EXPERT JURNAL MANAJEMEN SISTEM INFORMASI DAN TEKNOLOGI

Analisis Keamanan WLAN pada Kantor Pemerintah Menggunakan Penetration Testing

Muhammad Asghar Nazal[1*], **Noven Jonathan Tigau**[2], **Mingsep Rante Sampebua**[3]
[1,2,3] Jurusan/Program Studi Sistem Informasi, Fakultas MIPA, Universitas Cenderawasih, Jayapura, Indonesia
[1*] asghar.nazalm@gmail.com, [2] novenjtigau@gmail.com, [3] mingsep75@gmail.com

ABSTRACT – A common problem with internet access is data leaks or disruption of network access, due to a lack of awareness among network technicians regarding network security systems. This study aims to analyze the security of Wireless LAN networks at the Papua Province Ministry of Religious Affairs Office using the Penetration Testing method. This method is used to identify security vulnerabilities through two types of attacks, namely Man In the Middle Attack and Bypassing MAC Authentication. Testing was carried out using the Kali Linux operating system in a virtualization loop using Oracle VirtualBox. The results of the study indicate that the Man In the Middle attack was successful in blocking internet access for the target device without being detected, while the Bypassing MAC Authentication attack was not successful but resulted in abnormal conditions on the network. This study provides an evaluation of the existing network security system and suggests the implementation of mitigations such as the use of WPA2-Enterprise with 802.1X, static ARP binding, DHCP snooping, client isolation, and the implementation of an IDS/IPS system to improve overall network security.

Keywords: Kali Linux; Penetration Testing; MAC Spoofing; MITM; Network Security; Wireless LAN.

ABSTRAK – Masalah yang sering terjadi terhadap penggunaan akses internet adalah terjadinya kebocoran data atau terganggunya akses jaringan, karena kurangnya kesadaran dari teknisi jaringan terhadap sistem keamanan jaringan. Penelitian ini bertujuan untuk menganalisis keamanan jaringan *Wireless* LAN di Kantor Kementerian Agama Provinsi Papua dengan menggunakan metode *Penetration Testing*. Metode ini digunakan untuk mengidentifikasi celah keamanan melalui dua jenis serangan, yaitu *Man In the Middle Attack* dan *Bypassing* MAC *Authentication*. Pengujian dilakukan dengan memanfaatkan sistem operasi Kali Linux dalam lingkungan virtualisasi menggunakan Oracle VirtualBox. Hasil penelitian menunjukkan bahwa serangan *Man In the Middle* berhasil dilakukan dengan memblokir akses internet perangkat target tanpa terdeteksi, sedangkan serangan *Bypassing* MAC *Authentication* tidak berhasil namun menghasilkan kondisi abnormal pada jaringan. Penelitian ini memberikan evaluasi terhadap sistem keamanan jaringan yang ada dan menyarankan penerapan mitigasi seperti penggunaan WPA2- Enterprise dengan 802.1X, *static* ARP *binding*, DHCP *snooping*, *client isolation*, serta implementasi sistem IDS/IPS untuk meningkatkan keamanan jaringan secara menyeluruh.

Kata Kunci: Keamanan jaringan; Kali Linux; MITM; MAC Spoofing; Penetration Testing; Wireless LAN.

1. PENDAHULUAN

Pemanfaatan jaringan *Wireless Local Area Network* (WLAN) pada instansi pemerintahan terus meningkat karena mendukung mobilitas kerja, efisiensi instalasi, dan kemudahan akses internet. Namun, penggunaan jaringan nirkabel juga meningkatkan risiko keamanan seperti penyadapan data, akses ilegal, *spoofing*, dan gangguan layanan jaringan. Kerentanan tersebut umumnya terjadi akibat lemahnya konfigurasi keamanan maupun kurang optimalnya mekanisme pengawasan jaringan.

Kantor Kementerian Agama Provinsi Papua merupakan salah satu instansi yang menggunakan jaringan WLAN untuk mendukung aktivitas operasional kantor. Berdasarkan hasil observasi dan wawancara, jaringan yang digunakan belum pernah dilakukan pengujian keamanan secara khusus menggunakan metode *Penetration Testing*. Kondisi ini menyebabkan tingkat kerentanan jaringan terhadap serangan siber belum diketahui secara pasti, padahal jaringan digunakan untuk mendukung pertukaran data dan akses layanan internal instansi.

