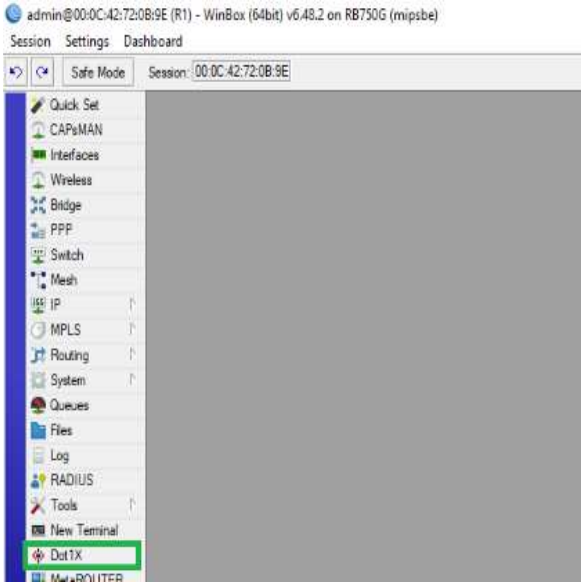
```
$sudo apt -y install wget unzip
$wget https://github.com/lirantal/daloradius/archive/master.zip
unzip master.zip
```

```
$cd daloradius-master
$sudo mysql -u root -p radius < contrib/db/fr2-mysql-daloradius-and-freeradius.sql
$sudo mysql -u root -p radius < contrib/db/mysql-daloradius.sql
```

file telah di unzip setelah itu select file daloradius agar bisa di akses ke directorynya dan lakukan import ke database radius yang sudah dibuat sebelumnya.

4.3. Konfigurasi 802.1x Di Router MikroTik

Setelah proses diatas dilakukan pada tahap selanjutnya adalah proses konfigurasi pada Router MikroTik Adapun konfigurasi tersebut akan dijelaskan dalam bentuk gambar dibawah. Pada gambar dibawah adalah awal masuk pada aplikasi WinBox, setelah itu masuk pada menu dot.1x yang telah ditandai dengan warna hijau pada gambar di bawah.

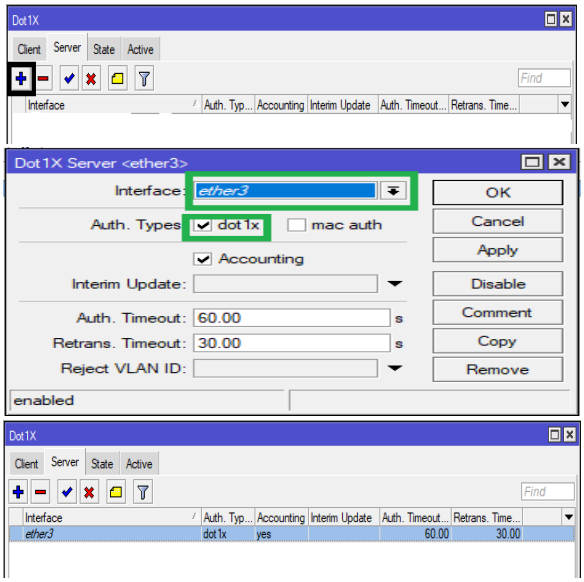


Gambar 4. Tampilan Router Utama

Apa bila sudah masuk pada Dot1X maka tahap sealanjutnya pindah pada tab server dan klik tanda tambah (+) untuk menambahkan Dot1x.

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

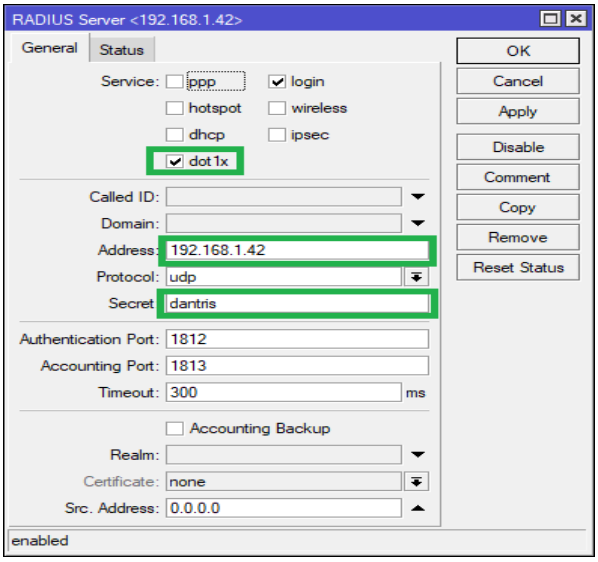
Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)



Gambar 5. Tampilan Dot1x Server

Jika sudah klik tanda tambah maka akan muncul jendela dot1X server. Pada kolom interfacenya dikarenakan pada penelitian ini proses authentikasinya akan diterapkan di ether3 maka interfacenya pilih ether3 dengan authentikasi types di centang dot1x setelah itu apply dan ok. Jika tahap diatas sudah dilakukan maka akan ada muncul tampilan seperti gambar diatas. Jika sudah maka keluar dari menu dot1x dan pindah ke tahap selanjutnya.

