Laman web jurnal: https://ejournal.unama.ac.id/index.php/processor

Jurnal Processor

P-ISSN: 1907-6738 | E-ISSN: 2528-0082

Perancangan Sistem Autentikasi Jaringan Nirkabel dan File Server menggunakan RADIUS dan WPA2-Enterprise

Tristanto Ari Aji[1*], Muhammad Kurniawan [2], Yudi Sutanto[3], Andika Agus Slameto[4], Ravenusa Arjuna Kristiary[5]

[1,2,3,4,5] Informatika Universitas AMIKOM Yogyakarta, Jl. Ringroad Utara Condongcatur Depok Sleman, Yogyakarta, 55598, Indonesia.
*Penulis Korespondensi, Email: tristanto.a@amikom.ac.id

Abstrak−Keamanan jaringan dan efisiensi merupakan aspek penting dalam pengelolaan infrastruktur jaringan, terutama pada jaringan nirkabel yang rawan terhadap berbagai bentuk serangan. Penelitian ini bertujuan merancang sistem autentikasi jaringan nirkabel dan *file server* yang lebih aman dan efisien dengan menggunakan protokol WPA2-Enterprise dan server RADIUS. Dalam rancangan ini, protokol WPA2-Enterprise digunakan untuk meningkatkan keamanan akses jaringan nirkabel dengan metode autentikasi berbasis identitas pengguna, bukan hanya sandi umum. Untuk meningkatkan efisiensi proses autentikasi menggunakan *server* RADIUS. *Server* RADIUS (*Remote Authentication Dial-In User Service*) berfungsi sebagai pusat autentikasi yang memverifikasi kredensial pengguna dari database yang telah ditentukan. Sistem pada penelitian ini mengintegrasikan autentikasi layanan *file server* dan autentikasi penggunaan jaringan nirkabel. Hasil pengujian menunjukkan bahwa rancangan ini berhasil memberikan otentikasi yang lebih aman, mencegah akses tidak sah, serta mempermudah pengelolaan pengguna dan hak akses. Penggunaan *server* RADIUS dan protokol WPA2-Enterprise memungkinkan fleksibilitas serta efisiensi penerapan sistem pada lingkungan kampus. Implementasi sistem ini dapat menjadi solusi praktis dalam meningkatkan keamanan dan efisiensi proses autentikasi jaringan nirkabel dan layanan *file server* internal.

Kata Kunci: Autentikasi; Jaringan Nirkabel; File Server; RADIUS; WPA2-Enterprise.

Abstract−Network security and efficiency are important aspects in managing network infrastructure, especially in wireless networks that are prone to various forms of attacks. This research aims to design a more secure and efficient wireless network and file server authentication system using the WPA2-Enterprise protocol and a RADIUS server. In this design, the WPA2-Enterprise protocol is used to improve the security of wireless network access with a user identity-based authentication method, not just a generic password. To improve the efficiency of the authentication process, a RADIUS server is used. The RADIUS (Remote Authentication Dial-In User Service) server functions as a centralised authentication centre that verifies user credentials from a predefined database. The system in this research integrates file server service authentication and wireless network usage authentication. Test results show that this design successfully provides more secure authentication, prevents unauthorised access, and simplifies user and access rights management. The use of a RADIUS server and the WPA2-Enterprise protocol allows for flexibility and efficiency in implementing the system in a campus environment. The implementation of this system can be a practical solution in improving the security and efficiency of the wireless network authentication process and internal file server services.

Keywords: Authentication; Wireless Network; File Server; RADIUS; WPA2-Enterprise.

1. PENDAHULUAN

Dalam perkembangan teknologi jaringan komputer, proses autentikasi pengguna sebelum menggunakan suatu layanan pada sebuah jaringan komputer merupakan aspek yang sangat penting. Salah satu mekanisme dalam pengelolaan keamanan jaringan komputer adalah proses autentikasi dan otorisasi user [1] . Beberapa contohnya adalah autentikasi sebelum melakukan akses jaringan *internet* menggunakan nirkabel (WIFI) dan autentikasi sebelum masuk ke dalam sebuah *file server*. Hal ini diperlukan dalam menjaga keamanan jaringan dan data dari beberapa ancaman serangan yang ada saat ini seperti *Man In The Middle*, *brute force* dan *eavesdropping* [2].

Penelitian ini dilakukan di sebuah kampus XYZ yang memiliki banyak ruang kelas dan laboratorium komputer. Pada saat proses belajar mengajar mahasiswa membutuhkan akses *internet* dan untuk dapat menggunakan akses *internet* di ruang kelas mengharuskan mahasiswa terhubung ke jaringan nirkabel. Proses autentikasi jaringan nirkabel saat ini dilakukan menggunakan metode *hotspot* pada mikrotik. Metode ini menggunakan *captive portal* untuk proses autentikasinya. Saat proses autentikasi komunikasi dengan router mikrotik menggunakan protokol *HyperText Transfer Protocol (HTTP)* sehingga *user* dan *password* dikirimkan dalam bentuk *plain text*, hal ini sangat mudah untuk dibajak[3]. Menurut hasil penelitian Michael dkk (2021) pada sistem *captive portal* dari 10 sampel yang diujikan semua sampel berhasil dibobol [4].

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted: 25 Oktober 2025; Published: 31 Oktober 2025

Proses belajar mengajar diawali dengan membagikan materi dan diakhiri dengan mengumpulkan tugas. Hal ini dapat dilakukan menggunakan beberapa layanan *cloud* melalui *internet*, akan tetapi jika *file* yang dibagikan memiliki ukuran yang besar dan pengguna yang banyak maka akan membebani jaringan *internet* yang menyebabkan akses layanan *cloud* melambat. Selain itu kapasitas penyimpanan di *cloud* juga sangat terbatas. Untuk mengatasi hal ini digunakan *file server* yang bersifat lokal, yang menyediakan kecepatan akses yang lebih baik dan kapasitas penyimpanan yang lebih besar [5]. Untuk dapat menggunakan *file server* ini dosen dan mahasiswa harus melakukan autentikasi terlebih dahulu.

Kondisi ini menimbulkan beberapa permasalahan, antara lain:

1. Pengguna harus menggunakan sistem autentikasi yang berbeda untuk dapat melakukan akses terhadap 2 layanan (akses *internet* melalui jaringan nirkabel dan akses *file server*), yang mengharuskan pengguna memiliki 2 kredensial yang berbeda. Hal ini menyebabkan manajemen kredesial yang tidak efisien baik dari sisi pengguna maupun sisi *administrator* jaringan.
2. Keamanan data yang lemah pada proses autentikasi karena tidak menerapkan protokol keamanan yang baik. Komunikasi antara pengguna dan *server* melalui jaringan komputer dapat dengan mudah disadap atau dimanipulasi oleh pihak tidak bertanggung jawab.