Beberapa penelitian sebelumnya menunjukkan bahwa metode penetration testing efektif digunakan untuk mengidentifikasi celah keamanan jaringan. Penelitian Dwi Sabdho dan Maria menyatakan bahwa simulasi serangan pada jaringan WLAN mampu memperlihatkan kelemahan konfigurasi keamanan jaringan [1]. Penelitian Hasibuan dan Elhanafi menunjukkan bahwa metode MAC *filtering* masih memiliki kelemahan terhadap teknik MAC *spoofing* [2]. Selain itu, penelitian Auliafitri dkk. membuktikan bahwa serangan *Man in the Middle* (MITM) dapat dimanfaatkan untuk melakukan intersepsi lalu lintas data pada jaringan yang tidak memiliki proteksi ARP yang baik [3]. Namun, sebagian besar penelitian tersebut dilakukan pada lingkungan simulasi laboratorium dan belum banyak diterapkan pada jaringan instansi pemerintahan secara langsung.

Berdasarkan kondisi tersebut, penelitian ini dilakukan untuk menganalisis keamanan jaringan WLAN

pada Kantor Kementerian Agama Provinsi Papua menggunakan metode penetration testing melalui dua skenario serangan, yaitu *Bypassing* MAC *Authentication* dan *Man in the Middle Attack*. Berbeda dengan penelitian sebelumnya yang umumnya menggunakan lingkungan laboratorium atau jaringan simulasi, penelitian ini melakukan pengujian langsung pada jaringan operasional Kantor Kementerian Agama Provinsi Papua. Jaringan yang diuji menggunakan topologi *star* dengan satu router, dua switch, dan sepuluh *access point*, serta telah menerapkan *firewall* MikroTik dan autentikasi *hotspot login* (*Captive Portal*). Kondisi tersebut menjadi dasar untuk mengevaluasi sejauh mana mekanisme keamanan yang diterapkan mampu menghadapi serangan *Man in the Middle* dan *Bypassing MAC Authentication* pada lingkungan nyata.

Adapun pertanyaan penelitian dalam penelitian ini adalah bagaimana tingkat keamanan jaringan WLAN pada Kantor Kementerian Agama Provinsi Papua terhadap serangan *Bypassing* MAC *Authentication* dan *Man in the Middle Attack*, serta bagaimana metode penetration testing dapat digunakan untuk mengidentifikasi kerentanan keamanan jaringan tersebut.

2. DASAR TEORI

Penelitian mengenai keamanan jaringan *Wireless Local Area Network* (WLAN) telah banyak dilakukan, khususnya terkait pengujian kerentanan menggunakan metode *penetration testing*. Metode ini digunakan untuk mengidentifikasi kelemahan sistem keamanan jaringan melalui simulasi serangan yang menyerupai kondisi nyata. Pada penelitian ini, fokus pengujian dilakukan terhadap jaringan WLAN menggunakan dua teknik serangan yaitu *Man in the Middle Attack* (MITM) dan *Bypassing* MAC *Authentication* [4].

Menurut penelitian yang dilakukan oleh Dwi Sabdho dan Maria, penetration testing merupakan serangkaian aktivitas untuk mengidentifikasi serta mengeksploitasi kerentanan keamanan pada jaringan komputer sehingga dapat diketahui tingkat keamanan jaringan yang digunakan [1]. Pendekatan ini dinilai efektif karena mampu memberikan gambaran nyata mengenai potensi ancaman yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

Jaringan Wireless LAN dipilih sebagai objek penelitian karena teknologi ini banyak digunakan pada instansi maupun perusahaan akibat kemudahan instalasi, fleksibilitas, serta efisiensi biaya operasional. Namun demikian, jaringan nirkabel memiliki risiko keamanan yang lebih tinggi dibanding jaringan kabel karena media transmisinya menggunakan gelombang radio yang dapat diakses dari berbagai arah. Menurut Saharuna dan Nur, WLAN memiliki kelemahan pada aspek keamanan apabila tidak didukung dengan mekanisme autentikasi dan pengamanan yang baik [5].

Konsep keamanan jaringan sendiri merupakan mekanisme perlindungan terhadap sistem jaringan untuk menjaga kerahasiaan, integritas, dan ketersediaan data dari ancaman serangan. Amarudin menyatakan bahwa banyak gangguan jaringan terjadi akibat kelalaian pengelola jaringan dalam menerapkan sistem keamanan yang memadai sehingga membuka peluang bagi penyerang untuk melakukan eksploitasi terhadap jaringan komputer [6]. Oleh karena itu, evaluasi keamanan jaringan perlu dilakukan secara berkala untuk mengetahui kelemahan sistem yang masih dapat dimanfaatkan.

Salah satu serangan yang sering digunakan dalam pengujian keamanan jaringan adalah *Man in the Middle Attack* (MITM). Serangan ini dilakukan dengan menempatkan penyerang di antara komunikasi dua perangkat sehingga penyerang dapat memantau, memanipulasi, bahkan memutus komunikasi data tanpa diketahui pengguna. Menurut Auliafitri dkk., serangan MITM memungkinkan penyerang melakukan intersepsi lalu lintas jaringan dan memperoleh informasi penting dari korban [3]. Dalam penelitian ini, serangan MITM dilakukan menggunakan tools Ettercap Graphical dan Evil Limiter untuk melakukan ARP *poisoning* serta memblokir akses internet target.

