Jurnal Komputer Multidisipliner

Vol.9 No.2, February 2026
ISSN: 24559633

ANALISIS KEAMANAN JARINGAN WLAN MENGGUNAKAN METODE VULNERABILITY ASSESSMENT DAN PENETRATION TESTING PADA HOTEL NUSA INDAH PALOPO

Marchella Angel[1], Siaulhak[2]
Universitas Cokroaminoto Palopo
E-mail: marchellaangel187@gmail.com[1],
siaulhak@uncp.ac.id[2]

Abstrak

Perkembangan teknologi jaringan nirkabel (Wireless Local Area Network/WLAN) memberikan kemudahan akses internet di berbagai sektor, termasuk industri perhotelan. Hotel sebagai penyedia layanan publik memanfaatkan jaringan WLAN untuk mendukung kebutuhan tamu dan operasional internal. Namun, tingginya jumlah pengguna serta sifat jaringan yang terbuka menjadikan WLAN sebagai target potensial berbagai ancaman keamanan siber seperti penyadapan data (sniffing), serangan man-in-the-middle, dan akses ilegalPenelitian ini bertujuan untuk menganalisis tingkat keamanan jaringan WLAN pada Hotel Nusa Indah Palopo menggunakan metode Vulnerability Assessment (VA) dan Penetration Testing (PT). Metode VA digunakan untuk mengidentifikasi celah keamanan, sedangkan PT dilakukan untuk mensimulasikan serangan nyata terhadap sistem. Pengumpulan data dilakukan melalui observasi jaringan, analisis lalu lintas paket menggunakan Wireshark, serta pengujian port eksternal menggunakan ShieldsUP.Hasil penelitian menunjukkan bahwa sistem jaringan masih menggunakan protokol HTTP tanpa enkripsi sehingga data pengguna dapat terbaca selama proses sniffing. Di sisi lain, konfigurasi firewall Mikrotik telah mampu menutup sebagian besar port umum sehingga relatif aman dari serangan eksternal. Kerentanan utama ditemukan pada sisi internal jaringan, terutama pada mekanisme enkripsi data dan sistem autentikasi pengguna hotspot.

Kata Kunci: Keamanan Jaringan, WLAN, Mikrotik, Vulnerability Assessment, Penetration Testing.

1. PENDAHULUAN

Pemanfaatan jaringan WLAN pada sektor perhotelan menjadi kebutuhan utama dalam mendukung layanan digital, mulai dari komunikasi tamu, transaksi daring, hingga sistem manajemen hotel. Jaringan nirkabel menawarkan fleksibilitas tinggi, namun di sisi lain memiliki risiko keamanan yang lebih besar dibanding jaringan kabel karena sifat transmisinya yang dapat diakses melalui udara.Hotel Nusa Indah Palopo menyediakan fasilitas hotspot gratis bagi tamu dan staf. Berdasarkan pengamatan awal, belum terdapat evaluasi menyeluruh terhadap keamanan jaringan tersebut. Kondisi ini berpotensi menimbulkan risiko kebocoran data, penyalahgunaan akses, hingga gangguan terhadap sistem operasional hotel.Oleh karena itu, penelitian ini dilakukan untuk mengevaluasi keamanan jaringan WLAN menggunakan pendekatan Vulnerability Assessment dan Penetration Testing guna mengetahui tingkat kerentanan sistem serta memberikan rekomendasi peningkatan keamanan.

TINJAUAN PUSTAKA

Vulnerability Assessment

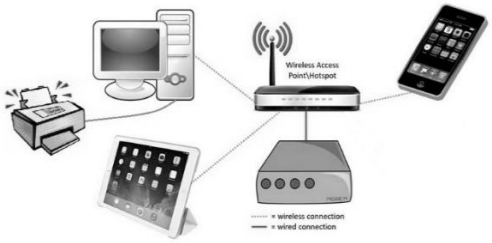
Vulnerability assessment (VA) adalah evaluasi komprehensif dan mendalam terhadap aspek-aspek keamanan, termasuk keamanan informasi, hasil pemindaian jaringan, pengelolaan sistem, konfigurasi, kesadaran keamanan dari pihak yang terlibat, serta aspek keamanan fisik, dengan tujuan untuk mengidentifikasi semua potensi kerentanan kritis yang mungkin ada (Darojat, 2022).

Penetration Testing

Penetration testing adalah proses simulasi serangan pada sistem yang memerlukan sertifikasi keamanan jaringan untuk mencegah peretas atau penyerang jaringan yang menyebabkan kehilangan data pribadi dan data perusahaan. Orang yang melakukan metode ini juga disebut sebagai pentester. Uji penetrasi adalah serangan jaringan yang disimulasikan pada sistem komputer untuk mengungkap kerentanan, ancaman, dan risiko dalam aplikasi 6 perangkat lunak, jaringan, atau aplikasi web yang dapat digunakan oleh penyerang (N. A. Santoso, 2022).