Untuk mengatasi permasalahan ini, diperlukan sistem yang menggunakan metode autentikasi yang lebih efektif dan dilengkapi mekanisme enkripsi [2]. Proses autentikasi dapat diatasi menggunakan satu database pengguna yang dikelola menggunakan RADIUS server. Sehingga proses autentikasi layanan jaringan nirkabel dan *file server* terpusat pada 1 database yang sama . RADIUS dapat menggunakan *Two Factor Authentication (2FA)* untuk login sehingga meningkatkan standar keamanan. Proses pengiriman data dapat diamankan dengan menerapkan protokol WPA2-Enterprise yang melakukan proses enkripsi data menggunakan algoritma *Advanced Encryption Standard (AES*), sehingga dapat menjamin kerahasiaan dalam proses pengiriman datanya [2].

RADIUS (*Remote Authentication Dial-In User Service*) adalah protokol jaringan yang dapat menangani Autentikasi (Authentication), Otorisasi (Authorization), dan Akuntansi (Acounting) pada jaringan.Radius server merupakan metode yang kuat untuk melindungi jaringan nirkabel [6]. RADIUS *server* menggunakan *Two Factor Authentication (2FA)* untuk login. Hanya user yang mempunyai *username* dan *password* yang benar yang diijinkan [7]. RADIUS server dapat melakukan autentikasi terpusat jika pengguna akan melakukan akses jaringan dan layanan lain, seperti *file server*. RADIUS menggunakan standar IEEE 802.1X yang digunakan dalam WPA2-*Enterprise*.

Menurut penelitian Kemas Ocha Khairi Saputra dkk, (2024) salah satu isu yang muncul pada keamanan berbasis WPA2-PSK user hanya diminta memasukan *password* pada saat melakukan autentikasi. Permasalahan yang dihadapi adalah dalam mengidentifikasi *user* yang mengakses jaringan [8]. Pada sistem yang menggunakan WPA-*Enterprise*, *user* diminta memasukan *username* dan *password* pada saat proses autentikasi. Sehingga WPA -*Enterprise* menyediakan metode autentikasi, otorisasi dan *enkripsi* yang lebih kuat daripada WPA-*Personal*. Metode ini digunakan pada jaringan nirkabel yang membutuhkan tingkat keamanan tinggi dan jumlah perangkat nirkabel yang dikelola cukup banyak. Menurut penelitian Diyar Waysi Naaman dkk (2020) penggunaan WPA2-Enterprise dan RADIUS *server* membuat jaringan lebih aman dari serangan jaringan [9]. Menurut penelitian Penggunaan WPA2 Enterprise dengan protokol PEAP (Protected EAP) memberikan keamanan transmisi data yang tinggi [10],[11] . Protokol WPA-Enterprise ini memiliki beberapa keunggulan yaitu;

1. Protokol ini memungkinkan penggunaan EAP (*Extensible Authentication Protocol)* sehingga memungkinkan pengguna memasukan nama pengguna dan kata sandi dalam melakukan authentikasi.
2. Setiap pengguna mempunyai kunci enkripsi yang unik sehingga meningkatkan keamanan semua perangkat yang terhubung.
3. Kemudahan dalam mengelola dan mengontrol *user* dan *password* pengguna karena semua terpusat pada 1 *database server*.
4. Memudahkan *administrator* dalam mengembangkan jaringan menjadi lebih besar karena protokol ini sudah didukung oleh sebagian besar perangkat jaringan yang ada saat ini serta tinggal mengarahkan proses autentikasi ke RADIUS *server* yang digunakan.

Menurut penelitian I. Fatihul Busyro dkk, (2023) Windows Server 2019 memiliki sistem *File Server Resource Manager* yang baik, yang dapat memudahkan admin *server* dalam mengontrol data yang masuk pada sebuah *server* [12]. Selain itu Windows Server 2019 juga memiliki *Network Policy Server* yang menjalankan RADIUS *server* untuk menangani proses autentikasi dan otorisasi user. Database user pada RADIUS server yang terdapat di Windows Server dapat digunakan juga untuk proses autentikasi dan otorisasi akses ke *file server* yang terdapat juga terdapat di Windows Server[13]. Sistem ini memungkinkan *administrator* untuk mengelola hak akses user, sehingga setiap pengguna hanya dapat mengakses file sesuai dengan izin yang diberikan. Oleh karena itu pada penelitian ini peneliti menggunakan Windows Server 2019 sebagai sistem operasi pada komputer server untuk menjalankan RADIUS *server* dan *file server*.

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

2. METODOLOGI PENELITIAN

Penelitian ini dimulai dengan menyusun tujuan dan kebutuhan apa saja yang akan digunakan. Tujuan dari penelitian ini adalah meningkatkan keamanan dan efisiensi proses autentikasi jaringan nirkabel dan *file server* pada sistem lama di kampus XYZ . Pada sistem lama proses autentikasi menggunakan 2 database yang berbeda, 1 database digunakan dalam proses autentikasi jaringan nirkabel dan 1 database lain digunakan dalam proses autentikasi *file server*. Pada sistem baru yang akan diteliti untuk menangani 2 proses auntentikasi hanya menggunakan 1 database. Kemudian dari sisi keamanan jaringan pada sistem lama tidak menerapkan protokol keamanan jaringan, pada sistem baru yang diteliti akan menggunakan protokol keamanan jaringan yang lebih baik. Solusi yang ditawarkan pada sistem yang baru yaitu mengimplementasikan RADIUS *server* sebagai metode autentikasi dan protokol WPA2-*Enterpise* untuk meningkatkan keamanan proses autentikasi pengguna.

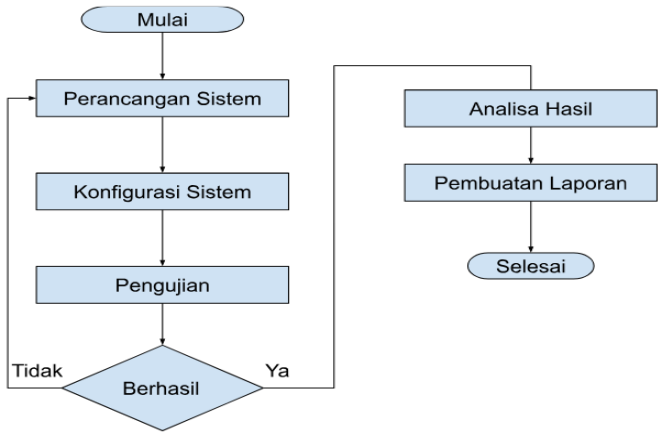
Pada penelitian ini kebutuhan perangkat yang akan digunakan yaitu 1 unit *server* sebagai *server* RADIUS dan *file server* menggunakan sistem operasi Windows Server 2019 , kemudian perangkat keras jaringan berupa kabel jaringan, *switch* , *access point* Unifi , 1 unit router mikrotik dan beberapa *Laptop/Handphone* sebagai *client*.

