JULIKOM
Jurnal Ilmu Komputer
Doi:
Web: https://journal.penus.or.id/index.php/julikom
Vol. 2, No. 3, Juni 2026
Hal. 71-78
E-ISSN: 3089-3194

ANALISIS KERENTANAN WPA2-PSK PADA JARINGAN WI-FI MENGGUNAKAN PENETRATION TESTING

Ilham Asy'ari[1*], Andi Saputra[2], Wawan Kurniawan[3]

[1]Program Studi Ilmu Komputer, Universitas Persada Bunda Indonesia
email: iamasyari@gmail.com

Abstrak

Jaringan Wi-Fi pada ruang publik menghadapi risiko akses tidak sah ketika protokol WPA2-PSK dikombinasikan dengan kata sandi yang lemah. Penelitian ini bertujuan mengidentifikasi konfigurasi jaringan Wi-Fi pada Cafe Saraja Coffee, mengevaluasi risiko serangan kamus terhadap autentikasi WPA2-PSK, serta merumuskan tindakan mitigasi. Metode yang digunakan adalah penetration testing dengan tahapan pengumpulan informasi, pemetaan jaringan, persiapan berkas 4-way handshake dalam lingkungan simulasi terkendali, pelaksanaan offline dictionary attack menggunakan Aircrack-ng, analisis paket menggunakan Wireshark, dan penilaian risiko. Identifikasi menunjukkan jaringan operasional menggunakan WPA2-Personal, router Huawei EG8141H5, dan repeater TP-Link WA885RE. Pada skenario simulasi, Aircrack-ng menemukan PSK 'password1' secara instan karena kata sandi tersebut tersedia dalam wordlist. Temuan ini menunjukkan bahwa kekuatan WPA2-PSK sangat bergantung pada entropi kata sandi dan bahwa pemrosesan offline memungkinkan percobaan dilakukan tanpa interaksi lanjutan dengan jaringan. Mitigasi prioritas meliputi kata sandi unik minimal 12 karakter, segmentasi jaringan internal dan tamu, aktivasi isolasi klien, pembaruan firmware, dan migrasi bertahap ke WPA3.

Kata Kunci : Aircrack-ng; keamanan jaringan; penetration testing; WPA2-PSK; Wi-Fi

Abstract

Public Wi-Fi networks face unauthorized-access risks when WPA2-PSK is combined with a weak password. This study aims to identify the Wi-Fi configuration at Cafe Saraja Coffee, evaluate the risk of dictionary attacks against WPA2-PSK authentication, and formulate mitigation measures. The penetration-testing method comprised information gathering, network mapping, preparation of a 4-way-handshake capture in a controlled simulation environment, an offline dictionary attack using Aircrack-ng, packet analysis using Wireshark, and risk assessment. The operational network was identified as using WPA2-Personal with a Huawei EG8141H5 router and a TP-Link WA885RE repeater. In the controlled scenario, Aircrack-ng recovered the PSK 'password1' instantly because it was contained in the supplied wordlist. The result demonstrates that WPA2-PSK resilience strongly depends on password entropy and that offline processing allows repeated attempts without further interaction with the target network. Priority mitigations include a unique password of at least 12 characters, separation of internal and guest networks, client isolation, regular firmware updates, and a phased migration to WPA3.

Keyword : *Aircrack-ng; network security; penetration testing; WPA2-PSK; Wi-Fi*

JULIKOM: Jurnal Ilmu Komputer E-ISSN: 3089-3194
Vol. 2, No. 3, Juni 2026, Hal. 71-78
DOI: xxxxxx
Available online at https://journal.penus.or.id/index.php/julikom/issue/view/8

PENDAHULUAN

Teknologi Wi-Fi menjadi infrastruktur penting bagi aktivitas pendidikan, bisnis, pemerintahan, dan layanan publik karena memungkinkan perangkat terhubung tanpa kabel secara fleksibel. Pada lingkungan kafe, layanan ini bukan hanya fasilitas tambahan, tetapi juga bagian dari pengalaman pelanggan dan pendukung operasional. Peningkatan jumlah pengguna dan perangkat memperluas permukaan serangan: sinyal dapat diterima di luar batas fisik organisasi, identitas pengguna sulit dikendalikan, serta lalu lintas internal berpotensi bercampur dengan akses publik. Kondisi tersebut menuntut pengelolaan keamanan yang tidak berhenti pada pemasangan kata sandi.