Wireless Local Area Network (WLAN)

Jaringan tanpa kabel (wireless) atau jaringan nirkabel merupakan suatu jalan keluar terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Pada saat ini jaringan nirkabel atau wireless sudah banyak digunakan dengan memanfaatkan jasa satelit dan bahkan mampu memberi kecepatan akses yang lebih cepat bila dibandingkan dengan jaringan yang menggunakan kabel (Mulyanto, 2022).



Sumber: smktibaliglobalsingaraja.sch.id (2024)

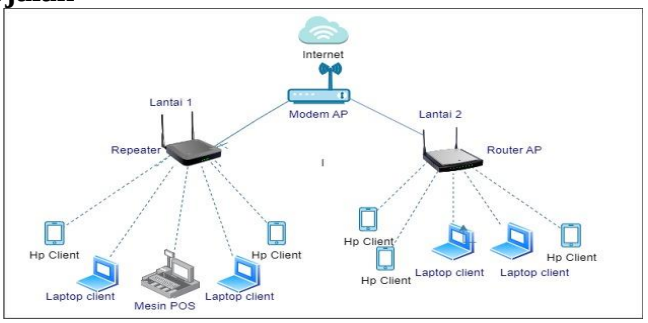
Wireshark

Wireshark merupakan sebuah alat analisis jaringan yang digunakan untuk memantau dan merekam lalu lintas data yang melewati jaringan komputer. Perangkat lunak ini mampu menangkap serta menampilkan informasi detail dari setiap paket data yang dikirim maupun diterima, sehingga memudahkan pengguna dalam menganalisis aktivitas jaringan secara menyeluruh. (Reivaldi Kesuma Kagi, 2020).

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif yang dilakukan melalui beberapa tahapan, yaitu reconnaissance untuk mengumpulkan informasi jaringan, scanning dan enumeration untuk mengidentifikasi perangkat serta layanan yang aktif, vulnerability assessment untuk memetakan celah keamanan, penetration testing sebagai simulasi serangan, risk analysis untuk menentukan tingkat risiko, serta recommendation berupa penyusunan solusi keamanan yang sesuai.

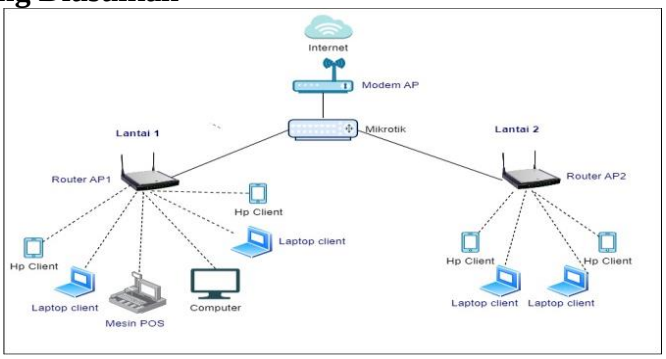
Analisis Sistem Berjalan



Gambar. Sistem yang Berjalan

Sumber: Rancangan Penulis (2024)

Analisis Sistem yang Diusulkan



Gambar. Sistem yang Diusulkan

Sumber: Rancangan Penulis (2024)

4. HASIL DAN PEMBAHASAN

Hasil pengujian menunjukkan beberapa temuan penting terkait keamanan jaringan.

Hasil Recconnaissance

Tahap reconnaissance merupakan langkah awal yang penting dalam penelitian ini, diawali dengan konfigurasi awal jaringan WLAN menggunakan router Mikrotik. Tahapan ini bertujuan untuk mempersiapkan infrastruktur jaringan agar berfungsi optimal dan siap digunakan pada tahap pengujian selanjutnya.

Tabel . Hasil Penelitian Testing

No.	Jenis Testing	Keterangan
1	Sniffing Data (HTTP)	Perlu implementasi HTTPS
2	Pengujian Port Eksternal	Aman dari serangan luar
3	Autentikasi Hotspot	Perlu voucher unik dan limit waktu akses
4	Update Sistem	Risiko exploit dari versi lama

Sumber: Hasil Olah Data (2025)

Selain itu, hasil uji pada masing-masing pengguna voucher ditunjukkan pada tabel berikut:

Tabel 2. Hasil Uji Pengguna Voucher

No.	ID Pengguna	Username Voucher	Durasi Akses
1	User-01	voucher01	30 menit
2	User-02	voucher02	25 menit
3	User-03	voucher03	0 menit
4	User-04	voucher04	20 menit

Sumber: Hasil Olah Data (2025)

Hasil Penetration Testing

Dengan pengujian ini dapat disimpulkan, secara lokal data dapat dibaca jika tidak menggunakan enkripsi (terlihat pada wireshark), namun secara eksternal port UPnP dinyatakan tertutup sehingga meminimalisir serangan dari internet (terlihat pada shieldsUP).

