ANALISIS KEAMANAN JARINGAN WPA2 TERHADAP SERANGAN BRUTE FORCE DAN PACKET SNIFFING DENGAN METODE PENETRATION TESTING

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

Fahrudin Nur Latif

21.83.0666

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

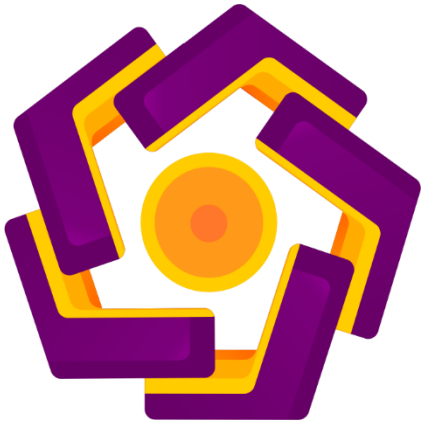
2025

ANALISIS KEAMANAN JARINGAN WPA2 TERHADAP SERANGAN BRUTE FORCE DAN PACKET SNIFFING DENGAN METODE PENETRATION TESTING

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer



disusun oleh

Fahrudin Nur Latif

21.83.0666

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KEAMANAN JARINGAN WPA2 TERHADAP SERANGAN BRUTE FORCE DAN PACKET SNIFFING DENGAN METODE PENETRATION TESTING

yang disusun dan diajukan oleh

Fahrudin Nur Latif

21.83.0666

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 8 Juli 2025

Dosen Pembimbing,

Muhammad Koprawi, S.Kom, M.Eng
NIK. 190302454

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS KEAMANAN JARINGAN WPA2 TERHADAP SERANGAN BRUTE FORCE DAN PACKET SNIFFING DENGAN METODE PENETRATION TESTING

yang disusun dan diajukan oleh

Fahrudin Nur Latif

21.83.0666

Telah dipertahankan di depan Dewan Penguji
pada tanggal 24 Juli 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dr. Dony Ariyus, S.S., M.Kom. **NIK. 190302128**	
Wahid Miftahul Ashari, S.Kom., M.T. **NIK. 190302452**	
Muhammad Koprawi ,S.Kom, M.Eng. **NIK. 190302454**	

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

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Fahrudin Nur Latif
NIM : 21.83.0666

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Keamanan Jaringan WPA2 Terhadap Serangan Brute Force dan Packet Sniffing Dengan Metode Penetration Testing

Dosen Pembimbing : Muhammad Koprawi, S.Kom, M.Eng

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 Juli 2025

Yang Menyatakan,

Fahrudin Nur Latif

HALAMAN PERSEMBAHAN

Puji syukur saya panjatkan ke hadirat Tuhan Yang Maha Esa atas segala limpahan rahmat dan karunia-Nya, sehingga skripsi ini dapat diselesaikan dengan baik. Dengan penuh kerendahan hati, saya persembahkan karya ini kepada:

1. Orang tua tercinta, yang selalu menjadi sumber kekuatan dan inspirasi dalam setiap langkah kehidupan saya. Doa, dukungan, serta kasih sayang yang tak terhingga dari mereka adalah landasan utama keberhasilan saya menuntaskan pendidikan ini. Segala nasihat dan semangat yang mereka berikan selalu menjadi penyemangat dalam perjalanan akademik saya.
2. Keluarga besar, yang senantiasa memberikan dorongan moral dan perhatian tulus dalam berbagai bentuk. Kehadiran dan dukungan mereka menjadi sumber motivasi saat menghadapi berbagai tantangan, serta tempat berbagi kebahagiaan atas pencapaian yang diraih.
3. Dosen pembimbing dan penguji, yang dengan sabar dan tulus membimbing serta memberikan arahan yang sangat berarti selama proses penyusunan skripsi ini. Setiap masukan dan koreksi yang diberikan sangat membantu dalam penyempurnaan penelitian ini. Saya mengucapkan terima kasih yang sebesar-besarnya atas ilmu dan bimbingan yang telah diberikan.
4. Teman-teman seperjuangan, yang telah menjadi bagian penting dalam perjalanan akademik saya. Kebersamaan, dukungan, dan semangat yang mereka berikan menjadi motivasi agar saya terus berusaha sampai mencapai titik akhir ini.
5. Almamater tercinta, tempat saya menimba ilmu dan mengembangkan kemampuan, sehingga saya dapat menjadi pribadi yang lebih baik. Semoga ilmu yang saya peroleh dapat memberikan manfaat bagi masyarakat luas dan dunia pendidikan.