WPA2-Personal menggunakan Pre-Shared Key (PSK) sebagai dasar autentikasi. Protokol ini masih banyak digunakan karena kompatibel dengan perangkat lama, tetapi efektivitasnya sangat bergantung pada kualitas PSK, pengaturan router, dan pemisahan akses. Kata sandi yang umum, pendek, atau terkait nama tempat dapat dicocokkan menggunakan wordlist setelah penyerang memperoleh data autentikasi yang memadai. Kajian mengenai cracking WPA2 juga menunjukkan bahwa kata sandi lemah tetap menjadi faktor dominan dalam keberhasilan serangan [1]. Di sisi lain, teknik inspeksi jaringan nirkabel dapat membantu administrator menemukan konfigurasi dan perangkat yang tidak sesuai kebijakan [2].

Penetration testing digunakan untuk mengevaluasi keamanan melalui simulasi serangan yang terencana, terbatas, dan terdokumentasi. Pendekatan ini memberikan bukti teknis mengenai jalur serangan, dampak yang mungkin terjadi, dan prioritas perbaikan. Penelitian penerapan PTES pada jaringan nirkabel menekankan pentingnya fase pengumpulan informasi, analisis kerentanan, eksploitasi terkontrol, dan pelaporan [3]. Penelitian lain menunjukkan bahwa pengujian keamanan harus ditempatkan dalam tata kelola yang memuat izin, batas ruang lingkup, kriteria penghentian, dan perlindungan data [4], [5].

Objek penelitian adalah jaringan Wi-Fi di Cafe Saraja Coffee. Identifikasi awal pada skripsi menemukan SSID 'Hangtuah' dengan keamanan WPA2-Personal, router Huawei EG8141H5, dan repeater TP-Link WA885RE. Selain risiko PSK lemah, penggunaan satu segmen yang sama untuk pelanggan dan kebutuhan internal dapat memperbesar dampak apabila kredensial publik disalahgunakan. Segmentasi dibutuhkan agar kompromi pada jaringan tamu tidak langsung membuka jalur menuju perangkat operasional.

Penelitian ini tidak mengklaim melakukan pemecahan kata sandi terhadap jaringan operasional. Pengujian password cracking dilakukan secara offline pada berkas capture contoh yang memuat 4-way handshake dan SSID simulasi 'CEHLabs'. Pemisahan konteks tersebut penting agar interpretasi hasil tetap valid: keberhasilan uji menunjukkan risiko penggunaan kata sandi lemah pada WPA2-PSK, bukan bukti bahwa kredensial aktual Cafe Saraja Coffee telah diperoleh. Prinsip yang sama digunakan dalam praktik red teaming, yaitu menguji kontrol keamanan tanpa menimbulkan gangguan yang tidak perlu [6].

Berdasarkan permasalahan tersebut, penelitian bertujuan: (1) mengidentifikasi konfigurasi dan arsitektur jaringan Wi-Fi pada objek penelitian; (2) mengevaluasi risiko offline dictionary attack terhadap WPA2-PSK menggunakan Aircrack-ng; (3) menganalisis implikasi keamanan dari hasil pengujian; dan (4) menyusun rekomendasi mitigasi yang dapat diterapkan oleh pengelola jaringan. Kontribusi penelitian terletak pada penyajian bukti praktis mengenai hubungan antara kekuatan PSK, ketersediaan handshake, dan keberhasilan serangan kamus, disertai prioritas pengamanan bagi jaringan Wi-Fi publik.