Selanjutnya peneliti membuat desain sistem yang akan dibuat termasuk desain topologi jaringan yang akan digunakan. Perangkat keras yang akan digunakan dalam penelitian ini terdiri dari 1 server menggunakan Windows *Server* yang berfungsi sebagai *file server* dan RADIUS *server*, 1 buah router yang menghubungkan jaringan lokal ke *internet*, 1 buah *switch* yang menghubungkan semua perangkat jaringan (*router , server, personal computer* dan access pointt), 2 unit *laptop* yang menggunakan Sistem Operasi Windows dan macOS, dan *smartphone* juga menggunakan Sistem Operasi Windows dan macOS yang berfungsi sebagai client.

Langkah berikutnya peneliti membangun jaringan komputer sesuai dengan topologi jaringan yang sudah dibuat sebelumnya dan memastikan semua perangkat saling terhubung jaringan dengan baik. Langkah selanjutnya yaitu melakukan konfigurasi di Windows *Server* agar dapat berfungsi sebagai *file server* dan RADIUS *server* pada saat yang bersamaan. Setelah *server* siap maka selanjutnya melakukan konfigurasi di access pointt Unifi agar dapat melakukan proses autentikasi pengguna melalui RADIUS *server*. Protokol yang digunakan adalah WPA2-Enterprise.

Untuk memastikan tujuan penelitian tercapai maka perlu dilakukan pengujian. Pengujian ini bertujuan untuk memastikan bahwa implementasi RADIUS *server* dan WPA2-Enterprise dapat meningkatkan keamanan dan efisiensi dalam proses autentikasi jaringan nirkabel dan *file server*. Pengujian dilakukan dalam beberapa langkah. Pertama dilakukan pengukuran tingkat keberhasilan proses autentikasi masuk ke jaringan nirkabel menggunakan *user* yang sudah terdaftar di RADIUS *server*. Pengujian ini dilakukan menggunakan beberapa jenis sistem operasi menggunakan *laptop* dan *smartphone* untuk memastikan tingkat kompatibilitasnya. Kedua dilakukan pengukuran tingkat keberhasilan proses autentikasi ke *file server* menggunakan *user* yang sudah terdaftar di RADIUS *server*. Apakah *user* berhasil masuk atau tidak dan memeriksa hak akses terhadap *folder* dan *file* apakah sesuai dengan yang sudah dikonfigurasi pada masing-masing *user*. Ketiga dilakukan pengetesan tingkat keamanan pada jaringan nirkabel menggunakan *aircrack-ng*.

Langkah langkah pengujian dicatat dan hasilnya dianalisis untuk menentukan tingkat keberhasilan penelitian ini. Jumlah pengujian ditentukan berdasarkan tingkat kesulitan skenario pengujian dan ketersediaan sumber daya. Setelah selesai melakukan pengujian, hasil pengujian divalidasi dengan membandingkan dengan hasil yang diharapkan, jika hasil peneltian sesuai dengan harapan maka dapat disimpulkan bahwa Perancangan Sistem Autentikasi Jaringan nirkabel dan *file server* menggunakan RADIUS dan WPA2 *Enterprise* pada Kampus XYZ dinyatakan berhasil. Pada gambar 1 menunjukan alur penelitian yang peneliti gunakan dalam penelitian ini.



https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

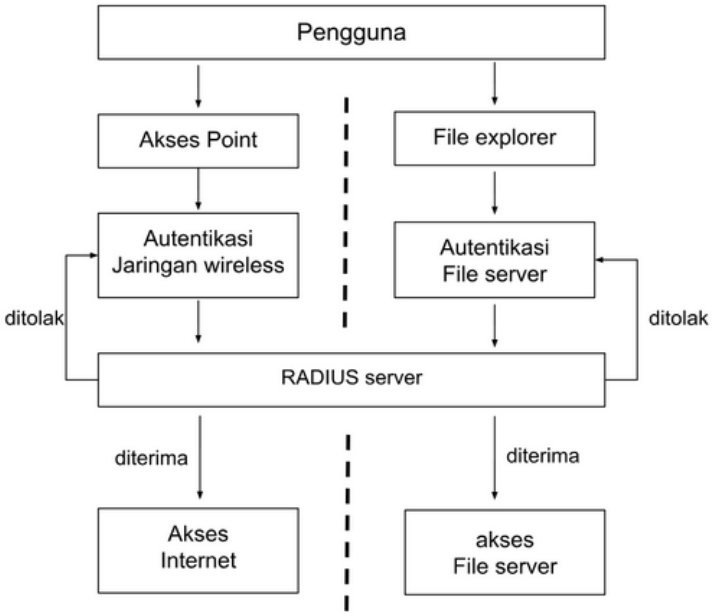
Gambar 1. Alur Penelitian

3. HASIL DAN PEMBAHASAN

Pada bagian ini peneliti melakukan perancang sistem yang akan membahas alur proses yang akan berjalan pada Sistem Autentikasi Jaringan nirkabel dan *file server* menggunakan RADIUS dan WPA2 Enterprise. Selanjutnya peneliti merancang topologi fisik jaringan yang akan digunkan pada penelitian ini. Terakhir peneiti membuat rancangan pengujian yang memaparkan beberapa skenario dan uji kasus yang akan digunakan memvalidasi apakah Sistem Autentikasi Jaringan nirkabel dan *file server* menggunakan RADIUS dan WPA2 Enterprise dapat meningkatkan keamanan dan efisiensi proses autentikasi penggunaan jaringan komputer dari sistem sebelumnya.

3.1 Rancangan Sistem

Sistem autentikasi baik jaringan *nirkabel* maupun *file server* dirancang menggunakan RADIUS server sebagai *validator*. Baik proses autentikasi pengguna melaluai access point maupun *file server* akan bertanya ke RADIUS *server* apakah sebuah *user* diterima atau tidak. Jika *user* valid maka akan diijinkan masuk dan jika tidak maka harus melakukan proses *autentikasi* kembali seperti ditunjukan pada gambar 2.



Gambar 2. Rancangan Sistem

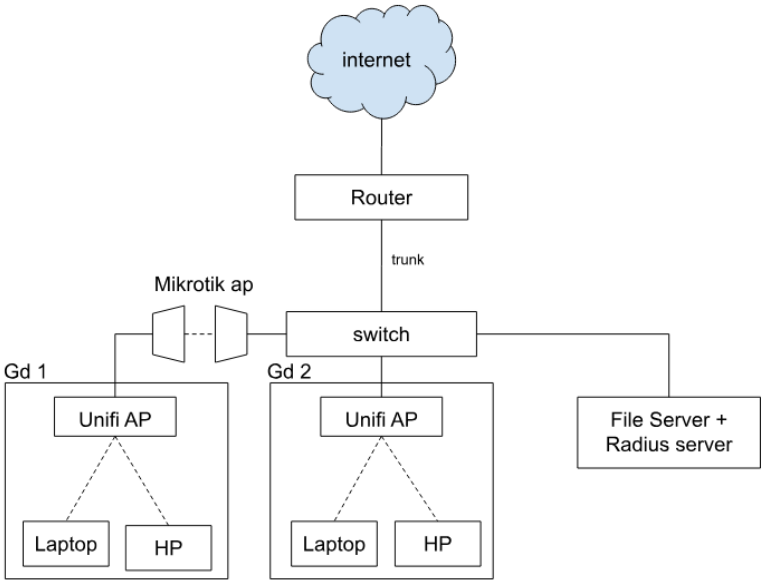
Rancangan folder pada *file server* dikelompokan menjadi 2 tipe yaitu *folder* materi dan *folder* tugas. Perbedaan authorisasinya adalah sebagai berikut:

1. Folder materi berfungsi untuk membagikan materi yang akan dipergunakan untuk perkuliahan. Dosen akan memiliki *sub folder* sendiri-sendiri kemudian mempunyai hak akses penuh terhadap *sub folder* masing-masing. *User* mahasiswa hanya mempunyai hak akses membaca saja disemua folder materi dan sub folder dosen.
2. Folder tugas berfungsi untuk mengumpulkan tugas yang sudah dikerjakan oleh mahasiswa . Dosen akan memiliki *sub folder* sendiri sendiri kemudian mempunyai hak akses penuh terhadap *sub folder* masing masing. Mahasiswa hanya memiliki hak akses bisa menyalin (*copy*) file tugas yang sudah selesai ke *sub folder* dosen kemudian mahasiswa tidak dapat merubah, menduplikasi atau membuka *file* yang telah dikumpulkan. Hal ini untuk mencegah plagiasi tugas dan secara tidak sengaja menghapus tugas mahasiswa lain.

3.2 Rancangan Topologi Jaringan

Topologi yang digunakan adalah terdapat 1 router mikrotik yang terhubung ke swicth . Swicth kemudian membagi jaringan ke File server dan Radius Server dan menuju ke akses point yang ada dilingkungan laboratorium seperti ditunjukan pada gambar 3. Jaringan ini menggunakan *VLAN* untuk meningkatkan kinerja dan keamanan [14].

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025



Gambar 3. Rancangan Topologi Jaringan

3.3 Rancangan Pengujian

Rancangan pengujian dilakukan untuk mengevaluasi proses autentikasi dan keamanan dari implementasi sistem *autentikasi* jaringan nirkabel dan *file server* menggunakan RADIUS *server*. Pengujian ini terdiri dari beberapa skenario dan uji kasus untuk memvalidasi apakah sistem dapat bekerja seperti yang diharapkan. Rancangan pengujian yang akan dilakukan seperti dibawah ini :

1. Pengujian proses autentikasi jaringan *nirkabel* yang dilakukan dengan cara sebagai berikut:
   a. Pengujian *client laptop* menggunakan sistem operasi Windows dan mac OS yang diukur adalah lama waktu proses autentikasi dan tingkat keberhasilannya.
   b. Pengujian keberhasilan *client smartphone* menggunakan sistem operasi Android dan macOS yang diukur adalah lama waktu proses autentikasi dan tingkat keberhasilannya.
2. Pengujian keberhasilan proses *autentikasi* user dosen dan mahasiswa masuk kedalam *file server*, *yang* diukur adalah adalah lama waktu proses autentikasi dan tingkat keberhasilannya.
3. Pengujian keamanan *nirkabel* dilakukan dengan cara mencoba membobol proses autentikasi jaringan *nirkabel* menggunakan *aircrack-ng*. Di antara berbagai alat penetration testing *aircrack-ng* adalah salah satu yang paling populer karena kemampuannya dalam monitoring jaringan, mengumpulkan paket data, menangkap handshake, dan cracking kata sandi [15].

3.4 Implementasi

Pada bagian ini peneliti melakukan proses implementasi dari rancangan yang sudah dibuat sebelumnya. Yang pertama adalah membangun jaringan sesuai dengan rancangan topologi jaringan yang sudah dibuat. Selanjutnya peneliti melakukan konfigurasi pada RADIUS *server* dan File *server* agar bisa sesuai dengan rancangan. Terakhir dilakukan proses pengujian sistem dengan beberapa skenario yang sudah direncanakan.

3.4.1 Membangun Jaringan

Peneliti membangun jaringan sesuai dengan rancangan topologi yang sudah dibuat. Untuk menghubungkan antar perangkat menggunakan kabel *Unshielded Twisted Pair (UTP) Cat 6*. Setelah itu melakukan konfigurasi *ip address* pada semua perangkat. Proses selanjutnya yaitu melakukan konfigurasi *VLAN* pada *router* dan *switch*. Terakhir memastikan bahwa semua perangkat telah terhubung ke jaringan dengan baik .

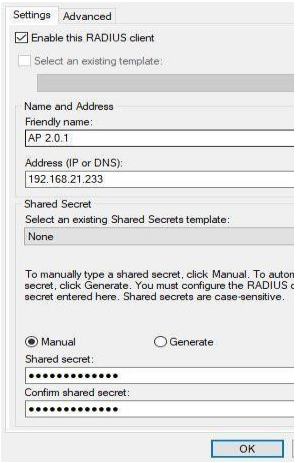
3.4.2 Konfigurasi RADIUS Server

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

Pada penelitian ini peneliti menggunakan Windows Server 2019 sebagai RADIUS *server*. Langkah pertama yang dilakukan adalah melakukan instalasi *Role Network Policy and Access Service* . Konfigurasi dapat dilakukan melalui *Server Manager* pada bagian *Add Roles and Features*.

3.4.2.1 Konfigurasi RADIUS Client dalam NPS

Setelah *role Network Policy and Access Service* terinstal, selanjutnya adalah proses menambahkan RADIUS *client*. Proses penambahan *client* ini dilakukan dengan menambahkan *ip access point* yang ada. Konfigurasi dapat dilakukan pada bagian *Network Policy Server*. Pada bagian *RADIUS Clients and Server*, peneliti memasukan *ip access point* yang akan menjadi RADIUS *client*. *Properties* yang peneliti konfigurasi mulai dari nama *ip address* dan *shared secret* yang telah di buat pada perangkat *access point* seperti pada gambar 4 dibawah ini .



Gambar 4. RADIUS Client *Properties*

3.4.2.2 Konfigurasi Network Policy pada Klien Nirkabel (*Wireless Client)*

Setelah *access point client* Unifi ditambahkan, proses selanjutnya adalah membuat *policy* untuk *wireless client*. *Policy* adalah aturan atau kebijakan yang berfungsi untuk menentukan apakah *client* dapat terkoneksi, siapa saja, dan kapan mereka dapat terkoneksi. Pada penelitian ini, peneliti mengambil daftar *database client* dari *Windows Group* yang sudah ada.

