Analisis Keamanan Jaringan Nirkabel Melalui Metode Penetration Testing Pada SD Kartika VII-3 Denpasar

I Gede Putu Agus Pranatha Jaya[1)], Ni Kadek Sukerti[2)], I Made Ari Santosa[3)]
Sistem Komputer[1),3)], Sistem Informasi[2)],
Institut Teknologi dan Bisnis STIKOM Bali
Denpasar, Indonesia
e-mail: 200010034@stikom-bali.ac.id[1)], dektisamuh@gmail.com[2)], arisantosamade@gmail.com[3)]

Abstrak

Keamanan jaringan nirkabel menjadi faktor krusial dalam mendukung proses pembelajaran di era digital, termasuk di Yayasan Kartika Jaya SD Kartika VII-3 Denpasar. Jaringan nirkabel di sekolah ini, yang melayani 200 siswa dan staf, digunakan untuk berbagai kegiatan pembelajaran berbasis teknologi serta mendukung sistem administrasi digital. Namun, ancaman keamanan, seperti akses tidak sah dan potensi peretasan, menjadi tantangan yang perlu diatasi. Penelitian ini bertujuan untuk menganalisis keamanan jaringan nirkabel di SD Kartika VII-3 melalui metode penetration testing. Metode ini melibatkan serangkaian simulasi serangan untuk mengidentifikasi kerentanan pada jaringan dan menguji tingkat keamanannya. Pengujian dilakukan dengan menggunakan alat Kali Linux, mencakup serangan terhadap enkripsi WPA2-PSK, bypassing MAC address authentication, serta DoS attack. Hasil penelitian menunjukkan bahwa jaringan ini rentan terhadap beberapa jenis serangan, terutama dalam hal cracking WPA key dan bypassing MAC address. Dengan demikian, diperlukan langkah-langkah perbaikan, termasuk penguatan konfigurasi keamanan jaringan dan penggunaan password yang lebih kompleks. Penelitian ini memberikan wawasan penting bagi sekolah-sekolah untuk meningkatkan keamanan jaringan nirkabel guna melindungi data dan memastikan kelancaran proses pembelajaran.

Kata kunci: *Keamanan Jaringan Nirkabel, Penetration Testing, WPA2-PSK, Keamanan Data, Kerentanan Jaringan.*

1. Pendahuluan

Pendidikan di era digital yang semakin maju mengandalkan jaringan nirkabel (Wi-Fi) sebagai infrastruktur kunci, seperti yang ditemukan di Yayasan Kartika Jaya SD Kartika VII-3 Denpasar. Jaringan nirkabel ini tidak hanya berfungsi sebagai sarana koneksi internet, tetapi juga sebagai alat komunikasi yang mendukung berbagai aspek proses pembelajaran dan administrasi sekolah. Yayasan Kartika Jaya SD Kartika VII-3 memiliki jaringan nirkabel dengan tiga titik akses (*access point*) yang tersebar di seluruh lingkungan sekolah, termasuk di ruang kelas, perpustakaan, dan kantor guru, yang melayani sekitar 200 siswa dan staf setiap harinya. Jaringan ini digunakan dalam kegiatan pembelajaran berbasis teknologi, seperti penggunaan *tablet* untuk membaca materi pelajaran, ujian berbasis komputer, serta penggunaan aplikasi pembelajaran daring. Jaringan ini juga memfasilitasi sistem administrasi digital sekolah, termasuk manajemen data siswa, operasi keuangan, dan komunikasi antara pendidik dan orang tua.

Meskipun jaringan ini telah membantu meningkatkan efisiensi operasional dan pembelajaran di sekolah, terdapat beberapa tantangan dalam aspek keamanannya. Salah satu tantangan yang dihadapi adalah potensi akses tidak sah ke jaringan. Sekolah pernah mengalami upaya penembusan jaringan oleh pihak yang tidak diketahui, yang memanfaatkan jaringan sekolah untuk mendapatkan internet gratis. Untuk mencegah masalah yang lebih serius, seperti peretasan dan hilangnya data penting, termasuk informasi siswa, lembaga pendidikan harus menerapkan tindakan pencegahan.