METODE PENELITIAN

Desain dan Ruang Lingkup

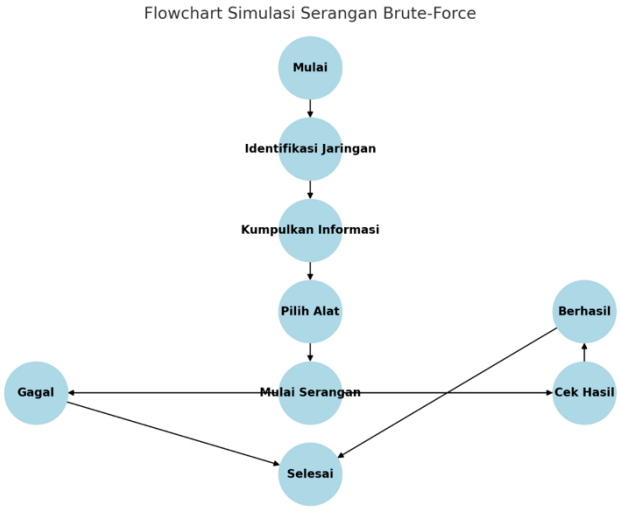
Penelitian menggunakan desain studi kasus deskriptif dengan metode penetration testing. Unit analisis meliputi konfigurasi akses nirkabel, perangkat penyusun jaringan, kebijakan akses, dan ketahanan autentikasi WPA2-PSK terhadap serangan kamus. Pengujian dibatasi pada aktivitas yang tidak merusak: identifikasi konfigurasi dilakukan terhadap jaringan objek, sedangkan proses cracking menggunakan bahan simulasi dalam lingkungan Kali Linux. Pendekatan ini menjaga ketersediaan layanan dan menghindari paparan kredensial operasional.

Data dikumpulkan melalui observasi konfigurasi, dokumentasi perangkat, identifikasi SSID dan tipe keamanan, analisis paket, serta pencatatan keluaran perangkat lunak. Aircrack-ng digunakan untuk memproses capture handshake dan wordlist; Wireshark digunakan untuk mengamati struktur lalu lintas jaringan. Metode serupa digunakan pada berbagai penelitian penetration testing untuk memperoleh bukti teknis yang dapat diterjemahkan menjadi rekomendasi [7]-[10].

JULIKOM: Jurnal Ilmu Komputer E-ISSN: 3089-3194
Vol. 2, No. 3, Juni 2026, Hal. 71-78
DOI: xxxxxx
Available online at https://journal.penus.or.id/index.php/julikom/issue/view/8

Tahap Penelitian

Tahapan penelitian terdiri atas enam kegiatan berurutan: identifikasi masalah, studi literatur, pengumpulan data, uji penetrasi, analisis data, dan penyusunan laporan. Alur tersebut ditunjukkan pada Gambar 1. Setiap tahap menghasilkan artefak pemeriksaan, mulai dari inventaris perangkat dan konfigurasi hingga bukti hasil simulasi serta daftar mitigasi.



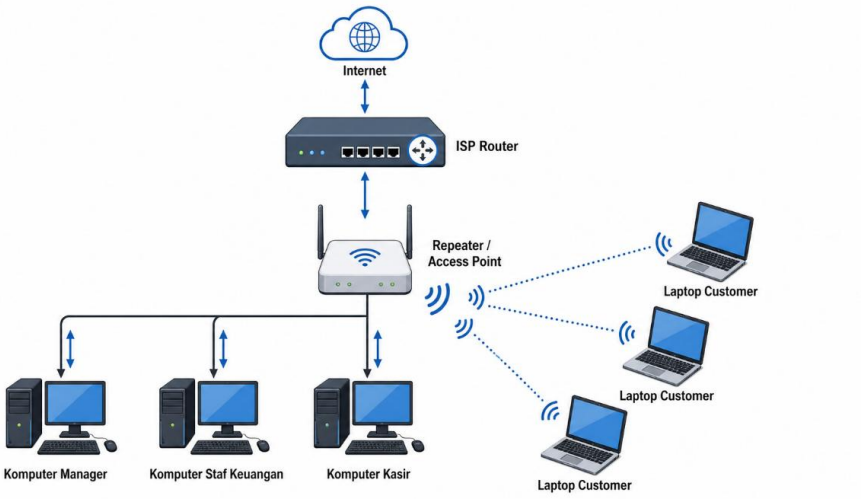
Gambar 1. Alur Simulasi Serangan Brute-Force

Lingkungan Pengujian

Tabel 1. Jenis Jenis Database

No.	Komponen	Fungsi
1	Huawei EG8141H5	Router dan gerbang utama akses internet
2	TP-Link WA885RE	Repeater/access point untuk memperluas jangkauan Wi-Fi
3	HP EliteBook 840 G7	Menjalankan lingkungan virtual dan alat pengujian
4	Kali Linux	Sistem operasi lingkungan simulasi terkendali
5	Aircrack-ng	Melakukan offline dictionary attack pada capture WPA2-PSK
6	Wireshark	Menginspeksi dan mendokumentasikan paket jaringan

Topologi jaringan menempatkan router sebagai gerbang internet dan repeater sebagai pemancar akses nirkabel kepada perangkat internal dan pelanggan. Gambar 2 memperlihatkan bahwa beberapa kategori pengguna secara konseptual berada pada infrastruktur yang sama. Kondisi ini menjadi dasar penilaian risiko segmentasi.