Selain MITM, penelitian ini juga menggunakan teknik *Bypassing* MAC *Authentication*. Teknik ini bertujuan untuk menguji apakah sistem keamanan jaringan masih mengandalkan MAC *filtering* sebagai mekanisme autentikasi utama. Hasibuan dan Elhanafi menjelaskan bahwa MAC *Authentication Bypass* dilakukan dengan cara meniru alamat MAC perangkat yang telah terdaftar agar dapat memperoleh akses ke jaringan target [2]. Pengujian dilakukan menggunakan *tools* Airodump-ng, Wireshark, dan Macchanger untuk menangkap lalu lintas jaringan serta melakukan MAC *spoofing*.

Dalam implementasi pengujian, penelitian ini memanfaatkan sistem operasi Kali Linux sebagai platform utama karena menyediakan berbagai tools keamanan jaringan yang lengkap untuk kebutuhan *penetration testing*. Menurut Eka Pratama dan Wiradarma, Kali Linux merupakan distribusi Linux yang dirancang khusus untuk pengujian keamanan sistem komputer dan analisis kerentanan jaringan [7]. Sistem operasi tersebut dijalankan melalui Oracle VM VirtualBox sehingga pengujian dapat dilakukan tanpa mengubah sistem operasi utama perangkat penelitian [8].

Selain itu, penelitian ini juga menggunakan Wireshark sebagai alat analisis paket data jaringan. Wireshark berfungsi untuk menangkap dan menganalisis lalu lintas jaringan secara detail sehingga mempermudah proses identifikasi perangkat target maupun aktivitas komunikasi pada jaringan WLAN [9].

Berdasarkan beberapa penelitian dan literatur sebelumnya, dapat disimpulkan bahwa keamanan jaringan WLAN masih memiliki berbagai celah yang dapat dimanfaatkan melalui teknik serangan tertentu apabila sistem keamanan tidak dikonfigurasi secara optimal. Oleh karena itu, penelitian ini dilakukan untuk menganalisis tingkat keamanan jaringan WLAN pada Kantor Kementerian Agama Provinsi Papua menggunakan metode *penetration testing* sebagai dasar evaluasi dan rekomendasi peningkatan keamanan jaringan.

DOI http://dx.doi.org/10.36448/expert.v16i1.4917
e-ISSN 2745-7265 p-ISSN 2088-5555 EXPERT Vol. 16 No. 1
June 30, 2026 – Hal. 123

3. METODOLOGI

Penelitian ini menggunakan metode *Penetration Testing* untuk menganalisis tingkat keamanan jaringan *Wireless Local Area Network* (WLAN) pada Kantor Kementerian Agama Provinsi Papua. Metode ini digunakan untuk mengidentifikasi kerentanan sistem keamanan jaringan dengan mensimulasikan serangan yang umum terjadi pada jaringan nirkabel, sehingga dapat diketahui kelemahan sistem dan rekomendasi mitigasi yang sesuai.

Desain penelitian yang digunakan adalah penelitian deskriptif dengan pendekatan eksperimental. Penelitian dilakukan melalui proses observasi langsung terhadap infrastruktur jaringan WLAN yang sedang digunakan, kemudian dilakukan pengujian keamanan menggunakan metode *Penetration Testing*. Pengujian dilakukan pada jaringan internal kantor dengan izin dan pengawasan pihak instansi terkait untuk memastikan keamanan serta menghindari gangguan terhadap operasional jaringan.

Lokasi penelitian dilakukan di Kantor Kementerian Agama Provinsi Papua yang beralamat di Jalan Raya Abepura, Entrop, Distrik Jayapura Selatan, Kota Jayapura, Papua. Objek penelitian berupa jaringan WLAN yang digunakan sebagai media akses internet pegawai dan perangkat jaringan yang terdiri dari *Router*, *Switch*, dan beberapa *Access Point*.

Teknik pengumpulan data dalam penelitian ini dilakukan melalui wawancara, observasi, dan pengujian langsung. Wawancara dilakukan dengan tenaga IT pada Kantor Kementerian Agama Provinsi Papua untuk memperoleh informasi mengenai topologi jaringan, sistem keamanan yang digunakan, serta mekanisme pengelolaan jaringan. Observasi dilakukan dengan mengamati perangkat jaringan dan kondisi infrastruktur WLAN secara langsung. Selanjutnya dilakukan pengujian penetrasi untuk mengetahui kemungkinan celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

Tahapan penelitian dimulai dari proses identifikasi kebutuhan perangkat keras dan perangkat lunak yang digunakan dalam pengujian. Perangkat keras yang digunakan berupa laptop dan *Wireless Adapter* dengan spesifikasi*TP-Link TL-WN725N v2* yang mendukung *Monitor Mode* dan *Packet Injection* untuk pengujian *WLAN*, sedangkan perangkat lunak yang digunakan meliputi sistem operasi Kali Linux, Oracle VM VirtualBox, Wireshark, Ettercap Graphical, Evil Limiter, Airodump-ng, dan Macchanger. Kali Linux dijalankan menggunakan teknologi virtualisasi melalui Oracle VM VirtualBox untuk mempermudah implementasi pengujian tanpa mengganti sistem operasi utama perangkat penelitian.