Pada menu *Condition* peneliti ini ingin mengambil data *condition* agar sesuai dengan *data user*, maka menggunakan *windows group* pada parameter ini. Pada menu *Constraints*, di bagian *Authentication Method* adalah konfigurasi enkripsi apa yang akan digunakan saat *wireless client*. Peneliti menggunakan EAP *default* yang digunakan adalah Microsoft: *Protected* EAP (PEAP). Kemudian untuk menu *less secure authentication method* peneliti menggunakan MS-CHAP-v2. Pada bagian PEAP, peneliti menggunakan *certificate* yang di *generate* melalui *cmd* dengan perintah berikut ini :

new-selfsignedcertificate -dnsname "FQDN server anda" -KeyLength 2048 -CertStoreLocation cert:LocalMachineMy -NotAfter (Get-Date).AddYears(20)

3.4.2.3 Manajemen user

Peneliti memasukan beberapa *user* baru melalui *Server Manager* pada bagian *Computer Management*. Pada bagian *User* yang terdapat pada *Local Users and Group* peneliti membuat beberapa *username* dosen dan mahasiswa yang akan digunakan pada penelitian. *Username* dan *password* sementara wajib diisi. Untuk meningkatkan keamanan *password* peneliti mengaktifkan *user must change password*.

Untuk memudahkan pengelompokan *user* peneliti membuat 2 grup yaitu grup dosen dan mahasiswa. Grup ini akan memiliki otorisasi yang berbeda sesuai kebijakan yang ada di rancangan sistem.

3.4.2.4 Konfigurasi *Access Point* menggunakan Unifi Controller

Konfigurasi dilakukan menggunakan Unifi Controler pada menu *Wireless Networks*. Untuk menggunakan RADIUS, peneliti melakukan konfigurasi keamanan protokol menggunakan WPA2-*Enterprise*.

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

3.4.2.5 Konfigurasi RADIUS Profile Unifi Controller

RADIUS Profile digunakan oleh Access Point untuk menyimpan konfigurasi konfigurasi nama profile, *ip address windows server* yang akan digunakan sebagai *server* RADIUS, *password/shared secret* autentikasi yang akan digunakan pada saat akan memasukan *access point* ke dalam RADIUS *client* dan *default port* untuk autentikasinya yaitu 1812. Pada menu *RADIUS Accounting Server* digunakan untuk menyimpan *log autentikasi RADIUS*, pada penelitian ini menggunakan *ip address* yang sama dengan *server* RADIUS dan *port default* yaitu 1813.

3.4.3 Konfigurasi *File Server*

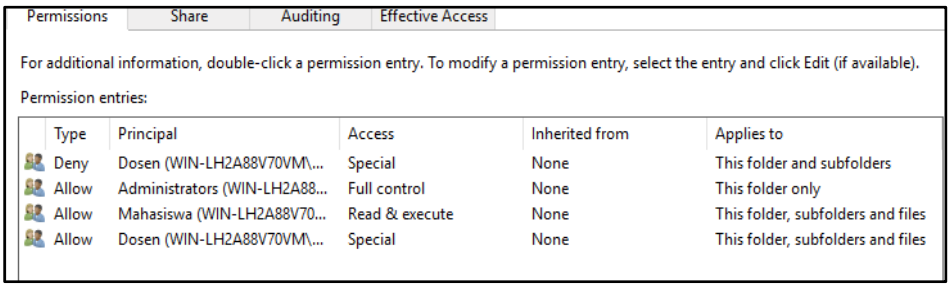
Agar user dapat menggunakan file server maka harus ada folder dan file yang dishare untuk user tersebut. Untuk penelitian ini peneliti membuat *folder* materi yang berisi beberapa *sub folder* dosen dan folder tugas menggunakan *windows explorer* . *Folder* materi dan tugas harus merupakan folder utama bukan sub folder agar konfigurasi *policy* bisa berjalan dengan baik. Konfigurasi kebijakan *folder* dilakukan didalam *properties* pada bagian *security*.

3.4.3.1 Konfigurasi Kebijakan *Folder* Materi

Konfigurasi kebijakan hak akses yang diberikan pada folder materi agar sesuai dengan rancangan adalah sebagai berikut :

1. Melarang user didalam grup Dosen membuat serta menghapus file dan sub folder yang ada di dalam folder Materi.
2. Mengijinkan user Administrator melakukan semua kebijakan yang ada (*full control*).
3. Mengijinkan user dalam grup Mahasiswa hanya dapat melihat dan membaca file.
4. Mengijinkan user dalam grup Dosen untuk dapat membuat, menghapus file dan sub folder didalam sub folder dosen yang terdapat didalam folder materi.
5.

Tampilan kebijakan *folder* materi di Windows Server seperti pada gambar 5.

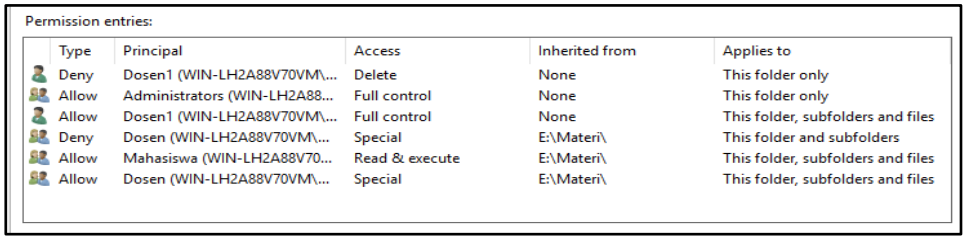


Gambar 5. Konfigurasi kebijakan hak akses *folder* materi

Di dalam *folder* materi terdapat *sub folder* masing-masing dosen. Konfigurasi kebijakan hak akses harus dilakukan di masing-masing *sub folder* Dosen *x* harus khusus dengan user Dosen *x*. Pada *sub folder* masing masing dosen didalam folder materi dilakukan konfigurasi kebijakan hak akses sebagai berikut :

1. Melarang user Dosen *x* menghapus sub folder dosen *x*.
2. Mengijinkan user Administrator melakukan semua kebijakan hak akses (*full control*)
3. Mengijinkan user Dosen *x* melakukan semua kebijakan hak akses (*full control*) di dalam sub folder dosen *x*.

Kebijakan sub folder Dosen 1 di Windows Server dapat dilihat pada gambar 6.



https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

Gambar 6. Konfigurasi kebijakan hak akses sub folder masing masing dosen

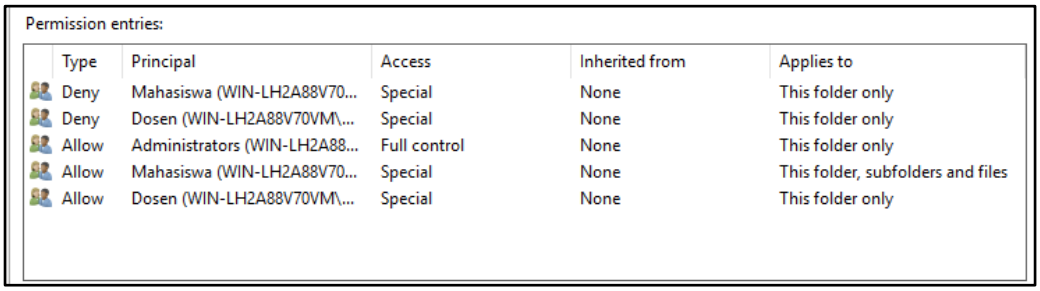
Pada gambar 6 terdapat kebijakan hak akses nomer 4, 5 dan 6 ini merupakan kebijakan hak akses turunan yang di dapat dari konfigurasi kebijakan hak akses yang dikonfigurasi di *folder* materi.

