ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN *PACKET SNIFFING* DI PENGINAPAN LA TULIP

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

Nur widiyanto

20.11.3456

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN *PACKET SNIFFING* DI PENGINAPAN LA TULIP

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

Nur widiyanto

20.11.3456

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN *PACKET SNIFFING* DI PENGINAPAN LA TULIP

yang disusun dan diajukan oleh

Nur Widiyanto

20.11.3456

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 12 Februari 2025

Dosen Pembimbing,

Lukman, S.Kom., M.Kom.

NIK. 190302151

HALAMAN PENGESAHAN

SKRIPSI
ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN *PACKET SNIFFING* DI PENGINAPAN LA TULIP

yang disusun dan diajukan oleh

Nur Widiyanto

20.11.3456

Telah dipertahankan di depan Dewan Penguji
pada tanggal 12 februari 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Agung Pambudi, ST, MA **NIK. 190302012**	
Yudi Sutanto M.Kom. **NIK. 190302039**	
Lukman, S.Kom., M.Kom. **NIK. 190302151**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 12 Februari 2025

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta,S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Nur Widiyanto
NIM : 20.11.3456

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Keamanan Jaringan (Wifi) Terhadap Serangan *Packet Sniffing* Di Penginapan La Tulip

Dosen Pembimbing : Lukman, S.Kom., M.Kom.

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,12 Februari 2025

Yang Menyatakan,

Nur Widiyanto

HALAMAN PERSEMBAHAN

Skripsi ini dipersembahkan kepada orang tua dan keluarga yang telah memberikan doa, dukungan, kepada dosen pembimbing serta seluruh pengajar yang telah memberikan bimbingan dan pengetahuan selama proses studi, kepada rekan-rekan dan teman-teman seperjuangan di Universitas Amikom Yogyakarta yang telah memberikan semangat dan dukungan, serta kepada seluruh pihak di Penginapan La Tulip yang telah memberikan kesempatan dan dukungan selama pelaksanaan penelitian. Semoga karya ini dapat memberikan manfaat dan menjadi langkah awal untuk kontribusi yang lebih signifikan di masa depan.

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini dengan judul "Analisis Keamanan Jaringan (Wifi) Terhadap Serangan Packet *Sniffing* Di Penginapan La Tulip" sebagai salah satu syarat untuk menyelesaikan studi di Universitas Amikom Yogyakarta.

Dalam proses penyelesaian skripsi ini, penulis menyadari banyak bantuan, dukungan, dan bimbingan yang telah diterima dari 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, yang telah memberikan kesempatan kepada penulis untuk menyelesaikan pendidikan di universitas ini.
2. Bapak Hanif Al-Fatta, M.Kom, Ph.D, selaku Dekan Fakultas Ilmu Komputer, yang telah memberikan dukungan dalam pelaksanaan kegiatan akademik.
3. Ibu Windha Mega Pradnya Dhuhita, M.Kom, selaku Kepala Program Studi Fakultas Informatika Universitas Amikom Yogyakarta, yang telah memberikan dukungan, arahan, dan motivasi yang sangat berarti dalam penyusunan skripsi ini.
4. Bapak Lukman, M.Kom, selaku dosen pembimbing yang telah memberikan arahan, bimbingan, serta masukan berharga dalam penyusunan skripsi ini.
5. Penginapan La Tulip, yang telah memberikan izin dan fasilitas kepada penulis untuk melakukan penelitian di lingkungan perusahaan.
6. Orang tua, keluarga, dan teman-teman yang senantiasa memberikan doa, dukungan moral, dan motivasi yang tiada henti selama proses penyusunan skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran konstruktif sangat diharapkan untuk perbaikan dan penyempurnaan karya ini di masa mendatang.

Akhirnya, penulis berharap semoga skripsi ini dapat memberikan manfaat, baik bagi dunia akademik maupun praktisi, khususnya dalam bidang layanan IT.