Setelah sudah selesai pada menu dot1x maka selanjutnya pindah ke menu RADIUS. Jika sudah masuk pada menu RADIUS maka selanjutnya klik tanda (+) untuk menambhakan radius sehingga menampilkan editor radius seperti pada gambar 6. pada kolom service dicentang dot1x agar saat freeradius tau jika service yang digunakan adalah dot1x, selanjutnya adalah kolom address di isi dengan ip address server freeradius, dikarenakan ip address freeradius mendapatkan ip DHCP Server maka ip tersebut di isi dengan 192.168.1.42. selanjutnya kolom secret diisikan dantris sesuaikan dengan secret yang dibuat difreeradius.



Gambar 6. Konfigurasi Radius Server

Jika cara diatas telah dilakukan maka akan muncul tampilan konfigurasi yang telah dibuat didalam tampilan RADIUS.

4.4. Verifikasi Sistem

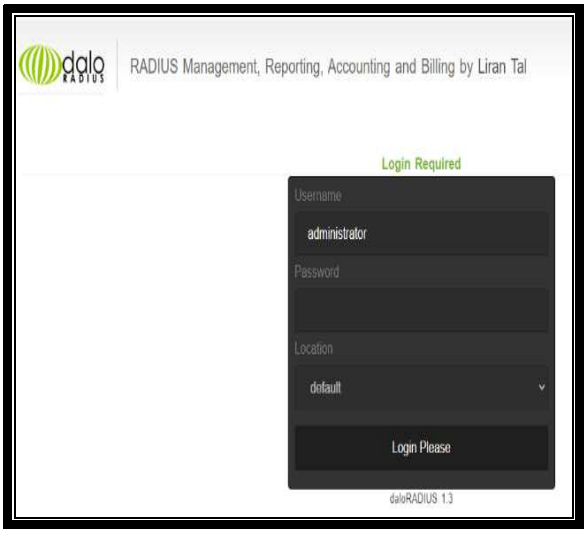
Verifikasi system dibutuhkan untuk menguji bahwa instalasi yang dilakukan diatas tidak terjadi masalah dan telah terintegrasi seluruhnya. Pada kali ini akan mencoba fungsional router, FreeRadius, dan DaloRadius.

4.5. Verifikasi Fungsional Daloradius

Cara menguji fungsional daloradius kali ini dengan mencoba mangakses ke via web dengan mengsikan ip address server sebagai contoh **http://server_ip_address/daloradius,** dikarenakan ip server dapat dhcp client 192.168.1.42 maka akses di web dengan http://192.168.1.42/daloradius jika sudah maka tampilan login daloradius akan muncul seperti gambar 7.

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

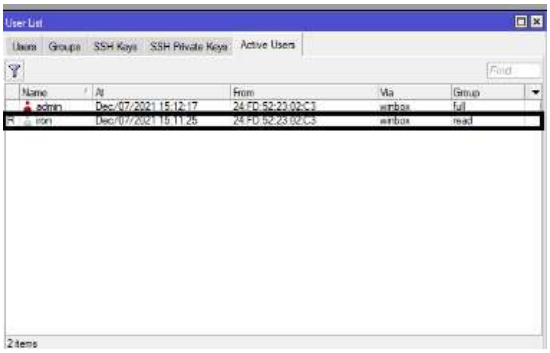
Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)



Gambar 7. Tampilan Login Daloradius

4.6. Verifikasi Fungsional 802.1x Router

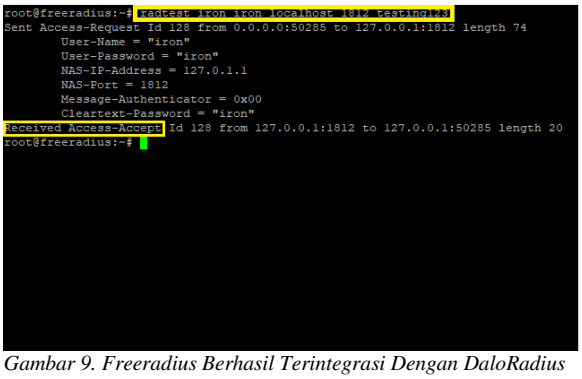
Untuk menguji fungsional dari Router adalah dengan membuka tab user pada tampilan Winbox dibawah. Dapat dilihat pada user **iron** telah tertambah secara otomatis pada tampilan user dirouter MikroTik dikarenakan daloradius telah berhasil diintegrasi dengan Router.