3.4.3.2 Konfigurasi *Folder* Tugas

Konfigurasi kebijakan hak akses yang diberikan pada folder tugas agar sesuai dengan rancangan adalah sebagai berikut :

1. Melarang user dalam grup Mahasiswa membuat serta menghapus *file*, *folder* dan *subfolder* didalam *folder* tugas.
2. Melarang user dalam grup Dosen membuat serta menghapus file, folder dan subfolder didalam *folder* tugas.
3. Mengijinkan user Administrator melakukan semua kebijakan hak akses (*full control*)
4. Mengijinkan user dalam grup Mahasiswa melihat *list file*, membuat *file*, membuat *folder*, menuliskan *attributes* dan menuliskan *extended attributes*.
5. Mengijinkan user dalam grup Dosen melihat list file, membaca attributes, membaca *extended attribute*, menulis attributes, menuliskan *extended attributes*, membaca, merubah permissions dan merubah kepemilikan suatu file.

Kebijakan folder tugas di Windows Server dapat dilihat pada gambar 7.

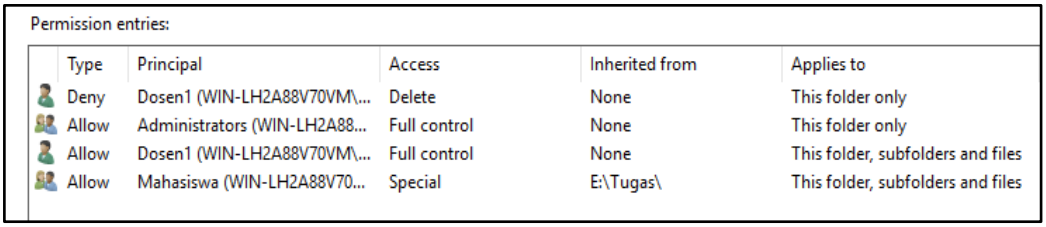


Gambar 7. Konfigurasi kebijkan hak akses folder tugas

Di dalam *folder* tugas terdapat *sub folder* tugas masing-masing dosen. Konfigurasi kebijakan hak akses pada *sub folder* Tugas Dosen *x* harus khusus user Dosen *x*. Pada *sub folder* masing masing dosen didalam *folder* tugas dilakukan konfigurasi kebijakan hak akses sebagai berikut :

1. Melarang user Dosen *x* menghapus sub folder Tugas Dosen *x*.
2. Mengijinkan user Administrator melakukan semua kebijakan hak akses (*full control*)
3. Mengijinkan user Dosen *x* melakukan semua kebijakan hak akses (*full control*) di dalam sub folder Tugas Dosen *x* .
4. Terdapat kebijakan user grup Mahasiswa turunan dari konfigurasi kebijakan hak akses dari folder Tugas.
5.

Kebijakan hak akses folder Tugas Dosen 1 di Windows Server dapat dilihat pada gambar 8.



Gambar 8. Konfigurasi kebijakan hak akses sub folder Tugas Dosen 1

3.5 Pengujian

Tujuan pengujian ini adalah untuk memastikan bahwa sistem autentikasi jaringan nirkabel dan *file server* dapat bekerja di beberapa tipe perangkat dan sistem operasi yang berbeda. Perangkat yang dipergunakaan pada pengujian penelitian ini adalah sebagai berikut:

1. Layanan yang akan diintegrasikan proses autentikasinya adalah layanan autentikasi jaringan *nirkabel* dan *file server*.

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

2. Menggunakan *access point* merk Unify.
3. Metode autentikasi yang diteliti menggunakan WPA2-Enterprise.
4. *Server* autentikasi yang digunakan adalah RADIUS Server.
5. File *server* yang digunakan adalah Windows Server 2019
6. Spesifikasi Server yang digunakan AMD Ryzen 7 8 core, Memory 32 Gb, HDD 1 TB
7. Jumlah client yang digunakan untuk pengujian 20 unit (10 unit laptop dan 10 unit smart phone).

3.5.1 Pengujian autentikasi jaringan nirkabel.

Langkah-langkah pengujian autentikasi jaringan nirkabel adalah sebagai berikut:

a. Pengujian keberhasilan autentikasi jaringan nirkabel pada *laptop* dengan sistem operasi Windows dan macOS.
    1. Pengujian pada *laptop* dengan sistem operasi windows dilakukan dengan cara menghubungkan perangkat ke jaringan nirkabel kampus. Selanjutnya mencoba masuk menggunakan *user* dan *password* sesuai yang terdaftar di *server* RADIUS. Selain itu juga dilakukan ujicoba masuk menggunakan *user* dan *password* yang tidak terdaftar di *server* RADIUS. Pengujian dilakukan pada 5 perangkat. Peneliti memeriksa lama waktu yang diperlukan untuk proses autentikasi, tingkat keberhasilan *user* terdaftar dan kegagalan *user* yang tidak terdaftar di *server* RADIUS dalam mengakses jaringan nirkabel. Untuk waktu proses autentikasi user yang tidak terdaftar yang diukur ialah lama waktu yang dibutuhkan sistem untuk memberitahu jika proses autentikasi gagal.
    2. Pengujian pada *laptop* dengan sistem operasi mac OS dilakukan dengan cara menghubungkan perangkat ke jaringan nirkabel kampus. Selanjutnya mencoba masuk menggunakan *user* dan *password* sesuai yang terdaftar di *server* RADIUS. Selain itu juga dilakukan ujicoba masuk menggunakan *user* dan *password* yang tidak terdaftar di *server* RADIUS. Pengujian dilakukan pada 5 perangkat. Peneliti memeriksa lama waktu yang diperlukan untuk proses autentikasi, tingkat keberhasilan *user* terdaftar dan kegagalan *user* yang tidak terdaftar di *server* RADIUS dalam mengakses jaringan nirkabel. Untuk waktu proses autentikasi user yang tidak terdaftar yang diukur ialah lama waktu yang dibutuhkan sistem untuk memberitahu jika proses autentikasi gagal.