Gambar 2. Topologi Jaringan Pada Objek Penelitian

JULIKOM: Jurnal Ilmu Komputer E-ISSN: 3089-3194
Vol. 2, No. 3, Juni 2026, Hal. 71-78
DOI: xxxxxx
Available online at https://journal.penus.or.id/index.php/julikom/issue/view/8

Skenario dan Kriteria Evaluasi

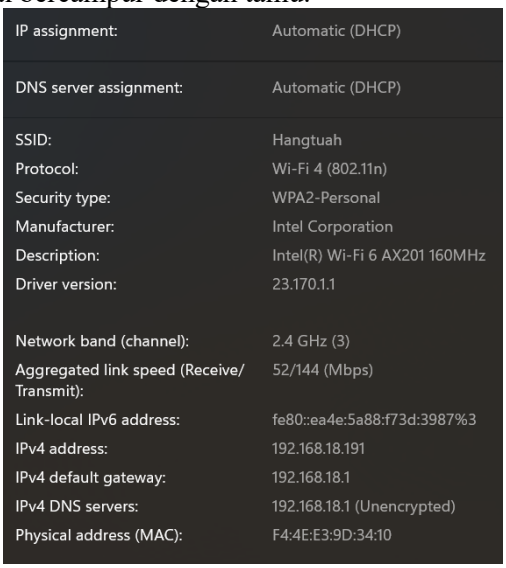
Skenario pengujian dibagi menjadi dua. Pertama, identifikasi pasif terhadap SSID, protokol keamanan, perangkat, kanal, alamat jaringan, dan struktur akses. Kedua, simulasi offline dictionary attack pada capture WPA2-PSK yang telah tersedia. Perintah pengujian menjalankan Aircrack-ng dengan wordlist dan berkas capture sebagai masukan. Tool menghitung kandidat PMK dan PTK untuk setiap entri, kemudian membandingkannya dengan nilai pada handshake sampai kandidat cocok ditemukan atau seluruh wordlist selesai diuji.

Evaluasi menggunakan empat kriteria: validitas handshake, jumlah kandidat yang diuji, waktu hingga PSK ditemukan, dan konsekuensi terhadap kerahasiaan serta kontrol akses. Tingkat risiko ditentukan secara kualitatif dari kombinasi kemungkinan eksploitasi dan dampak. Keberhasilan mendapatkan PSK dari wordlist dikategorikan sebagai risiko tinggi untuk kebijakan kata sandi; tidak adanya pemisahan jaringan internal dan tamu dikategorikan tinggi karena memperluas dampak setelah akses diperoleh.

HASIL DAN PEMBAHASAN

Hasil Identifikasi Jaringan

Identifikasi menunjukkan bahwa SSID operasional adalah 'Hangtuah' dengan protokol WPA2-Personal pada pita 2,4 GHz. Router memiliki alamat gateway 192.168.18.1 dan berfungsi sebagai DHCP server, sedangkan repeater memperluas cakupan sinyal. Informasi konfigurasi yang terekam ditunjukkan pada Gambar 3. Penggunaan WPA2-Personal lebih baik daripada jaringan terbuka, tetapi tidak otomatis menjamin keamanan ketika PSK mudah ditebak, antarmuka administrasi tidak diamankan, firmware tidak diperbarui, atau pengguna internal bercampur dengan tamu.