Keamanan jaringan sangat penting karena kelemahan yang tidak diatasi dapat menyebabkan kerugian seperti kehilangan data, kerusakan sistem, atau bahkan pencurian aset berharga. Ancaman seperti *DDoS attacks*, *hacker*, *virus*, dan *trojan* semakin meningkat, terutama ketika jaringan terhubung ke internet. Oleh karena itu, keamanan jaringan harus diutamakan untuk menjaga sistem terhadap ancaman yang semakin kompleks dan beragam[1].

Solusi yang tepat untuk masalah ini adalah penerapan pengujian penetrasi. adalah serangkaian prosedur dan teknik yang dirancang untuk menilai keamanan sistem atau jaringan komputer dengan mensimulasikan serangan untuk mengidentifikasi kerentanan, yang memungkinkan penutupan atau

perbaikan selanjutnya. *Penetration testing* dilakukan sebagai strategi proaktif untuk mengurangi risiko peretasan pada suatu sistem[2].

Berdasarkan penelitian yang dilakukan oleh Nugroho Adhi Santoso[3], penelitian ini mengkaji penerapan teknik pengujian penetrasi pada keamanan jaringan *WLAN* yang beroperasi pada frekuensi 2,4 *GHz* dan 5 *GHz* di SMK Bhakti Praja Adiwerna, Kabupaten Tegal. Menggunakan alat dari *Kali Linux* versi 2021.1, penelitian ini berhasil menguji keamanan jaringan nirkabel, mengidentifikasi kunci *WPA* dengan database *Wordlist*, dan memberikan dasar untuk penerapan keamanan yang lebih kuat di lingkungan pendidikan. Hasil penelitian ini penting untuk memahami kerentanan keamanan pada jaringan *WLAN*.

Berdasarkan penelitian yang dilakukan Afrio Triputra Sitompul [4], dalam penelitiannya di Universitas Maritim Raja Ali Haji (UMRAH), ia meneliti keamanan jaringan WLAN melalui metodologi *Penetration testing*. Hasil penelitian menunjukkan bahwa jaringan *WLAN* di UMRAH rentan terhadap serangan seperti *DeAuth* dan *Man In The Middle* (*MITM*) *Attack*. Percobaan serangan dengan *Evil Limiter* dan *Aireplay-ng* berhasil mengidentifikasi kelemahan keamanan. Penelitian ini menyoroti perlunya langkah-langkah perbaikan keamanan yang lebih kuat di lingkungan kampus.

Berdasarkan penelitian yang dilakukan oleh Harry Dwi Sabdho [5], Analisis keamanan jaringan nirkabel dilakukan di kantor PT. Mora Telematika Indonesia Regional Palembang dengan menggunakan pendekatan *Penetration testing*. Penelitian bertujuan untuk mengidentifikasi potensi kerentanan dalam sistem jaringan *WLAN* perusahaan serta mengevaluasi langkah-langkah keamanan yang telah diimplementasikan. Para peneliti melakukan serangkaian uji penetrasi untuk menyelidiki berbagai serangan potensial, termasuk pembobolan enkripsi, serangan *Denial of Service (DoS)*, dan serangan *Man-in-the-Middle (MITM)*. Hasil penelitian memberikan gambaran tentang kelemahan sistem jaringan *WLAN* yang perlu diperbaiki guna meningkatkan keamanan.

Dengan demikian, penelitian ini menjadi langkah penting dalam menjaga integritas dan keberlanjutan proses pendidikan di era digital yang semakin kompleks dan berisiko. Dengan meningkatnya peran jaringan nirkabel dalam pendidikan, keamanan jaringan harus diutamakan untuk melindungi data siswa, menjaga kelancaran pembelajaran, dan memberikan lingkungan yang aman bagi seluruh komunitas sekolah. Dengan penelitian ini, diharapkan sekolah-sekolah dapat lebih siap menghadapi ancaman siber dan menjaga keberlanjutan pendidikan di masa depan.