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Allah SWT. Berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan skripsi yang berjudul "Analisis Keamanan Jaringan WPA2 Terhadap Serangan Brute Force dan Packet Sniffing Dengan Metode Penetration Testing".

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Jurusan Teknik Komputer, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta.

Penulisan skripsi ini didasarkan pada data yang diperoleh dari studi literatur, hasil percobaan, serta bimbingan dari dosen pembimbing. Penyelesaian skripsi ini tidak terlepas dari bantuan dan dukungan berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Prof. Dr. Kusrini, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
3. Bapak Muhammad Koprawi, S.Kom., M.Eng., selaku dosen pembimbing skripsi yang telah memberikan bimbingan, arahan, dan motivasi selama proses penyusunan skripsi ini.
4. Dosen penguji, yang telah meluangkan waktu untuk memberikan masukan dan evaluasi yang sangat berharga demi kesempurnaan skripsi ini.
5. Bapak dan Ibu Dosen atas bimbingan dan ilmu yang telah diberikan selama proses perkuliahan.
6. Kedua Orang Tua tercinta, yang selalu memberikan kasih sayang, dan dukungan tanpa henti selama perjalanan studi ini.
7. Kedua Kakak tercinta, yang selalu memberikan semangat, doa, dan dukungan selama perjalanan studi ini.
8. Teman seperjuangan 21TK02 atas segala kebersamaan selama menempuh masa studi.

9. Sahabat-sahabat terbaik yang selalu memberikan semangat, motivasi, dan kebersamaan yang berarti dalam setiap langkah.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan dan belum mencapai kesempurnaan. Oleh karena itu, dengan penuh kerendahan hati, penulis sangat mengharapkan kritik dan saran yang membangun dari para pembaca sebagai bahan evaluasi untuk perbaikan dan penyempurnaan karya ini di masa yang akan datang. Semoga skripsi ini dapat memberikan manfaat yang berarti serta menjadi kontribusi positif bagi pengembangan ilmu pengetahuan dan memberikan manfaat bagi masyarakat luas dan dunia pendidikan.

Yogyakarta, 24 Juli 2025
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

WiFi	:	Wireless Fidelity
LAN	:	Local Area Network
WAN	:	Wide Area Network
HTTP	:	HyperText Transfer Protocol
HTTPS	:	HyperText Transfer Protocol Secure
TCP/IP	;	Transmission Control Protocol / Internet Protocol
UDP	:	User Datagram Protocol
WPA2	:	Wi-Fi Protected Access 2
ARP	:	Address Resolution Protocol
MAC	:	Media Access Control
MITM	:	Man-In-The-Middle
VPN	:	Virtual Private Network
TLS	:	Transport Layer Security
IP	:	Internet Protocol
PCAP	:	Packet Capture
OS	:	Operating System
SAE	:	Simultaneous Authentication of Equals

DAFTAR ISTILAH

Jaringan Komputer	Kumpulan komputer yang terhubung untuk berbagi data.
Jaringan WiFi	Jaringan nirkabel menggunakan gelombang radio.
Keamanan Jaringan	Perlindungan jaringan dari ancaman.
Packet Sniffing	Penyadapan data jaringan tanpa izin.
Passive Sniffing	Merekam data tanpa mengubah paket.
Active Sniffing	Memanipulasi protokol untuk mengalihkan data.
Wireshark	Software untuk menangkap paket data.
Ettercap	Software untuk serangan sniffing dan MitM.
ARP Spoofing	Mengirim ARP palsu untuk mengaitkan MAC dan IP.
Man-in-the-Middle	Menyadap dan manipulasi komunikasi.
Enkripsi WPA2	Standar enkripsi utama WiFi.
Protokol HTTP	Protokol web tanpa enkripsi.
Protokol HTTPS	HTTP dengan enkripsi TLS/SSL.
Vulnerability Scanning	Pemindaian untuk cari celah keamanan.
Firewall Rule	Aturan kontrol lalu lintas jaringan.
VirtualBox	Software virtualisasi lingkungan simulasi.
Open Network	Jaringan WiFi tanpa enkripsi.
Password Shared	Password sama untuk semua pengguna.
Payload	Data sebenarnya dalam paket.
Header Paket	Info kontrol paket data.
Penetration Testing	Simulasi serangan untuk uji keamanan.
System Failure Attack	Serangan yang menyebabkan sistem gagal.
Trojan dan Malware	Program berbahaya pencuri data.