Gambar 3. Informasi Konfigurasi Jaringan Wi-Fi

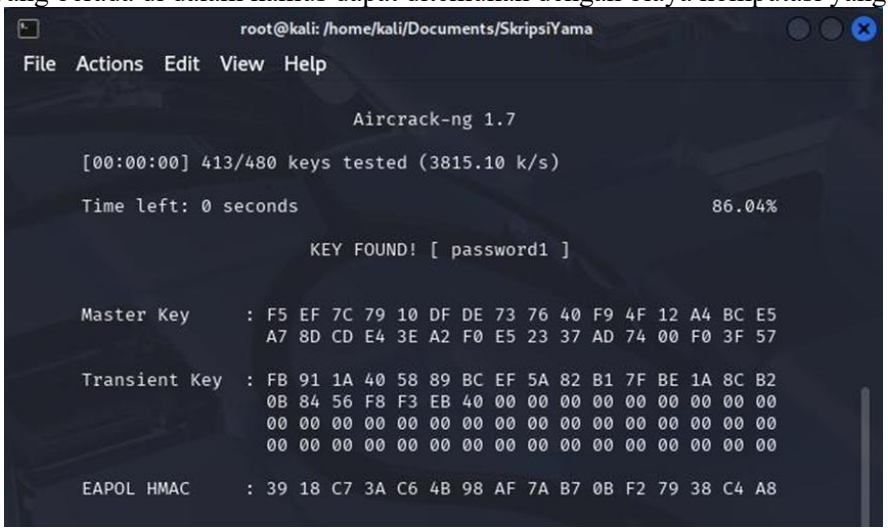
Arsitektur yang melayani komputer manajer, staf keuangan, kasir, dan laptop pelanggan melalui perangkat jaringan yang sama meningkatkan kebutuhan isolasi. Tanpa guest network, VLAN, atau pembatasan akses antar-klien, keberhasilan autentikasi ke jaringan publik dapat memperluas peluang pemindaian alamat internal, pengamatan layanan, atau penyalahgunaan koneksi. Temuan ini konsisten dengan penelitian tentang perancangan keamanan infrastruktur yang menempatkan segmentasi dan kontrol berlapis sebagai mekanisme mitigasi utama [11].

Hasil Simulasi Offline Dictionary Attack

Lingkungan simulasi menggunakan capture WPA2crack-01.cap yang berisi 4-way handshake valid untuk SSID 'CEHLabs' dan wordlist password.txt. Setelah kedua berkas dipastikan berada pada direktori kerja, Aircrack-ng memuat handshake dan menguji kandidat secara berurutan. Proses tidak membutuhkan interaksi berikutnya dengan access point karena verifikasi dilakukan secara offline. Karakteristik ini mengurangi peluang deteksi dari jaringan target setelah handshake tersedia.

JULIKOM: Jurnal Ilmu Komputer E-ISSN: 3089-3194
Vol. 2, No. 3, Juni 2026, Hal. 71-78
DOI: xxxxxx
Available online at https://journal.penus.or.id/index.php/julikom/issue/view/8

Aircrack-ng membaca 16.644 paket dan menampilkan satu target potensial dengan WPA handshake. Pada keluaran akhir, tool menguji 413 dari 480 kandidat dengan laju sekitar 3.815 kunci per detik dan menemukan PSK 'password1' pada waktu yang ditampilkan sebagai 0 detik. Gambar 4 memperlihatkan keluaran 'KEY FOUND!'. Hasil tersebut bukan ukuran universal kecepatan cracking karena dipengaruhi perangkat keras, ukuran wordlist, dan bentuk kata sandi; hasil ini secara khusus menunjukkan bahwa kandidat umum yang berada di dalam kamus dapat ditemukan dengan biaya komputasi yang sangat rendah.



Gambar 4. Aircrack-ng Menemukan PSK Yang Terdapat Dalam Wordlist

Tabel 2. Ringkasan Skenario Dan Hasil Pengujian

Tahap	Masukan/Observasi	Hasil
Identifikasi	SSID Hangtuah; WPA2-Personal; pita 2,4 GHz	Konfigurasi dasar berhasil dipetakan
Validasi capture	WPA2crack-01.cap; SSID CEHLabs	Satu 4-way handshake valid terdeteksi
Uji kamus	password.txt; 480 kandidat	413 kandidat diuji sebelum kunci ditemukan
Kinerja	Sekitar 3.815 kandidat/detik	Waktu tampilan 0 detik (instan)
Keluaran	PSK berada di dalam wordlist	KEY FOUND: password1
Interpretasi	Simulasi terkendali, bukan kredensial operasional	Membuktikan risiko PSK lemah pada WPA2

Analisis Kerentanan

Temuan utama adalah ketergantungan keamanan WPA2-PSK pada entropi PSK. Protokol menyediakan mekanisme kriptografi untuk membangun kunci sesi, tetapi penyerang dapat memanfaatkan handshake sebagai bahan verifikasi kandidat secara offline. Apabila PSK merupakan kata kamus, pola umum, atau variasi sederhana, ruang pencarian menyusut drastis. Hasil instan pada 'password1' menggambarkan kasus terburuk dari kebijakan kata sandi yang tidak mempertimbangkan prediktabilitas.