Metode pengujian yang digunakan dalam penelitian ini terdiri dari dua jenis serangan yaitu *Man in the Middle Attack* dan *Bypassing* MAC *Authentication*. Pada pengujian *Bypassing* MAC *Authentication*, tahapan pertama dilakukan dengan mengidentifikasi jaringan target menggunakan tools Airodump-ng untuk memperoleh informasi BSSID, *channel*, dan perangkat yang telah terhubung pada jaringan. Setelah mendapatkan alamat MAC perangkat yang sah, dilakukan proses MAC *spoofing* menggunakan Macchanger untuk mencoba menyamarkan identitas perangkat penguji agar menyerupai perangkat target. Tahap terakhir adalah melakukan percobaan koneksi terhadap jaringan yang menggunakan sistem MAC *filtering*.

Pada pengujian *Man in the Middle Attack* (MITM), penelitian dilakukan menggunakan tools Ettercap Graphical dan Evil Limiter. Ettercap digunakan untuk melakukan *host scanning* dan ARP *poisoning* terhadap perangkat target yang berada dalam jaringan WLAN yang sama. Setelah target berhasil diidentifikasi, Evil Limiter digunakan untuk melakukan pembatasan atau pemutusan akses internet pada perangkat target guna membuktikan keberhasilan serangan MITM terhadap jaringan. Pengujian dilakukan dengan memonitor perubahan koneksi jaringan pada perangkat target sebelum dan sesudah serangan dijalankan.

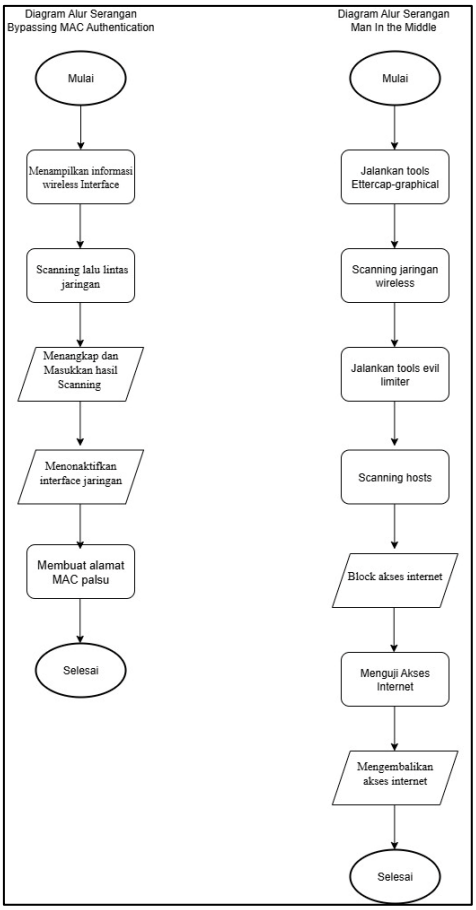
Teknik analisis data dilakukan secara deskriptif berdasarkan hasil pengujian yang diperoleh selama proses *Penetration Testing*. Hasil pengujian dianalisis untuk mengetahui tingkat keberhasilan serangan, bentuk kerentanan yang ditemukan, serta dampak yang ditimbulkan terhadap keamanan jaringan WLAN. Selain itu dilakukan analisis terhadap mekanisme keamanan yang telah diterapkan oleh instansi, kemudian disusun rekomendasi mitigasi keamanan seperti penerapan WPA2-Enterprise dengan autentikasi 802.1X, *static* ARP *binding*, DHCP *snooping*, *client isolation*, serta implementasi IDS/IPS guna meningkatkan keamanan jaringan secara menyeluruh.

Penelitian ini dilaksanakan setelah memperoleh izin dari pihak Kantor Kementerian Agama Provinsi Papua sebagai lokasi penelitian. Seluruh proses pengujian penetration testing dilakukan dengan sepengetahuan dan persetujuan pihak instansi serta hanya dilakukan pada jaringan yang telah ditentukan sebagai objek penelitian. Pengujian bertujuan untuk mengidentifikasi potensi kerentanan keamanan jaringan tanpa mengubah konfigurasi permanen, merusak sistem, maupun mengakses data yang bersifat rahasia. Seluruh hasil pengujian digunakan hanya untuk kepentingan akademik dan penyusunan rekomendasi peningkatan keamanan jaringan.