INTISARI

Perkembangan teknologi informasi yang pesat menjadikan jaringan WiFi sebagai kebutuhan utama dalam berbagai aktivitas. Namun demikian, masih banyak jaringan Wi-Fi, khususnya di lingkungan tempat tinggal bersama seperti rumah kos, yang belum menerapkan konfigurasi keamanan secara optimal. Protokol WPA2 yang umum digunakan masih menyisakan celah keamanan, yang rentan dieksploitasi melalui serangan brute force dan packet sniffing. Kondisi ini dapat mengakibatkan kebocoran data sensitif serta membuka peluang akses tidak sah oleh pihak yang tidak berwenang.

Penelitian ini menggunakan metode penetration testing dengan pendekatan deskriptif kualitatif untuk mengidentifikasi dan menganalisis tingkat kerentanan jaringan Wi-Fi terhadap dua jenis serangan, yaitu brute force dan packet sniffing. Teknik brute force diterapkan untuk menguji kekuatan kata sandi jaringan menggunakan pendekatan dictionary attack, sedangkan teknik packet sniffing dilakukan untuk mengamati lalu lintas jaringan dan mengidentifikasi potensi kebocoran informasi, terutama pada protokol HTTP dan HTTPS. Penelitian dilakukan pada jaringan Wi-Fi di lingkungan kos peneliti yang menggunakan protokol WPA2.

Hasil penelitian menunjukkan bahwa jaringan Wi-Fi yang diuji berhasil dibobol melalui serangan brute force, menandakan lemahnya sistem autentikasi yang diterapkan. Selain itu, data sensitif seperti username dan password pada protokol HTTP dapat disadap dengan mudah, sedangkan komunikasi pada protokol HTTPS terlindungi oleh enkripsi TLS. Temuan ini menunjukkan pentingnya penggunaan protokol yang aman dan penguatan kebijakan keamanan jaringan. Penelitian ini dapat dimanfaatkan oleh pengelola jaringan, pengguna Wi-Fi, dan praktisi keamanan siber sebagai dasar dalam meningkatkan perlindungan terhadap jaringan lokal. Penelitian lanjutan disarankan untuk mengevaluasi efektivitas protokol WPA3 serta implementasi sistem deteksi intrusi sebagai langkah preventif terhadap serangan.

Kata Kunci : Keamanan Jaringan, WPA2, Brute Force, Packet Sniffing, Penetration Testing

ABSTRACT

The rapid advancement of information technology has made Wi-Fi networks an essential component in various daily activities. However, many Wi-Fi networks—particularly those in shared living environments such as boarding houses—still lack optimal security configurations. The widely adopted WPA2 protocol continues to present vulnerabilities that can be exploited through brute force and packet sniffing attacks. These conditions may lead to the leakage of sensitive data and unauthorized access by malicious actors.

This research employs a penetration testing method with a descriptive qualitative approach to identify and analyze the level of vulnerability of Wi-Fi networks to two specific attack types: brute force and packet sniffing. The brute force technique was used to test the strength of the Wi-Fi password through a dictionary attack approach, while packet sniffing was performed to monitor network traffic and detect potential information leakage, particularly over HTTP and HTTPS protocols. The testing was conducted on a WPA2-based Wi-Fi network in the researcher's boarding house environment.

The results indicate that the Wi-Fi password was successfully cracked using a brute force attack, revealing the weakness of the network's authentication system. Moreover, sensitive data such as usernames and passwords transmitted over HTTP could be easily intercepted, while HTTPS communications remained protected through TLS encryption. These findings highlight the importance of using secure communication protocols and strengthening network security policies. The research may serve as a reference for network administrators, Wi-Fi users, and cybersecurity practitioners in enhancing the protection of local wireless networks. Further research is recommended to evaluate the effectiveness of WPA3 and to explore the implementation of intrusion detection systems as a preventive measure.

Keywords : Network Security, WPA2, Brute Force, Packet Sniffing, Penetration Testing