Gambar 8. Tampilan Terintegrasi Daloradius dengan Router

4.7. Verifikasi Fungsional FreeRadius

Pengujian fungsional FreeRadius sendiri akan dicoba dengan perintah **radtest** di server FreeRadius. Untuk pengujian akan dilakukan dengan format perintah **radtest {username} {password}**



Gambar 9. Freeradius Berhasil Terintegrasi Dengan DaloRadius

{hostname} 10 {radius_secret} Maksudnya adalah username dan password = (username yang sudah didaftarkan didaloradius sebelumnya), hostname = (server dintsall mana, dikarenakan pada penelitian ini menggunakan localhost maka isikan localhost), 10 = (port yang digunakan) pada penelitian ini port yang digunakan adalah 1812, radius_secret = (radius_secret terdapat pada file **client.conf**) pada penelitian ini radius_secret masi default yaitu *testing123*. Untuk lebih jelasnya bisa dilihat pada gambar dibawah.

5. Kesimpulan Dan Saran

Berdasarkan penelitian yang telah dilakukan, dari hasil simulasi protokol authentikasi 802.1x pada jaringan kabel, dengan menggunakan protokol IEEE 802.1x maka diperoleh kesimpulan bahwa simulasi dengan tingkat keamanan infrastuktur sistem pada jaringan kabel ini berhasil meningkatkan keamanan pada jaringan di lab networking ummu. Pada penelitian ini penulis belum melakukan simulasi standar protokol 802.1x dengan menggunakan via Nirkabel/Wireless, maka disarankan kepada pengembang dari penelitian ini, selanjutnya bisa diterapkan pada jaringan Nirkabel/Wireless.

Referensi

Andre Rizal Sinaga, Rakhmadhany Primananda, Primantara Hari Trisnawan. 2018 “Implementasi Authentikasi Mode Multi-Auth Pada Jaringan Local Area Network Berbasis Kabel Menggunakan Protocol IEEE 802.1X Dan Radius Server.

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)

Jurnal Teknologi Informatika (J-TIFA) V.3.No.2 September 2020
DOI: https://doi.org/10.52046/j-tifa.v3i2.1044
ISSN: 2654-2617 (Cetak)
ISSN: 2654-2633(Online)

Ichsan Wiratama, Putu Sugiartawan, September 2019. "Peningkatan Keamnan Wireless Pada Jaringan Komputer di Universitas Amikom Menggunakan Protokol IEEE802.1X"

D. Gibson, 20011 "MCITP Guide to Microsoft Windows Server 2008 Enterprise Administration" Citraweb Solusi Teknologi. 2019. "Implementasi Dot1X di MikroTik", https://citraweb.com/artikel_lihat.php?id=345 , Di Akses pada 10 Oktober 2019.

WikipediA 9 juni 2019. "Dasar Sistem Keamanan Komputer", https://id.wikipedia.org/wiki/ Di Akses pada 10 Oktober 2019.

Belajar Ngonfig, Fathurhoho, 4 November 2018 "Penjelasan TCP/IP Serta Enkapsulasinya", https://ngonfig.net/tcp-ip.html, Di Akses pada 10 Oktober 2019.

Qwords, Andy, 13 Januari 2020 "Mengenal Macam – Macam Topology Jaringan Komputer", https://qwords.com/blog/topologi-jaringan-komputer/, Di akses pada 8 Desember 2020.

Ardanisite, ARDANI, 20 Mei 2020 " Sistem Keamanan Jaringan Nirkabel / Wireless Lengkap", https://www.ardanisite.com/ nirkabel/Di Akses pada 8 Desember 2020.

Neliti, Mukhammad Andri Setiawan, Gesit Singgih Febyatmoko, 12 January 2006 "Sistem Autentikasi, Otorisasi, Dan Pelaporan Koneksi User Pada Jaringan Wireless Menggunakan Chillispot Dan Server Radius", https://www.neliti.com, Di akses pada 8 Desember 2020.

Rantri Anggraini.2016. "Definisi Authentication, Cara kerja dan Defini Enkripsi". http://rantrianggraini12.blogspot.com

Rexzax's Weblog. 2009. "Menegenal Protokol Keamanan AAA". https://rexzax.wordpress.com/

WikipediA 9 juni 2019. "Dasar Sistem Keamanan Komputer", https://id.wikipedia.org/wiki/Dasar_sistem_keamanan_komputer , Di Akses pada 10 Oktober 2019.

Yuliarti Swan. 2021. "Switch: Pengertian, Fungsi, Jenis dan Cara Kerjanya". https://tedas.id/teknologi/komputer/switch/.

Riwayat Artikel: Menerima(23 Juli 2020), Revisi (27 Juli 2020), Diterima (11 Agustus 2020), Online (3 September 2020)