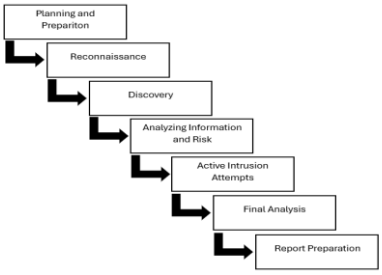
2. Metode Penelitian

Penelitian ini menggunakan metode pengujian penetrasi. *Penetration testing* adalah pendekatan proaktif yang digunakan untuk menilai keamanan aset digital dengan cara mendeteksi dan mengeksploitasi kelemahan sistem secara aktif[6]. Metode ini berupaya mengidentifikasi dan mencatat kerentanan keamanan yang dapat dieksploitasi oleh entitas yang lalai. Selain itu, pengujian ini juga membantu dalam memahami potensi dampak yang dihasilkan oleh celah tersebut serta memberikan rekomendasi perbaikan yang relevan[7].

Secara umum, *penetration testing* dapat mencakup uji penetrasi terhadap jaringan maupun aplikasi keamanan, serta evaluasi terhadap kontrol dan proses yang diterapkan pada jaringan tersebut. Pengujian dapat dilakukan dari luar jaringan (*external testing*) untuk mencoba menerobos perlindungan eksternal, atau dari dalam jaringan (*internal testing*) untuk memeriksa kelemahan yang mungkin ada pada sistem internal[8].

Tujuan utama pendekatan pengujian penetrasi ini adalah untuk mendeteksi kerentanan keamanan akibat masalah konfigurasi atau kelemahan perangkat lunak, yang dapat memberikan peluang bagi ancaman eksternal maupun internal[9]. Melalui simulasi serangan jaringan, metode ini tidak hanya menemukan kelemahan sistem tetapi juga membantu organisasi memperkuat kebijakan keamanan serta merancang strategi mitigasi yang lebih efektif untuk menghadapi ancaman baru.

Prosedur yang terlibat dalam metodologi pengujian penetrasi mencakup langkah-langkah berikut:



Gambar 1. Metode *Penetration Testing*

a. *Planning and Preparation*
Tetapkan tujuan dan sasaran yang ingin dicapai selama proses penilaian pengujian penetrasi. Tahap awal *planning and preparation* bertujuan untuk memfasilitasi pelacakan yang jelas dan lugas selama proses pengujian. Secara keseluruhan, tahap ini menekankan pada pendeteksian kerentanan dan peningkatan langkah-langkah keamanan.

b. *Reconnasissance*
Reconnasissance mengacu pada pengumpulan data, yang dapat diklasifikasikan sebagai *passive penetration testing*, karena melibatkan pengumpulan data manual melalui dokumentasi dari entitas terkait atau informasi yang diminta secara terbuka dari pihak-pihak yang terkait dengan sistem.

c. *Discovery*
Discovery melibatkan pengumpulan informasi melalui teknologi otomatis yang memeriksa kerentanan dalam sistem, yang mencakup jaringan, server, perangkat, dan data.

d. *Analyzing Information and Risk*
Tahap ini melibatkan peninjauan menyeluruh terhadap informasi yang diperoleh sebelumnya (fase *reconnaissance* dan *discovery*) untuk mengidentifikasi risiko dan kerentanan keamanan yang melekat pada sistem yang diterapkan.