4. HASIL DAN PEMBAHASAN

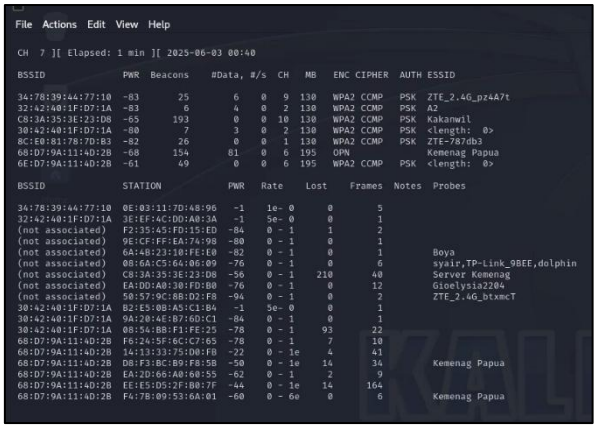
Penelitian ini dilakukan untuk menganalisis tingkat keamanan jaringan *Wireless* LAN pada Kantor Kementerian Agama Provinsi Papua menggunakan metode *Penetration Testing*. Pengujian dilakukan dengan dua skenario serangan, yaitu *Bypassing* MAC *Authentication* dan *Man in the Middle Attack* (MITM) menggunakan sistem operasi Kali Linux yang dijalankan melalui Oracle VM VirtualBox. Hasil pengujian menunjukkan bahwa sistem keamanan jaringan masih memiliki beberapa celah yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab.

DOI http://dx.doi.org/10.36448/expert.v16i1.4917
e-ISSN 2745-7265 p-ISSN 2088-5555 EXPERT Vol. 16 No. 1
June 30, 2026 – Hal. 124



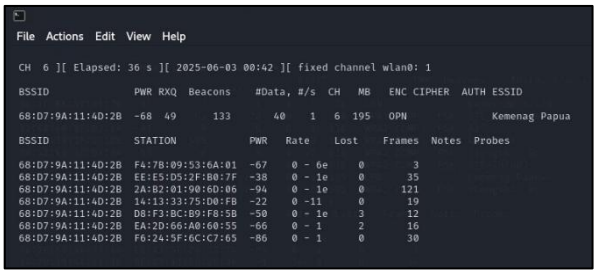
Gambar 1. Alur Serangan

Pengujian pertama dilakukan dengan metode *Bypassing* MAC *Authentication* untuk mengetahui apakah jaringan menggunakan mekanisme pembatasan akses berbasis MAC *Address*. Tahapan pengujian dimulai dengan proses identifikasi jaringan menggunakan Airodump-ng untuk memperoleh informasi BSSID, *channel*, serta perangkat yang terhubung ke jaringan *Wireless* LAN.



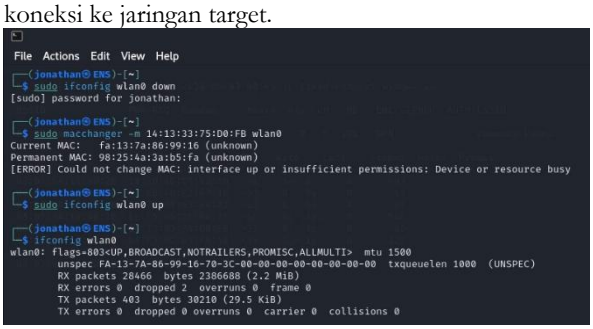
Gambar 2. Hasil Scanning Lalu Lintas Jaringan

Hasil pengamatan menunjukkan bahwa jaringan target menggunakan ESSID **Kemenag Papua** dengan BSSID **68:D7:9A:11:4D:2B** pada **channel 6**. Selanjutnya dilakukan proses penangkapan alamat MAC *Address* perangkat yang telah terhubung ke jaringan. Salah satu alamat MAC yang berhasil diperoleh adalah 14:13:33:75:D0:FB.



Gambar 3. Hasil Scanning BSSID dan Channel

Tahapan berikutnya dilakukan perubahan identitas MAC *Address* menggunakan *tools* Macchanger. Proses dilakukan dengan menonaktifkan antarmuka jaringan terlebih dahulu, kemudian mengganti alamat MAC perangkat penguji agar menyerupai perangkat target. Namun, hasil pengujian menunjukkan bahwa perubahan MAC *Address* tidak berjalan secara sempurna. Sistem menampilkan status *unspecified* (unspec) dengan alamat tidak valid sehingga perangkat penguji gagal memperoleh koneksi ke jaringan target.