Gambar. Pengujian Menggunakan ShieldsUp

Sumber: Hasil Dokumentasi Penulis (2025)

Vulnerability Assessment

Pada tahap ini dilakukan analisis lanjutan terhadap hasil pengujian sebelumnya. Hasil Wireshark menunjukkan lalu lintas HTTP pada hotspot masih menggunakan plain text sehingga rentan disadap di jaringan lokal, sedangkan pengujian ShieldsUP menyatakan port UPnP dan layanan publik tertutup, menandakan konfigurasi NAT dan firewall Mikrotik telah berfungsi dengan baik dalam melindungi dari serangan eksternal.

Tabel 3. Analisis Risiko Keamanan Jaringan WLAN

No	Aspek yang Dinilai	Temuan/Hasil Pengujian	Potensi Kerentanan	Severity (Risiko)	Tindakan Pencegahan / Rekomendasi
1	Lalu lintas *HTTP*	Data terlihat *plain text* di *Wireshark* (*GET /connecttest.txt*)	Rentan disadap (*sniffing*) di jaringan lokal	Tinggi	Gunakan *HTTPS / SSL login* hotspot
2	*Firewall dan NAT*	*Port UPnP dan service* lain terblokir (*ShieldsUP*)	Tidak ada celah akses dari luar	Rendah	Pertahankan konfigurasi *NAT* dan *firewall*
3	Port publik	Tidak merespons probe *UPnP* dari internet	Layanan publik tertutup	Rendah	Terus pantau dan blokir port tidak perlu
4	*DHCP dan Hotspot Auth*	*DHCP aktif*, *login* hotspot manual	Risiko *credential sharing / abuse*	Sedang	Gunakan *voucher* unik dan batasi waktu akses
5	*Update RouterOS*	Belum terverifikasi *patch* terbaru	Potensi *exploit OS* lama	Sedang - Tinggi	*Update RouterOS* secara berkala

Sumber: Hasil Olah Data (2025)

Final Analysis

Analisis menunjukkan bahwa kelemahan terbesar berada pada penggunaan HTTP tanpa enkripsi, yang memungkinkan penyadapan data pengguna. Selain itu, tidak adanya segmentasi jaringan membuat seluruh klien berada dalam satu broadcast domain sehingga meningkatkan risiko serangan internal.Firewall eksternal telah dikonfigurasi dengan baik,

terbukti dari hasil pengujian port scanning yang menunjukkan mayoritas port dalam kondisi tertutup. Hal ini mengurangi kemungkinan serangan dari luar jaringan.

Pembahasan Penelitian

Penelitian ini menunjukkan bahwa kelemahan utama keamanan jaringan hotspot Mikrotik Hotel Nusa Indah Palopo berada pada sisi internal, khususnya penggunaan protokol HTTP tanpa enkripsi yang rentan terhadap penyadapan. Sementara itu, sisi eksternal relatif aman berkat konfigurasi firewall dan NAT yang baik. Oleh karena itu, diperlukan penguatan enkripsi, autentikasi pengguna, serta pembaruan dan pemantauan sistem secara berkala.

5. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan mengenai keamanan jaringan WLAN di Hotel Nusa Indah Palopo, serta merujuk pada rumusan dan batasan masalah yang telah ditentukan, dapat disimpulkan bahwa infrastruktur jaringan nirkabel di hotel tersebut masih memiliki beberapa celah keamanan, khususnya pada lalu lintas data internal yang belum dilindungi dengan enkripsi yang memadai. Melalui proses pengujian menggunakan aplikasi wireshark, teridentifikasi bahwa komunikasi antara klien dan server hotspot masih memanfaatkan protokol HTTP tanpa lapisan pengamanan, sehingga informasi seperti kredensial login dan permintaan URL dapat terlihat secara langsung dalam bentuk teks biasa. Kondisi ini membuka peluang bagi pihak tidak bertanggung jawab untuk melakukan penyadapan maupun serangan man-in-the-middle.

Saran

Setelah dilakukan penelitian pada jaringan WLAN Hotel Nusa Indah Palopo, penulis menyarankan penerapan protokol HTTPS pada halaman login hotspot untuk melindungi data pengguna dari penyadapan dan mencegah serangan man-in-the-middle, pengaturan penggunaan voucher dengan username dan password yang unik guna meminimalkan penyalahgunaan akses, serta pembaruan sistem operasi Mikrotik secara berkala oleh administrator jaringan untuk menutup potensi celah keamanan pada versi perangkat lunak sebelumnya.