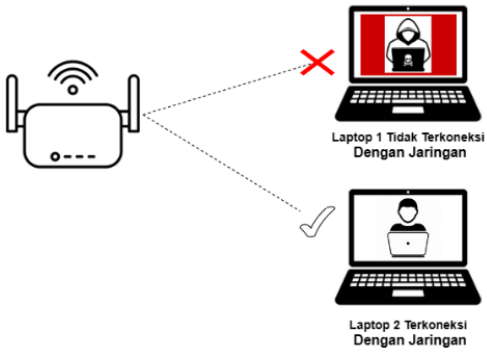
e. *Active Intrusion Attempts*
Tingkat ini melibatkan penyediaan instruksi aktif mengenai keamanan sistem untuk memperbaiki kelemahan yang teridentifikasi dan meningkatkan langkah-langkah keamanan.

f. *Final Analysis*
Analisis akhir yang komprehensif menyajikan ringkasan semua temuan dan rekomendasi teknis untuk meningkatkan keamanan mengikuti kerangka kerja analitis yang metodis.

g. *Report Preparation*
Tahap akhir aktivitas pengujian penetrasi melibatkan penyampaian laporan yang merinci temuan *investigasi* dan rekomendasi kepada pemangku kepentingan terkait yang bertanggung jawab atas sistem, yang berfungsi sebagai referensi untuk meningkatkan keamanan sistem[10].

3. Hasil dan Pembahasan

Pengujian yang dilakukan menggunakan konfigurasi jaringan terdiri dari satu router nirkabel dan dua laptop. Satu laptop beroperasi pada OS Windows dan berfungsi sebagai klien yang terhubung ke jaringan titik akses, sementara laptop lainnya berfungsi sebagai penyerang menggunakan Kali Linux untuk mencoba membobol jaringan.



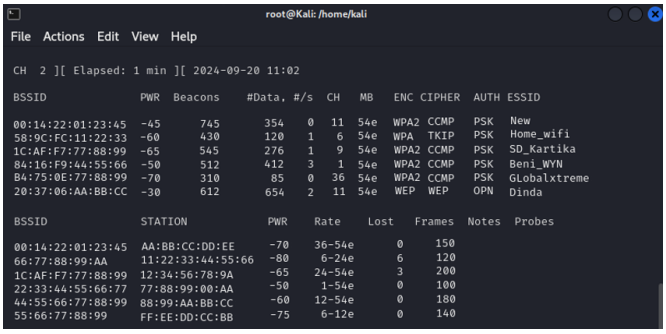
Gambar 2. Desain Jaringan

Dalam kerangka penilaian keamanan jaringan nirkabel ini, banyak jenis serangan yang akan dievaluasi meliputi:

3.1 *Cracking The Encryption*

Pada tahap awal pengujian ini, penulis menargetkan jaringan "SD_Kartika" untuk memverifikasi apakah jaringan tersebut dilindungi oleh protokol enkripsi seperti *WEP, WPA*, atau *WPA2-PSK*. Proses ini

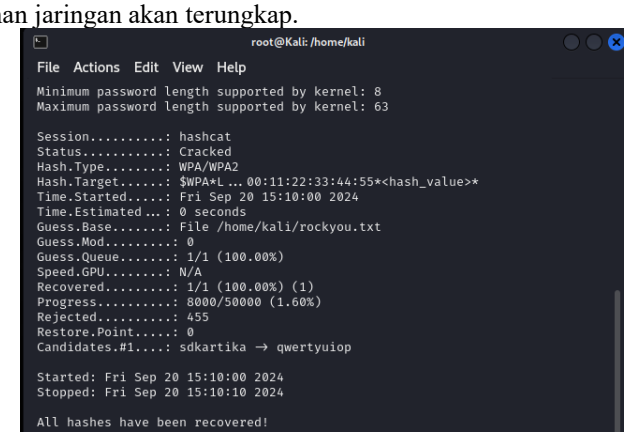
dimulai dengan memindai *Access Point* menggunakan alat *aircrack-ng* untuk mengidentifikasi dan mengumpulkan paket data.