Keberhasilan uji tidak berarti setiap jaringan WPA2 dapat ditembus dalam waktu yang sama. Kata sandi acak yang panjang, tidak terdapat dalam wordlist, dan memiliki kombinasi karakter yang luas akan meningkatkan biaya serangan secara eksponensial. Oleh karena itu, ukuran keberhasilan dalam penelitian ini bukan klaim kelemahan algoritma WPA2 secara menyeluruh, melainkan bukti bahwa implementasi WPA2-PSK dengan PSK lemah tidak memberikan ketahanan memadai. Perbandingan WPA2 dan WPA3 juga menunjukkan bahwa penguatan protokol perlu disertai konfigurasi dan kebijakan kredensial yang benar [12].

Kerentanan kedua adalah luas dampak setelah autentikasi. Jika perangkat staf dan pelanggan berada pada broadcast domain atau kebijakan akses yang sama, kompromi kredensial tamu dapat menjadi titik awal pemetaan layanan internal. Segmentasi mengubah satu kegagalan autentikasi menjadi insiden yang terisolasi. Guest network perlu menerapkan client isolation, pembatasan akses ke jaringan privat, DNS yang aman, pembatasan bandwidth, dan pencatatan aktivitas yang proporsional.

JULIKOM: Jurnal Ilmu Komputer
E-ISSN: 3089-3194
Vol. 2, No. 3, Juni 2026, Hal. 71-78
DOI: xxxxxx
Available online at https://journal.penus.or.id/index.php/julikom/issue/view/8

Kerentanan ketiga berkaitan dengan siklus hidup perangkat. Router dan repeater harus menerima pembaruan firmware, menonaktifkan WPS jika tidak diperlukan, mengganti kredensial administrasi bawaan, membatasi antarmuka manajemen hanya dari jaringan internal, dan menggunakan konfigurasi enkripsi terkuat yang kompatibel. Serangan terhadap implementasi WPA pada perangkat klien memperlihatkan bahwa keamanan tidak hanya bergantung pada access point, tetapi juga pada perangkat lunak supplicant dan pembaruannya [13].

Pembahasan dan Implikasi

Hasil penelitian memperkuat temuan studi penetration testing nirkabel bahwa pengumpulan informasi dan validasi konfigurasi perlu dilakukan sebelum eksploitasi terkontrol [3]. Pendekatan bertahap menghindari interpretasi yang hanya berpusat pada keberhasilan tool. Dalam kasus ini, keluaran Aircrack-ng menjadi bukti teknis, sedangkan keputusan pengamanan ditentukan oleh konteks bisnis: kafe memiliki pengguna sementara, perangkat internal yang bernilai, kebutuhan ketersediaan tinggi, dan kapasitas administrasi yang terbatas.

Dari perspektif kerahasiaan, PSK lemah membuka kemungkinan pihak tidak berwenang menggunakan koneksi dan mengamati layanan yang dapat dijangkau. Dari perspektif integritas, akses ke segmen internal dapat memberi peluang perubahan konfigurasi atau gangguan terhadap perangkat yang tidak terlindungi. Dari perspektif ketersediaan, penyalahgunaan bandwidth dan perubahan konfigurasi router dapat mengganggu layanan kasir serta pengalaman pelanggan. Karena itu, perbaikan harus memprioritaskan kontrol yang mengurangi kemungkinan sekaligus dampak.

Penelitian ini juga menegaskan keterbatasan penggunaan waktu cracking sebagai satu-satunya indikator. Hasil 0 detik terjadi karena PSK berada di dalam wordlist yang kecil; angka tersebut tidak dapat digeneralisasi ke kata sandi acak. Metrik yang lebih tepat adalah keberadaan kata sandi dalam korpus umum, panjang dan keunikan PSK, laju percobaan, serta estimasi ruang pencarian. Penelitian lanjutan dapat menggunakan beberapa kelas PSK dan mengukur distribusi waktu pada perangkat keras yang sama.