DAFTAR PUSTAKA

Afrio Triputra Sitompul, Nurfalinda, dan Ferdi Chahyadi. (2023). Analisis Penerapan Metode Penetration Testing Pada Keamanan Jaringan WLAN (Studi Kasus: Universitas Maritim Raja Ali Haji).

Anas, M. A., dan Soepriyanto, Y. (n.d.). Pengembangan Multimedia Tutorial Topologi Jaringan Untuk Smk Kelas X Teknik Komputer Dan Jaringan. 2019.

Anggraini, Y. (2021). Analisis Persiapan Guru dalam Pembelajaran Matematika di Sekolah Dasar. Jurnal Basicedu, 5(4), 2415–2422.

Arifudin, O. (2023). Analisis Teori Taksonomi Bloom Pada Pendidikan Di Indonesia. 2023.

Darojat, E. Z., Sediyono, E., dan Sembiring, I. (2022). Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner. 2022.

Dewi Laksmiati, E. (2020). Vulnerability Assessment Pada Situs Www.Hatsehat.Com Menggunakan Openvas. 5.

Dr.Muhammad Ramdhan, S. M. (2021). Metode Penelitian. Surabaya: Cipta Media Nusantara.

Farismana, R., dan Pramadhana, D. (2023). Vulnerability Assessment Untuk Analisis Tingkat Keamanan Pada Sistem Informasi Repositori Karya Ilmiah Politeknik Xyz. 3.

Irfan Murti Raazi, Ima Dwitawati, dan Putri Nabila. (2023). Uji Vulnerability Assessment Dalam

Mengetahui Tingkat Keamanan Web Aplikasi Sistem Informasi Laporan Diskominfo Dan Sandi Aceh. JINTECH: Journal Of Information Technology, 4(1), 1–15.

Jimmy Harianto Kabenarang, Rudy Harijadi Wibowo Pardanus, dan Mario Tulenan Parinsi. (2022). Analisis Dan Perancangan Jaringan Wireless Local Area Network Di Smk.

Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode PenetrationTesting(Studi Kasus: TP-Link Archer A6). 1(1).

Mochamad Adhari Adiguna dan Bambang Wisnu Widagdo. (2022). Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r).

Mulyanto, Y., Herfandi, H., dan Candra Kirana, R. (2022). Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi kasus:RS H.LMANAMBAI ABDULKADIR). Jurnal Informatika Teknologi dan Sains, 4(1), 26–35.

Nugroho, R., Budiyono, A., dan Widjajarto, A. (2020). Implementasi Dan Analisa Security Auditing Menggunakan Open Source Software Kali Linux Dengan Framework Cyber Kill Chain.

Rachman, R. (2021). Program Studi Teknik Informatika Fakultas Teknik Universitas Islam Riau Pekanbaru 202.

Ray R. A. A, Olivia Kembuan, dan Olivia Kembuan. (2020). Perancangan dan implementasi jaringan komputer SMK Negeri 1 Tahuna.

Reivaldi K. K., M. Ficky D., and H. Ajie, (2020) "Desain Dan Implementasi Pada Wifi Pustikom Free Access Di Pusat Teknologi Informasi Dan Komunikasi Universitas Negeri Jakarta Menggunakan Mikrotik Dan Wireshark Untuk Analisis Terhadap Serangan Packet Sniffing Dan Netcut,"

Santoso, J. D. (2019). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. 2019, 1(3).

Santoso, N. A., Ainurohman, M., dan Kurniawan, R. D. (2022). Penerapan Metode Penetration Testing Pada Keamanan Jaringan Nirkabel. 2022.

Satria Galang Saputra, Parga Zen, B., dan Abdurahman. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). Jurnal Sistem Informasi Galuh, 1(2), 43–51.

Syafrizal, M. (2020). Pengantar Jaringan Komputer. Yogyakarta: STMIK Amikom Yogyakarta.

T. A. Tamsir, Eggy S., K., and M.Tio F, (2023) "Analisis Paket Icmp Website Universitas Binadarma Menggunakan Wireshark," STORAGE J. Ilm. Tek. dan Ilmu Komput.,

Wahyudin, Sopiyan Dalis, Resti, dan Resti. (2024). Metode Vulnerability Assesment Dalam Pengujian Kinerja Sistem Keamanan Website Points of Sales.

Y. Mendrofa and R. Fauzi (2023), "Implementasi Keamanan Jaringan Menggunakan Port Knocking," Comput. Sci. Ind. Eng., vol. 9, no. 7, p. 30.