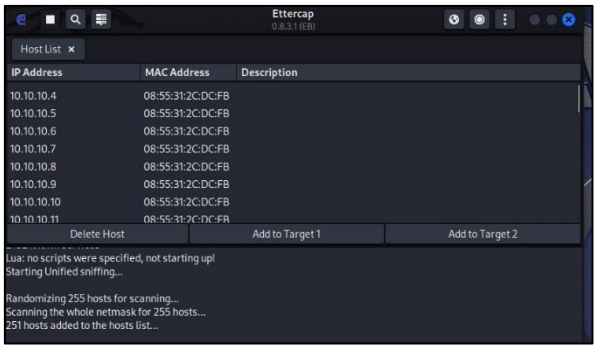


Gambar 4. Proses Macchanger dan Hasil

Hasil tersebut menunjukkan bahwa mekanisme keamanan jaringan masih mampu menolak akses tidak sah meskipun teknik MAC *spoofing* telah dilakukan. Akan tetapi, munculnya kondisi abnormal pada antarmuka jaringan menunjukkan bahwa sistem belum memiliki mekanisme deteksi dan validasi yang optimal terhadap aktivitas manipulasi MAC *Address*. Kondisi ini mengindikasikan bahwa jaringan masih berpotensi mengalami gangguan apabila terdapat percobaan serangan serupa dengan metode yang lebih kompleks.

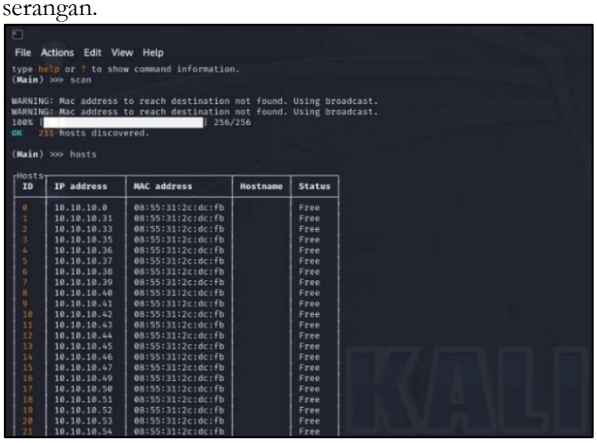
Pengujian kedua dilakukan menggunakan metode *Man in the Middle Attack* (MITM). Dalam pengujian ini, perangkat penguji telah terlebih dahulu terhubung ke jaringan *Wireless* LAN target sehingga dapat melakukan pemindaian terhadap seluruh host aktif dalam jaringan.

DOI http://dx.doi.org/10.36448/expert.v16i1.4917
e-ISSN 2745-7265 p-ISSN 2088-5555 EXPERT Vol. 16 No. 1
June 30, 2026 – Hal. 125



Gambar 5. Scanning jaringan *wireless*

Proses pengujian dilakukan menggunakan *tools* **Ettercap Graphical** untuk melakukan ARP *Poisoning*. Berdasarkan hasil pemindaian, diperoleh sebanyak 251 host aktif pada jaringan. Salah satu perangkat target memiliki alamat IP 10.10.10.191 dan dipilih sebagai target serangan.



Gambar 6. *Scanning Hosts*

Setelah proses ARP *Poisoning* berhasil dilakukan, pengujian dilanjutkan menggunakan *tools* **Evil Limiter**. *Tools* tersebut digunakan untuk melakukan pemindaian host dan memblokir akses internet perangkat target. Hasil pengujian menunjukkan bahwa perangkat target berhasil diblokir sehingga tidak dapat mengakses internet maupun membuka situs web yang diuji.

Gambar 7. Hasil *Block* IP

Pengujian kemudian dilanjutkan dengan proses pemulihan koneksi menggunakan perintah *free*. Setelah perintah dijalankan, akses internet pada perangkat target kembali normal dan situs web dapat diakses kembali tanpa kendala.

Keberhasilan serangan ini menunjukkan bahwa jaringan masih rentan terhadap serangan berbasis ARP *Spoofing*. Tidak adanya mekanisme keamanan tambahan seperti *static* ARP *binding*, DHCP *snooping*, maupun *client isolation* menyebabkan perangkat dalam jaringan dapat dimanipulasi oleh perangkat lain yang berada pada segmen jaringan yang sama.

Berdasarkan hasil pengujian yang telah dilakukan, terdapat perbedaan tingkat keberhasilan pada kedua metode serangan yang digunakan. Serangan *Bypassing* MAC *Authentication* tidak berhasil memperoleh akses ke jaringan target, sedangkan serangan *Man in the Middle Attack* berhasil memutus koneksi internet perangkat target tanpa terdeteksi oleh pengguna.

Hasil pengujian menunjukkan bahwa sistem keamanan jaringan pada Kantor Kementerian Agama Provinsi Papua telah memiliki perlindungan dasar terhadap manipulasi MAC *Address*, namun belum cukup kuat dalam menghadapi serangan berbasis manipulasi protokol jaringan seperti ARP *Spoofing*.