Keterbatasan lain adalah penggunaan sample capture untuk tahap cracking, sehingga penelitian tidak mengukur langsung ketahanan PSK operasional, jangkauan serangan, maupun efektivitas monitoring pada objek. Selain itu, belum dilakukan pengujian VLAN, client isolation, WPS, antarmuka administrasi router, WPA3-SAE, rogue access point, atau deauthentication. Keterbatasan ini tidak menghapus nilai demonstrasi, tetapi membatasi kesimpulan pada risiko offline dictionary attack terhadap WPA2-PSK dengan kata sandi lemah.

Rekomendasi Mitigasi

Tabel 3. Prioritas Risiko Dan Rekomendasi Mitigasi

Risiko	Tingkat	Rekomendasi Utama
PSK lemah atau umum	Tinggi	Gunakan PSK unik >=12 karakter; hindari nama tempat/pola kamus; rotasi saat terindikasi bocor
Jaringan internal dan tamu menyatu	Tinggi	Aktifkan guest network/VLAN, blok akses ke subnet internal, dan aktifkan client isolation
Kredensial admin bawaan/WPS	Tinggi	Ganti akun admin, nonaktifkan WPS, batasi manajemen dari segmen internal
Firmware tidak mutakhir	Sedang	Inventaris versi dan lakukan pembaruan berkala dengan prosedur pencadangan
Monitoring terbatas	Sedang	Tinjau log, perangkat terhubung, kegagalan autentikasi, dan perubahan konfigurasi
Ketergantungan WPA2	Sedang	Migrasi bertahap ke WPA3-SAE; gunakan mode transisi hanya selama diperlukan

Urutan implementasi disusun berdasarkan kemudahan dan dampak. Penggantian PSK serta pemisahan jaringan dapat dilakukan dengan biaya relatif rendah dan segera menurunkan risiko. Pengelola sebaiknya membuat PSK internal yang tidak dibagikan kepada pelanggan, sementara guest network menggunakan kredensial berbeda dan dapat dirotasi sesuai kebutuhan. Migrasi WPA3 dilakukan setelah

E-ISSN: 3089-3194

memastikan dukungan perangkat; perangkat lama yang tidak mendukung harus ditempatkan pada segmen dengan hak akses minimum.

Pengujian ulang perlu dilakukan setelah mitigasi untuk memastikan kontrol bekerja. Verifikasi mencakup akses tamu ke subnet internal, client-to-client communication, status WPS, keamanan halaman administrasi, versi firmware, serta upaya kamus pada PSK uji yang mewakili kebijakan baru. Hasil uji ulang menjadi baseline bagi audit berikutnya dan membantu pengelola membedakan antara kontrol yang sudah diterapkan dan kontrol yang benar-benar efektif.

KESIMPULAN

Penetration testing berhasil digunakan untuk memetakan konfigurasi jaringan Wi-Fi dan mendemonstrasikan risiko offline dictionary attack terhadap WPA2-PSK. Jaringan objek menggunakan WPA2-Personal dengan router Huawei EG8141H5 dan repeater TP-Link WA885RE. Pada simulasi terkendali, Aircrack-ng menemukan PSK 'password1' secara instan setelah menguji 413 dari 480 kandidat karena PSK tersebut berada dalam wordlist. Hasil ini membuktikan bahwa penggunaan WPA2-Personal tidak cukup apabila kata sandi bersifat umum dan mudah diprediksi.

Kesimpulan tidak diperluas menjadi klaim bahwa kredensial operasional Cafe Saraja Coffee berhasil dipecahkan, karena tahap cracking menggunakan sample capture untuk SSID simulasi. Risiko aktual yang dapat ditarik adalah lemahnya PSK memungkinkan verifikasi kandidat secara offline setelah handshake tersedia. Dampak menjadi lebih besar bila pengguna internal dan pelanggan berada pada jaringan yang sama.

Mitigasi prioritas adalah mengganti PSK dengan kata sandi unik minimal 12 karakter, memisahkan jaringan internal dan tamu, mengaktifkan client isolation, menonaktifkan WPS, mengamankan antarmuka administrasi, memperbarui firmware, meninjau log secara berkala, dan merencanakan migrasi ke WPA3-SAE. Penelitian lanjutan disarankan melakukan pengujian terotorisasi pada lingkungan uji yang mereplikasi topologi objek, membandingkan beberapa kelas PSK, serta mengevaluasi efektivitas segmentasi dan WPA3

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Lancang Kuning, pembimbing penelitian, serta pengelola Cafe Saraja Coffee yang telah mendukung proses observasi dan penyusunan penelitian ini.

