ANALISIS PERBANDINGAN KEAMANAN PROTOKOL WIFI WPA2 DAN WPA3 MELALUI PENETRASI AKTIF DAN PASIF

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana Program Studi S1 Teknik Komputer

disusun oleh

AZIZ SYAIFUL HAMZAH

18.83.0225

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

ANALISIS PERBANDINGAN KEAMANAN PROTOKOL WIFI WPA2 DAN WPA3 MELALUI PENETRASI AKTIF DAN PASIF

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana Program Studi S1 Teknik Komputer

disusun oleh

AZIZ SYAIFUL HAMZAH

18.83.0225

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERBANDINGAN KEAMANAN PROTOKOL WIFI WPA2 DAN WPA3 MELALUI PENETRASI AKTIF DAN PASIF

yang disusun dan diajukan oleh

Aziz Syaiful Hamzah

18.83.0225

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 7 November 2024

Dosen Pembimbing,

Wahid Miftahul Ashari, S.Kom.,M.T.

NIK. 190302452

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS PERBANDINGAN KEAMANAN PROTOKOL WIFI WPA2 DAN WPA3 MELALUI PENETRASI AKTIF DAN PASIF

yang disusun dan diajukan oleh
Aziz Syaiful Hamzah
18.83.0225

Telah dipertahankan di depan Dewan Penguji
pada tanggal 21 Januari 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, M.Kom. **NIK. 190302456**	
Melwin Syafrizal, S.Kom.,M.Eng. **NIK. 190302105**	
Wahid Miftahul Ashari, **NIK. 190302452**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 24 Januari 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof.Dr Kusrini, M.Kom
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Aziz Syaiful Hamzah
NIM : 18.83.0225

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS PERBANDINGAN KEAMANAN PROTOKOL WIFI WPA2 DAN WPA3 MELALUI PENETRASI AKTIF DAN PASIF

Dosen Pembimbing : Wahid Miftahul Ashari, S.Kom.,M.T

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 24 Februari 2025

Yang Menyatakan,

Aziz Syaiful Hamzah

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat, hidayah, dan karunia-Nya yang melimpah. Dalam kesempatan ini, penulis ingin menyampaikan rasa syukur dan terima kasih yang setinggi-tingginya kepada semua pihak yang telah memberikan dukungan, bantuan, dan kontribusi dalam penyelesaian skripsi ini.

Pertama-tama, penulis mengucapkan terima kasih yang tak terhingga kepada Wahid Miftahul Ashari, S.Kom.,M.T. sebagai pembimbing skripsi penulis. Terima kasih atas bimbingan, pengarahan, dan pengawasan yang luar biasa selama proses penelitian dan penulisan skripsi ini. Wahid Miftahul Ashari, S.Kom.,M.T. telah memberikan panduan yang sangat berharga, wawasan yang mendalam, dan dorongan yang tak terhingga bagi penulis dalam menyelesaikan skripsi ini.

Akhir kata, penulis menyampaikan permohonan maaf apabila terdapat kekurangan dalam penulisan skripsi ini. Penulis dengan tulus menerima kritik dan saran yang membangun untuk peningkatan di masa mendatang.

Yogyakarta, 27 Juni 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMBANG DAN SINGKATAN

Ω	Tahanan Listrik
μ	Konstanta gesekan
ANFIS	Adaptive Network Fuzzy Inference System
SVM	Support Vector Machines

DAFTAR ISTILAH

Brute Force	Teknik serangan keamanan yang mencoba semua kemungkinan kombinasi kata sandi atau kunci enkripsi hingga menemukan yang benar.
Dictionary Attack	Jenis serangan keamanan yang mencoba kata sandi yang umum atau kata sandi yang terdapat dalam daftar kata (dictionary) untuk mendapatkan akses tidak sah ke sistem.
TCP (*Transmission Control Protocol*)	Salah satu protokol utama dalam protokol internet yang mengatur pengiriman data antara komputer melalui jaringan.
MHz (*Megahertz*)	Satuan frekuensi yang digunakan untuk mengukur kecepatan prosesor atau frekuensi sinyal radio, setara dengan satu juta siklus per detik.
WLAN (*Wireless Local Area Network*)	Jaringan area lokal yang menggunakan teknologi nirkabel untuk menghubungkan perangkat.
Aircrack-ng	Suite perangkat lunak untuk mengaudit keamanan jaringan WiFi, yang memiliki kemampuan untuk menangkap paket data dan melakukan berbagai jenis serangan pada jaringan nirkabel.
AES (*Advanced Encryption Standard*)	Standar enkripsi yang digunakan untuk mengamankan data, dikenal karena keamanannya yang kuat dan digunakan dalam banyak aplikasi keamanan.