b. Pengujian keberhasilan smartphone menggunakan sistem operasi Android dan macOS.
    1. Pengujian pada *smartphone* dengan sistem operasi android . dilakukan dengan cara menghubungkan perangkat ke jaringan nirkabel kampus. Selanjutnya mencoba masuk menggunakan *user* dan *password* sesuai yang terdaftar di *server* RADIUS. Selain itu juga dilakukan ujicoba masuk menggunakan *user* dan *password* yang tidak terdaftar di *server* RADIUS. Pengujian dilakukan pada 5 perangkat. Peneliti memeriksa lama waktu yang diperlukan untuk proses autentikasi, tingkat keberhasilan *user* terdaftar dan kegagalan *user* yang tidak terdaftar di *server* RADIUS dalam mengakses jaringan nirkabel. Untuk waktu proses autentikasi user yang tidak terdaftar yang diukur ialah lama waktu yang dibutuhkan sistem untuk memberitahu jika proses autentikasi gagal.
    2. Pengujian pada *smartphone* dengan sistem operasi macOS dilakukan dengan cara menghubungkan perangkat ke jaringan nirkabel kampus. Selanjutnya mencoba masuk menggunakan *user* dan *password* sesuai yang terdaftar di *server* RADIUS. Selain itu juga dilakukan ujicoba masuk menggunakan *user* dan *password* yang tidak terdaftar di *server* RADIUS. Pengujian dilakukan pada 5 perangkat. Peneliti memeriksa lama waktu yang diperlukan untuk proses autentikasi, tingkat keberhasilan *user* terdaftar dan kegagalan *user* yang tidak terdaftar di *server* RADIUS dalam mengakses jaringan nirkabel. Untuk waktu proses autentikasi user yang tidak terdaftar yang diukur ialah lama waktu yang dibutuhkan sistem untuk memberitahu jika proses autentikasi gagal.

Tabel 1. Hasil Pengujian Autentikasi

No	Perangkat Diuji	Rata-Rata Lama Proses Autentikasi	Tingkat Berhasil Proses Autentikasi Jaringan Nirkabel
1	**Laptop Windows**		
	User terdaftar	1,6 detik	100 % berhasil
	User tidak terdaftar	1,8 detik	100% gagal
2	**Laptop Mac OS**		
	User terdaftar	1,7 detik	100 % berhasil
	User tidak terdaftar	1,6 detik	100% gagal

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

3	**Smartphone Android**		
	User terdaftar	1,5 detik	100 % berhasil
	User tidak terdaftar	1,7 detik	100% gagal
4	**Smartphone MacOS**		
	User terdaftar	1,8 detik	100 % berhasil
	User tidak terdaftar	1,7 detik	100% gagal

Pada tabel 1 menunjukan hasil pengujian autentikasi pada semua perangkat menggunakan user yang terdaftar di server Radius memiliki tingkat keberhasilan 100 % dengan waktu yang dibutuhkan untuk proses autentikasi < 2 detik. Kemudian hasil pengujian menggunakan user yang tidak terdaftar di server Radius menunjukan tingkat kegagalan 100% dengan waktu proses autentikasi < 2 detik .

3.5.2 Pengujian autentikasi *file server*.

Pengujian keberhasilan *login user* dosen untuk mengakses *file server*. Akses dilakukan melalui *file explorer* yang ada pada 5 perangkat sistem operasi Windows dan 5 perangkat dengan sistem operasi macOS.

a. Pengujian user dosen.
   Peneliti melakukan ujicoba login menggunakan 2 *user* dosen yang terdaftar di *server* RADIUS dan 2 user dosen yang tidak terdaftar di server RADIUS. Ujicoba dilakukan pada sub folder dosen yang ada di folder materi dan sub folder dosen yang ada di folder tugas. Kemudian dicatat lama waktu proses autentikasinya dan tingkat keberhasilannya.
b. Pengujian user mahasiswa.
   Peneliti melakukan ujicoba login menggunakan 2 user mahasiswa yang terdaftar di server RADIUS dan 2 user mahasiswa yang tidak terdaftar di server RADIUS. Ujicoba dilakukan pada *sub folder* dosen yang ada di *folder* materi dan *sub folder* dosen yang ada di folder tugas. Kemudian dicatat . Kemudian dicatat lama waktu proses autentikasinya dan tingkat keberhasilannya.

Tabel 2. Hasil pengujian autentikasi *file server*

No	User yang diuji	Rata-Rata Lama Proses Autentikasi	Tingkat Berhasil Proses Autentikasi File Server
1	Dosen terdaftar	1,5 detik	100 % berhasil
2	Dosen tidak terdaftar	1,7 detik	100% gagal
3	Mahasiswa terdaftar	1,6 detik	100 % berhasil
4	Mahasiswa tidak terdaftar	1,7 detik	100% gagal

Pada tabel 2 hasil pengujian autentikasi *file server* pada semua *user* yang terdaftar di server Radius menggunakan perangkat Windows maupun Mac memiliki tingkat keberhasilan 100% dan rata rata lama proses autentikasi < 2 detik. Kemudian hasil pengujian user yang tidak terdaftar di server Radius menggunakan perangkat Windows maupun Mac OS memiliki tingkat kegagalan 100% dengan rata rata lama proses proses autentikasi < 2 detik.

3.5.3 Pengujian keamanan jaringan nirkabel

Pengujian pada penelitian ini dilakukan menggunakan *aircrack-ng*. Pengujian dilakukan sebanyak 5 kali uji coba pembajakan *password*.

Tabel 3. Hasil pengujian keamanan nirkabel

No	Ujicoba	Hasil	Keterangan
1	Ujicoba pembajakan 1	Gagal	Gagal menagkap handsahake
2	Ujicoba pembajakan 2	Gagal	Gagal menagkap handsahake

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

3	Ujicoba pembajakan 3	Gagal	Gagal menagkap handsahake
4	Ujicoba pembajakan 4	Gagal	Gagal memecahkan password
5	Ujicoba pembajakan 5	Gagal	Gagal menagkap handsahake

Pada tabel 3 hasil pengujian pembajakan *password* menggunakan *aircrack-ng* sebagian besar mengalamai kegagalan pada saat proses menangkap *handshake*, tetapi terdapat 1 yang berhasil menangkap proses *handshake* akan tetapi gagal pada saat proses memecahkan kode password. Hal ini dapat disimpulkan proses pembajakan menggunakan *aircrack-ng* 100% gagal.

4. KESIMPULAN

Setelah pengujian yang dilakukan terhadap sistem autentikasi jaringan nirkabel dan *file server* menggunakan RADIUS server dan WPA2-*Enterprise* mendapatkan beberapa hasil yaitu, hasil pengujian proses autentikasi jaringan nirkabel pada semua perangkat menggunakan user yang terdaftar di Radius *server* memiliki tingkat keberhasilan 100 % dengan waktu yang dibutuhkan untuk proses autentikasi < 2 detik. Kemudian hasil pengujian proses autentikasi menggunakaan user yang tidak terdaftar di Radius *server* menunjukan tingkat kegagalan 100% dengan waktu proses autentikasi < 2 detik.

Hasil pengujian autentikasi *file server* pada semua *user* yang terdaftar di server Radius menggunakan perangkat Windows maupun Mac memiliki tingkat keberhasilan 100% dan rata rata lama proses autentikasi < 2 detik. Kemudian hasil pengujian user yang tidak terdaftar di server Radius menggunakan perangkat Windows maupun Mac memiliki tingkat kegagalan 100% dengam rata rata lama proses proses autentikasi < 2 detik. Hasil pengujian pembajakan *password* menggunakan *aircrack-ng* sebagian besar mengalamai kegagalan pada saat proses menangkap *handshake*, tetapi terdapat 1 yang berhasil menangkap proses *handshake* akan tetapi gagal pada saat proses memecahkan kode passwordnya . Hal ini dapat disimpulkan proses pembajakan menggunakan *aircrack-ng* 100% gagal.