Gambar 3. Proses *Scanning*

Gambar di atas menunjukkan proses scanning yang dilakukan terhadap jaringan "SD_Kartika," di mana data paket yang berhasil dikumpulkan menjadi dasar untuk tahap dekripsi selanjutnya. Hasil dari *scanning* ini menunjukkan bahwa data mentah berhasil dikumpulkan dan siap untuk didekripsi, menyoroti potensi kelemahan dalam mekanisme enkripsi yang ada.

Setelah data paket berhasil dikumpulkan, langkah selanjutnya adalah menentukan target untuk proses dekripsi menggunakan Hashcat, sebuah tool dalam *penetration testing* yang digunakan untuk memecahkan password dengan membandingkan data tersebut dengan kata sandi dalam kamus. Jika dekripsi berhasil, kunci keamanan jaringan akan terungkap.

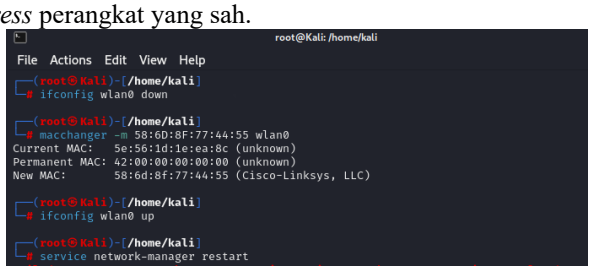


Gambar 4. Proses dekripsi menggunakan *hashcat*

Gambar ini menunjukkan proses dekripsi data dari "SD_Kartika" menggunakan *hashcat*. Proses ini mengungkap kelemahan enkripsi pada jaringan tersebut jika kunci keamanan dapat diretas.

3.2 *Bypassing MAC Address Authentication*

Pengujian tahap kedua berfokus pada evaluasi efektivitas *MAC address filtering* di jaringan "SD_Kartika." Proses ini dimulai dengan menggunakan aircrack-ng untuk memantau lalu lintas jaringan dan mengidentifikasi *MAC Address* dari perangkat yang aktif dalam jaringan. *MAC Address* adalah pengenal unik yang diberikan kepada setiap perangkat jaringan untuk komunikasi. Setelah *MAC Address* target diidentifikasi, macchanger digunakan untuk memodifikasi *MAC Address* perangkat penyerang agar cocok dengan *MAC Address* perangkat yang sah.



Gambar 5. Proses *Bypassing MAC Address*

Gambar di atas mengilustrasikan bagaimana *MAC Address* dari perangkat yang sah dalam jaringan "SD_Kartika" berhasil disalin dan digunakan untuk melewati filter *MAC*. Hasil pengujian menunjukkan bahwa *MAC filtering* yang diterapkan tidak cukup kuat untuk mencegah akses yang tidak sah, karena perangkat penyerang dapat dengan mudah masuk setelah mengganti *MAC Address*-nya.

3.3 *Attacking The Infrastructure*

Pada tahap ini, penulis melakukan serangan terhadap jaringan "SD_Kartika" dengan menggunakan metode *Denial of Service (DoS)* untuk mengganggu kinerja jaringan secara keseluruhan. Serangan ini bertujuan untuk memutuskan koneksi pengguna lain yang sedang terhubung ke jaringan. Langkah awal dimulai dengan mengakses jaringan menggunakan *password* yang telah diperoleh sebelumnya untuk menghubungkan perangkat penguji.

Gambar 6. Serangan *Dos(Denial of Service)*

Gambar di atas mengilustrasikan serangan *DoS* yang diterapkan pada jaringan "SD_Kartika," di mana serangan ini berhasil memutuskan koneksi perangkat lain yang terhubung. Pengujian ini mengungkap kelemahan pada lapisan infrastruktur jaringan yang memungkinkan gangguan signifikan terhadap pengguna yang sah.