DAFTAR PUSTAKA

[1] R. Sari, 'Analisis serangan cracking WPA2 pada jaringan Wi-Fi di perusahaan,' Jurnal Keamanan Data, vol. 6, no. 1, pp. 50-58, 2021.

[2] M. Purweni, D. Hariyadi, F. E. Nastiti, and F. Fazlurrahman, 'Model inspeksi keamanan jaringan nirkabel dengan teknik wardriving berbasis chatbot,' Jurnal Komtika, vol. 6, no. 2, pp. 83-90, 2022, doi: 10.31603/komtika.v6i2.7943.

[3] B. Parga Zen, S. G. Saputra, and Abdurahman, 'Analisis keamanan jaringan wireless menggunakan metode Penetration Testing Execution Standard (PTES),' Jurnal Sistem Informasi Galuh, vol. 1, no. 2, pp. 43-51, 2023, doi: 10.25157/jsig.v1i2.3152.

[4] F. Fattah, A. M. Putri, and H. Azis, 'Implementasi metode penetration testing pada layanan keamanan sistem kartu transaksi elektronik wahana permainan,' Techno.Com, vol. 23, no. 1, 2024, doi: 10.62411/tc.v23i1.9488.

[5] D. R. Dasmen, Rasmila, T. L. Widodo, K. Kundari, and M. T. Farizky, 'Pengujian penetrasi pada website elearning2.binadarma.ac.id dengan metode PTES,' J-ICON, vol. 11, no. 1, pp. 91-95, 2023, doi: 10.35508/jicon.v11i1.9809.

E-ISSN: 3089-3194

[6] S. Yulianto, B. Soewito, F. L. Gaol, and A. Kurniawan, 'The crucial role of red teaming: Strengthening Indonesia's cyber defenses through cybersecurity drill tests,' International Journal of Safety and Security Engineering, vol. 14, no. 4, pp. 1231-1242, 2024, doi: 10.18280/ijsse.140420.

[7] G. Suprianto, 'Penetration testing pada sistem informasi jabatan Universitas Hayam Wuruk Perbanas,' InComTech, vol. 12, no. 2, pp. 129-138, 2022, doi: 10.22441/incomtech.v12i2.15093.

[8] Y. A. Pohan, 'Meningkatkan keamanan webserver aplikasi pelaporan pajak daerah menggunakan metode Penetration Testing Execution Standard,' Jurnal Sistim Informasi dan Teknologi, vol. 3, no. 1, pp. 1-6, 2021, doi: 10.37034/jsisfotek.v3i1.36.

[9] F. Fachri, 'Optimasi keamanan web server terhadap serangan brute-force menggunakan penetration testing,' Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 10, no. 1, pp. 51-58, 2023, doi: 10.25126/jtiik.20231015872.

[10] R. T. N. Yamin, I. M. A. D. Suarjaya, and I. P. A. E. Pratama, 'Penetration testing on the SISAKTI application at Udayana University using the OWASP Testing Guide Version 4,' Jurnal Ilmiah Merpati, vol. 10, no. 3, p. 155, 2022, doi: 10.24843/JIM.2022.v10.i03.p04.

[11] P. A. Khairunnisa, N. Annisa, Yukandri, and J. P., 'Perancangan sistem keamanan jaringan berbasis cybersecurity untuk mitigasi ancaman siber pada infrastruktur TI: Studi kasus di Indonesia,' Jurnal Ilmu Teknik dan Informatika, vol. 3, no. 1, 2024, doi: 10.51903/teknik.v3i1.570.

[12] Y. Mulyanto, H. Herfandi, and R. C. Kirana, 'Analisis keamanan wireless local area network (WLAN) terhadap serangan brute force dengan metode penetration testing,' JINTEKS, vol. 4, no. 1, pp. 26-35, 2022, doi: 10.51401/jinteks.v4i1.1528.

[13] N. Trianto, D. F. Priambodo, and D. A. Insani, 'Implementasi KRACK dan KRACK Detector terhadap wpa_supplicant pada perangkat Android dan Linux Ubuntu,' Jurnal Teknologi Informasi dan Komunikasi, vol. 10, no. 2, p. 1, 2022, doi: 10.30646/tikomsin.v10i2.639.