Keberhasilan serangan MITM memperlihatkan bahwa komunikasi antar perangkat dalam jaringan masih belum memiliki validasi identitas yang kuat. Kondisi ini dapat dimanfaatkan penyerang tidak hanya untuk memutus koneksi internet, tetapi juga untuk melakukan penyadapan lalu lintas data, pencurian informasi, maupun manipulasi komunikasi jaringan.

Dari sisi keamanan jaringan, hasil penelitian ini menunjukkan bahwa penggunaan *hotspot login* dan *firewall* pada router saja belum cukup untuk melindungi jaringan *Wireless* LAN secara menyeluruh. Sistem keamanan perlu diperkuat dengan penerapan mekanisme keamanan berlapis agar mampu mendeteksi serta mencegah aktivitas penetrasi jaringan secara *real-time* [10].

Tabel 1. Hasil Analisis

Metode Serangan	Status	Dampak	Penyebab
MITM	Berhasil	Internet target terputus	Tidak ada DHCP Snooping
MAC Spoofing	Gagal parsial	Interface abnormal	Filtering masih aktif

Berdasarkan hasil analisis pengujian, terdapat beberapa rekomendasi mitigasi yang dapat diterapkan untuk meningkatkan keamanan jaringan *Wireless* LAN pada Kantor Kementerian Agama Provinsi Papua.

Penerapan autentikasi menggunakan WPA2-Enterprise dengan 802.1X direkomendasikan untuk menggantikan autentikasi berbasis MAC *filtering*. Metode ini menggunakan autentikasi berbasis identitas pengguna sehingga lebih sulit ditembus melalui teknik *spoofing*.

Selain itu, implementasi *static* ARP *binding* diperlukan untuk mencegah manipulasi tabel ARP oleh perangkat yang tidak sah. Dengan metode ini, router maupun switch hanya menerima pasangan IP dan MAC *Address* yang telah ditentukan sebelumnya.

Aktivasi fitur DHCP *snooping* juga penting untuk memvalidasi distribusi alamat IP dalam jaringan dan mencegah perangkat asing memberikan informasi jaringan palsu kepada pengguna lain [11].

Untuk mengurangi risiko komunikasi langsung antar pengguna dalam satu jaringan *Wireless* LAN, access point perlu menerapkan fitur *client isolation* atau AP *isolation*.

DOI http://dx.doi.org/10.36448/expert.v16i1.4917
e-ISSN 2745-7265 p-ISSN 2088-5555 EXPERT Vol. 16 No. 1
June 30, 2026 – Hal. 126

Fitur ini membatasi komunikasi antar perangkat sehingga serangan MITM menjadi lebih sulit dilakukan [12].

Selain itu, penggunaan sistem *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) seperti Snort dan Suricata dapat membantu administrator jaringan mendeteksi aktivitas abnormal secara otomatis. Sistem tersebut mampu memberikan notifikasi ketika terjadi percobaan MAC *spoofing*, ARP *poisoning*, maupun aktivitas penetrasi lainnya [13].

Secara keseluruhan, hasil penelitian ini membuktikan bahwa metode *Penetration Testing* efektif digunakan untuk mengevaluasi keamanan jaringan *Wireless* LAN. Pengujian yang dilakukan mampu menunjukkan kelemahan sistem keamanan yang sebelumnya tidak terdeteksi oleh pihak pengelola jaringan.

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan pada jaringan *Wireless* LAN di Kantor Kementerian Agama Provinsi Papua menggunakan metode *Penetration Testing*, dapat disimpulkan bahwa sistem keamanan jaringan masih memiliki beberapa celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pengujian menggunakan serangan *Man in the Middle* menunjukkan bahwa penyerang mampu melakukan manipulasi lalu lintas jaringan dan memutus akses internet perangkat target tanpa diketahui oleh pengguna. Hal tersebut menunjukkan bahwa mekanisme keamanan jaringan masih rentan terhadap serangan berbasis *ARP spoofing* dan belum menerapkan perlindungan jaringan internal secara optimal.

Sementara itu, pengujian menggunakan metode *Bypassing* MAC *Authentication* tidak berhasil sepenuhnya untuk memperoleh akses ke jaringan. Namun, proses pengujian menunjukkan adanya kondisi abnormal pada antarmuka jaringan ketika dilakukan pemalsuan alamat MAC *Address*. Kondisi ini mengindikasikan bahwa sistem keamanan yang diterapkan telah memiliki mekanisme pembatasan akses berbasis MAC *filtering*, tetapi masih memerlukan peningkatan konfigurasi agar lebih stabil dan aman terhadap percobaan *spoofing*.

Secara keseluruhan, metode *Penetration Testing* dapat digunakan sebagai pendekatan untuk mengevaluasi tingkat keamanan jaringan *Wireless* LAN karena mampu memberikan gambaran nyata mengenai potensi kerentanan pada sistem jaringan yang digunakan. Hasil penelitian ini juga menunjukkan pentingnya penerapan keamanan berlapis pada jaringan nirkabel guna meminimalkan risiko penyadapan, manipulasi data, maupun gangguan layanan jaringan.