IoT (*Internet of Things*)	Konsep di mana perangkat sehari-hari dilengkapi dengan kemampuan internet untuk mengumpulkan dan bertukar data.
SSID (*Service Set Identifier*)	Nama unik yang mengidentifikasi jaringan WiFi tertentu
Throughput	Jumlah data yang dapat dikirim melalui jaringan dalam periode waktu tertentu, biasanya diukur dalam bits per second (bps).
PMF (*Protected Management Frames*)	Fitur keamanan dalam jaringan WiFi yang melindungi frame manajemen dari serangan, memastikan keaslian dan integritas komunikasi.

INTISARI

Jaringan WiFi saat ini penting dalam kehidupan sehari-hari karena kemudahan dan fleksibilitasnya, namun keamanannya menjadi perhatian utama mengingat penggunaannya untuk mengirim data sensitif. Protokol keamanan seperti WPA, WPA2, dan WPA3 telah berkembang untuk mengatasi masalah ini. Penelitian ini membandingkan keamanan antara WPA2 dan WPA3 melalui penetrasi aktif dan pasif. Penetrasi aktif mencakup uji coba serangan langsung untuk mengidentifikasi kerentanan potensial, sementara penetrasi pasif melibatkan pemantauan lalu lintas jaringan tanpa intervensi langsung. Hasil penelitian menunjukkan bahwa WPA3 lebih tahan terhadap serangan dibandingkan WPA2. WPA2 terbukti rentan terhadap serangan brute force dan alat seperti Aircrack-ng, sementara WPA3 menunjukkan ketahanan yang lebih tinggi dengan tidak adanya upaya yang berhasil untuk memperoleh kata sandi. Pendekatan penetrasi pasif juga menunjukkan bahwa WPA3 tidak memiliki kerentanan signifikan yang ditemukan pada WPA2, seperti serangan offline terhadap handshake. Studi ini merekomendasikan implementasi WPA3 sebagai prioritas serta pembaruan rutin perangkat keras dan perangkat lunak untuk meningkatkan keamanan jaringan WiFi. Temuan ini memberikan panduan berharga bagi pengguna dalam memilih protokol keamanan yang tepat dan berkontribusi pada pengembangan keamanan jaringan di masa depan.

Kata Kunci: jaringan WiFi, WPA2, WPA3, penetrasi aktif, penetrasi pasif, keamanan jaringan

ABSTRACT

WiFi networks are essential in daily life due to their convenience and flexibility, yet their security is a major concern given their use for transmitting sensitive data. Security protocols like WPA, WPA2, and WPA3 have evolved to address these issues. This study compares the security of WPA2 and WPA3 through active and passive penetration testing. Active penetration involves direct attack attempts to identify potential vulnerabilities, while passive penetration monitors network traffic without direct intervention. Research findings indicate that WPA3 is more resilient to attacks compared to WPA2. WPA2 has been shown vulnerable to brute force attacks and tools like Aircrack-ng, whereas WPA3 demonstrates higher resilience with no successful attempts to obtain passwords. The passive penetration approach also reveals that WPA3 lacks significant vulnerabilities found in WPA2, such as offline attacks on handshakes. The study recommends prioritizing the implementation of WPA3 and regularly updating hardware and software to enhance WiFi network security. These findings provide valuable guidance for users in selecting appropriate security protocols and contribute to future network security development.

Keywords: WiFi networks, WPA2, WPA3, active penetration, passive penetration, network security