Untuk menguji kerentanan *WPA key* pada jaringan nirkabel SD Kartika VII, dilakukan serangkaian pengujian mendalam. Hasil dari pengujian ini mengungkapkan bahwa Jaringan Nirkabel pada SD Kartika VII memiliki tingkat kerentanan yang signifikan terhadap serangan. *Penetration testing*yang diterapkan memberikan wawasan mengenai kelemahan yang ada dalam sistem keamanan jaringan. Tabel 1 berikut menyajikan hasil dari metode *Penetration testing*yang digunakan, memberikan gambaran umum mengenai temuan dan potensi risiko yang diidentifikasi selama evaluasi jaringan ini.

Tabel 1. Hasil Uji Penetrasi Jaringan Nirkabel

Jenis Serangan	Data yang dibutuhkan	Keterangan
Cracking The *Ercryption*	*Wordlist database Password*	Berhasil
Bypassing MAC address Authentication	*List user* dalam jaringan yang sama	Berhasil
Attacking The Infrastructure	*Wpa Key* Hasil *Attacking WPA Key*	Berhasil

4. Kesimpulan

Berdasarkan hasil penelitian melalui pengujian penetrasi menggunakan *Kali Linux* di SD Kartika VII-Denpasar, ditemukan bahwa sistem keamanan jaringan nirkabel masih memiliki kelemahan signifikan, terutama akibat penggunaan *password* yang rentan terhadap serangan. Untuk meningkatkan keamanan jaringan *wireless* di SD Kartika VII-Denpasar, disarankan agar dilakukan penguatan dengan konfigurasi yang lebih aman dan penggunaan *WPA Key* yang lebih kompleks, yang mencakup kombinasi angka dan simbol. Penelitian ini juga menunjukkan bahwa pengujian penetrasi tidak hanya relevan untuk

mengidentifikasi kelemahan, tetapi juga penting untuk proses pembelajaran yang dapat diterapkan di berbagai lingkungan jaringan.

Daftar Pustaka

[1] M. Hasibuan and A. M. Elhanafi, "Penetration Testing Sistem Jaringan Komputer Menggunakan Kali Linux untuk Mengetahui Kerentanan Keamanan Server dengan Metode Black Box: Studi Kasus Web Server Diva Karaoke. co. id," *sudo Jurnal Teknik Informatika*, vol. 1, no. 4, pp. 171–177, 2022.

[2] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *Jurnal Algoritma*, vol. 18, no. 1, pp. 77–86, 2021.

[3] N. A. Santoso, M. Ainurohman, and R. D. Kurniawan, "Penerapan Metode Penetrasion Testing Pada Keamanan Jaringan Nirkabel," *Jurnal Responsif: Riset Sains Dan Informatika*, vol. 4, no. 2, pp. 162–167, 2022.

[4] A. T. Sitompul, F. Chahyadi, and Nurfalinda, "ANALISIS PENERAPAN METODE PENETRATION TESTING PADA KEAMANAN JARINGAN WLAN (Studi Kasus: Universitas Maritim Raja Ali Haji)," *Jurnal Sustainable: Jurnal Hasil Penelitian dan Industri Terapan*, vol. 12, pp. 23–29, May 2023.

[5] H. D. Sabdho and M. Ulfa, "Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang," in *Prosiding Seminar Hasil Penelitian Vokasi (Semhavok)*, 2018, pp. 15–24.

[6] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *Jurnal Informasi dan Teknologi*, pp. 160–165, 2022.

[7] K. Shravan, B. Neha, and B. Pawan, "Penetration Testing: A Review," *Compusoft*, vol. 3, no. 4, p. 752, 2014.

[8] M. A. Adiguna and B. W. Widagdo, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r)," *Jurnal SISKOM-KB (Sistem Komputer dan Kecerdasan Buatan)*, vol. 5, no. 2, pp. 1–8, 2022.

[9] H. Haeruddin and A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)," in *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, 2021, pp. 508–515.

[10] L. D. Samsumar and K. Gunawan, "Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram," *Jurnal Ilmiah Teknologi Infomasi Terapan*, vol. 4, no. 1, 2017.