Dari beberapa hasil pengujian yang telah dilakukan maka peneliti mengambil kesimpulan implementasi Sistem Autentikasi Jaringan Nirkabel dan *File Server* menggunakan RADIUS dan WPA2-*Enterprise* berhasil dan sesuai dengan tujuan penelitian yaitu berhasil meningkatkan keamanan dan efisiensi proses autentikasi jaringan nirkabel dan *file server* di lingkungan kampus XYZ .

Sistem Autentikasi Jaringan Nirkabel dan *File Server* menggunakan RADIUS dan WPA2-*Enterprise* pada penelitian ini memiliki masih memiliki beberapa keterbatasan. Pertama metode autentikasi cadangan perlu disiapkan sebagai antisipasi apabila Radius *server* utama mengalami gangguan. Pemilihan *password* dan *key* tetap harus memiliki kompleksitas yang tinggi dan panjang yang sesuai dengan standar keamanan. Pada penelitian ini *Server* RADIUS dan *file server* masih dalam 1 mesin yang sama, akan lebih baik jika Radius *server* dan *File server* terdapat pada 2 perangkat *server* yang berbeda. Pada penelitian ini belum menggunakan SSL yang valid akan lebih baik jika menggunakan sertifikat SSL yang valid yang terverifikasi oleh otoriras sertifikat terpercaya untuk meningkatkan keamanan proses *autentikas*i dan *enkripsi*. Yang terakhir perlu dipersiapkan spesifikasi server yang lebih handal untuk menangani jumlah user yang lebih banyak.

DAFTAR PUSTAKA

[1] E. Dolan and R. Widayanti, "Implementation of Authentication Systems on Hotspot Network Users to Improve Computer Network Security," *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 88–94, Mar. 2022, doi: 10.34306/ijcitsm.v2i1.93.

[2] T. H. Hadi, "Types of Attacks in Wireless Communication Networks," *Webology*, vol. 19, no. 1, pp. 718–728, Jan. 2022, doi: 10.14704/web/v19i1/web19051.

[3] Z. M. Luthfansa and U. D. Rosiani, "Pemanfaatan Wireshark untuk Sniffing Komunikasi Data Berprotokol HTTP pada Jaringan Internet," *Journal Information Engineering and Educational Technology*, vol. 5, no. 1, pp. 34–39, Jun. 2021, doi: 10.26740/jieet.v5n1.

[4] Michael, I. Ruslianto, and R. Hidayati, "Analisis Perbandingan Sistem Keamanan Jaringan WI-FI Protected Access 2-Pre Shared Key (WPA2-PSK) dan Captive Portal pada Jaringan Publik Wireless," *Coding : Jurnal Komputer dan Aplikasi*, vol. 09, no. 1, pp. 108–118, 2021, doi: 10.26418/coding.v9i01.45902.

[5] A. G. Gani and N. Permadi, "Sistem Administrasi Jaringan menggunakan Windows Server 2008," *Jurnal Sistem Informasi*, vol. 7, no. 1, pp. 1–22, Feb. 2020, doi: 10.35968/jsi.v7i1.378.

[6] C. A. Ochoa Villanueva and A. Roman-Gonzalez, "Implementation of a RADIUS server for access control through authentication in wireless networks," *International Journal of Advanced and Applied Sciences*, vol. 10, no. 3, pp. 183–188, Mar. 2023, doi: 10.21833/ijaas.2023.03.022.

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025

[7] A. D. Yudhistira and R. Harwahyu, “Implementation Strategy Analysis of Network Security using dalo RADIUS and Pi-hole DNS Server to enhance Computer Network Security, Case Study: XYZ as a Fintech Company,” *Jurnal Indonesia Sosial Teknologi*, vol. 5, no. 10, pp. 4364–4379, Oct. 2024, doi: 10.59141/jist.v5i10.5321.

[8] K. O. K. S. Kemas, A. R. Supriyatna, and S. D. Putra, “Autentikasi User Dengan Metode Single Sign-On Berbasis Windows Active Directory Pada PT. XYZ,” *ROUTERS: Jurnal Sistem dan Teknologi Informasi*, pp. 70–78, Jan. 2024, doi: 10.25181/rt.v2i2.3328.

[9] D. Naman, M. Abdulwahab, and A. Ibrahim, “RADIUS Authentication on Unifi Enterprise System Controller using Zero-Handoff Roaming in Wireless Communication,” *Journal of Applied Science and Technology Trends*, vol. 1, no. 2, pp. 118–124, Aug. 2020, doi: 10.38094/jastt1427.

[10] S. Syafii, M. Tahir, M. Dani, N. Maulidya, and N. Widad Haqiqi, “Jurnal Restikom : Riset Teknik Informatika dan Komputer Perancangan Sistem Keamanan Jaringan Nirkabel dengan WPA2 Enterprise,” vol. 7, no. 1, pp. 74–86, Apr. 2025, doi: 10.52005/restikom.v71.415.

[11] S. B. Hegde, A. Ranjan, A. Raj, K. Paul, and S. Santra, “WPA2 Based Wireless Enterprise Configuration,” in *2021 IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2021*, Institute of Electrical and Electronics Engineers Inc., 2021. doi: 10.1109/ICMNWC52512.2021.9688387.

[12] I. Fatihul Busyro, H. Umam, and A. Eko Musantono, “Implementasi Fitur File Server Resource Manager Pada Sistem Operasi Windows Server,” 2023. Accessed: May 16, 2025. [Online]. Available: https://jurnal.akd.ac.id/index.php/assembly/article/view/31/9

[13] “Network Policy Server overview.” Accessed: Oct. 24, 2025. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top

[14] N. Umah, F. A. Yudanto, and E. Rilvani, “Evaluasi Segmentasi VLAN dalam Optimalisasi Kinerja dan Keamanan pada Jaringan LAN di Universitas Pelita Bangsa,” *Jurnal Ilmu Komputer dan Informatika*, vol. 8, no. 1, pp. 38–47, Jan. 2025, doi: 10.47324/ilkominfo.v8i1.313.

[15] F. Anam and F. Fachri, “Evaluasi Kerentanan Keamanan Jaringan Nirkabel Menggunakan Metode Penetration Testing dengan Aircrack-NG,” *Rabit : Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 10, no. 1, pp. 1–8, Jan. 2025, doi: 10.36341/rabit.v10i1.5387.

https://doi.org/10.33998/processor.2025.20.2.2531
Submitted: 25 Agustus 2025; Reviewed Round-1: 12 September 2025; Reviewed Round-2; 16 Oktober 2025; Accepted; 28 Oktober 2025; Published: 31 Oktober 2025