Untuk penelitian selanjutnya, disarankan agar pengujian keamanan jaringan dilakukan dengan cakupan serangan yang lebih luas dan menggunakan metode pengujian yang lebih kompleks. Selain itu, penelitian berikutnya dapat mengembangkan implementasi sistem keamanan secara langsung, seperti penerapan WPA2-*Enterprise*, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), serta mekanisme monitoring jaringan secara real-time untuk meningkatkan tingkat keamanan jaringan secara menyeluruh.

6. UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terima kasih kepada seluruh pihak yang telah memberikan dukungan, bantuan, serta kontribusi dalam pelaksanaan penelitian ini. Ucapan terima kasih secara khusus disampaikan kepada pimpinan dan staf Kantor Kementerian Agama Provinsi Papua yang telah memberikan izin, informasi, serta kesempatan kepada penulis untuk melakukan penelitian dan pengujian jaringan Wireless LAN.

DAFTAR PUSTAKA

[1] H. Dwi Sabdho and U. Maria, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang," *Semhavok*, vol. 1, no. 1, pp. 15–24, 2018.

[2] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box," *sudo J. Tek. Inform.*, vol. 1, no. 4, pp. 171–177, 2022, doi: 10.56211/sudo.v1i4.160.

[3] D. Auliafitri, E. RizkiSuro, M. R. M. Malik, and A. Setiawan, "Optimalisasi Pengujian Penetrasi: Penerapan Serangan MITM (Man in the Middle Attack) menggunakan Websploit," *J. Internet Softw. Eng.*, vol. 1, no. 3, p. 12, 2024, doi: 10.47134/pjise.v1i3.2620.

[4] R. C. Mulyanto, Yudi; Herfandi; Kirana, "Analisis Keamanan Wireless Local Area Network (WLAN) Terhadap Serangan Brute Force dengan Metode Penetration Testing (Studi Kasus:RS H.Lmanambai Abdulkadir)," *JINTEKS (Jurnal Inform. Teknol. dan Sains)*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401.

[5] Z. Saharuna and R. Nur, "Desain Jaringan WLAN Berdasarkan Cakupan Area dan Kapasitas," *J. INFOTEL - Inform. Telekomun. Elektron.*, vol. 8, no. 2, p. 115, 2016, doi: 10.20895/infotel.v8i2.127.

[6] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.

[7] I. P. A. Eka Pratama and A. A. B. A. Wiradarma, "Implementasi Katoolin Sebagai Penetrasi Tools Kali Linux Pada Linux Ubuntu 16.04 (Studi Kasus: Reverse Engineering File .Apk)," *J. Resist. (Rekayasa Sist. Komputer)*, vol. 1, no. 2, pp. 86–93, 2018, doi: 10.31598/jurnalresistor.v1i2.278.

[8] M. K. Anam, D. Sudyana, A. Noviciatie, and N.

Lizarti, "Optimalisasi Penggunaan VirtualBox Sebagai Virtual Computer Laboratory untuk Simulasi Jaringan dan Praktikum pada SMK Taruna Mandiri Pekanbaru J-PEMAS STMIK Amik Riau," *http//jurnal.sar.ac.id/index.php/J-PEMAS Optim.*, vol. vol 1, no. 2, pp. 37–44, 2020.

[9] A. Aziz Khozindani, Y. Muhyidin, and M. A. Sunandar, "Perbandingan Kinerja Tools Wireshark Dan Burpsuite Untuk Penyerangan Website Dengan Metode Sniffing," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 7, no. 3, pp. 2026–2031, 2023, doi: 10.36040/jati.v7i3.7013.

[10] N. Ade Pratama, J. Dedy Irawan, and F. Xaverius Ariwibisono, "Rancang Bangun Aplikasi Firewall Pada Jaringan Komputer," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 6, no. 2, pp. 1147–1152, 2023, doi: 10.36040/jati.v6i2.5386.

[11] D. A. Pradana and A. S. Budiman, "The DHCP Snooping and DHCP Alert Method in Securing DHCP Server from DHCP Rogue Attack," *Int. J. Informatics Dev.*, vol. 10, no. 1, pp. 38–46, 2021, doi: 10.14421/ijid.2021.2287.

[12] T. Mirzoev and S. White, "The Role of Client Isolation in Protecting Wi-Fi Users from ARP Spoofing Attacks," *i-managers J. Inf. Technol.*, vol. 1, no. 2, 2014, doi: 10.48550/arXiv.1404.2172.

[13] A. A. E. Boukebous, M. I. Fettache, G. Bendiab, and S. Shiaeles, "A Comparative Analysis of Snort 3 and Suricata," in *IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, 2023. doi: 10.1109/GlobConET56651.2023.10150141.