Yogyakarta, 12 Februari 2025

Nur widiyanto

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

NDLC	*Network Development Life Cycle*
WiFi	*Wireless fidelity*
MitM	*Man-In-The-Middle*
ARP	*Address* Resolution Protocol
WPA	*Wi-Fi* Protected Access
WPA2	*Wi-Fi* Protected Access II
SSID	Service Set Identifier
MAC *Address*	Media Access Control *Address*
DNS	Domain Name System
CPU	Central Processing Unit
LAN	Local Area Network
MAN	Metropolitan Area Network
WAN	Wide Area Network
PDA	Personal Digital Assistant
ISP	Internet Service *Provider*
GNU	GNU's Not Unix
GPL	General Public License
SSD	Solid State Drive
DHCP	Dynamic Host Configuration Protocol
ACK	Acknowledgment
HTTP	Hypertext Transfer Protoco

DAFTAR ISTILAH

Sniffing Proses menangkap dan menganalisis data yang melintasi jaringan.

Hacker Individu yang memiliki keterampilan dalam komputer dan jaringan.

Packet Unit data yang dikirim melalui jaringan.

Encryption Proses mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi .

Firewall Sistem keamanan yang memantau dan mengontrol lalu lintas jaringan berdasarkan aturan keamanan yang telah ditentukan.

Malware Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau mendapatkan akses tidak sah ke sistem komputer.

Keylogger Jenis malware yang merekam penekanan tombol pada keyboard untuk mencuri informasi sensitif, seperti kata sandi dan data pribadi.

Backdoor Metode yang digunakan oleh penyerang untuk mendapatkan akses ke sistem tanpa otorisasi .

Phishing Teknik penipuan yang digunakan untuk mendapatkan informasi sensitif dengan menyamar sebagai entitas tepercaya dalam komunikasi elektronik.

Protokol Aturan atau standar yang ditetapkan untuk komunikasi antara perangkat dalam jaringan.

Capturing Proses menangkap data atau informasi dari sumber tertentu, Proses menangkap data atau informasi dari sumber tertentu.

Scanning Proses memindai jaringan atau sistem untuk mengidentifikasi perangkat, layanan, atau kerentanan.

INTISARI

Penelitian ini berfokus pada analisis keamanan jaringan *Wi-Fi* di penginapan La Tulip, yang menghadapi ancaman serangan *Packet Sniffing*. Masalah yang diidentifikasi adalah kerentanan jaringan yang dapat mengakibatkan pencurian data sensitif pengguna, seperti informasi login dan data pribadi. Dampak dari masalah ini tidak hanya merugikan penginapan, tetapi juga dapat mengancam privasi tamu yang menggunakan jaringan tersebut. Untuk menyelesaikan masalah ini, peneliti menggunakan metode eksperimen dengan alat analisis jaringan seperti *Wireshark* dan *Ettercap*. Langkah-langkah yang dilakukan meliputi pengumpulan data lalu lintas jaringan, simulasi serangan *sniffing*, serta evaluasi terhadap protokol keamanan yang digunakan, yaitu *WPA* dan *WPA2*.

Hasil penelitian menunjukkan bahwa meskipun protokol *WPA2* lebih aman dibandingkan *WPA*, masih terdapat celah yang dapat dieksploitasi oleh penyerang. Penelitian ini memberikan rekomendasi untuk meningkatkan keamanan jaringan dengan menerapkan protokol yang lebih kuat dan melakukan edukasi kepada pengguna tentang praktik keamanan yang baik. Kontribusi dari penelitian ini diharapkan dapat dimanfaatkan oleh pengelola penginapan dan penyedia layanan *Wi-Fi* untuk meningkatkan perlindungan data pengguna serta menjadi referensi bagi penelitian lebih lanjut di bidang keamanan jaringan.

Kata kunci: keamanan jaringan, *Wi-Fi*, *Packet Sniffing*, *WPA*, *WPA2*.

ABSTRACT

This research focuses on analysing the security of the Wi-Fi network at La Tulip inn, which faces the threat of Packet Sniffing attacks. The problem identified was a network vulnerability that could result in the theft of sensitive user data, such as login information and personal data. The impact of this problem is not only detrimental to the inn, but can also threaten the privacy of guests using the network. To solve this problem, researchers used experimental methods with network analysis tools such as Wireshark and Ettercap. The steps taken include collecting network traffic data, simulating sniffing attacks, and evaluating the security protocols used, namely WPA and WPA2.

The results show that although the WPA2 protocol is more secure than WPA, there are still gaps that can be exploited by attackers. This research provides recommendations to improve network security by implementing stronger protocols and educating users on good security practices. The contribution of this research is expected to be utilised by lodging managers and Wi-Fi service Providers to improve user data protection and become a reference for further research in the field of network security .

Keyword**:** *network security , Wi-Fi, Packet Sniffing, WPA, WPA2.*