

**ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI*  
TERHADAP SERANGAN *SNIFFING***

**SKRIPSI**



**Oleh:**

**Putri Rosayanti Silalahi  
180210034**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KOMPUTER  
UNIVERSITAS PUTERA BATAM  
2024**

**ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI*  
TERHADAP SERANGAN *SNIFFING***

**SKRIPSI**

**Untuk memenuhi salah satu syarat  
memperoleh gelar sarjana**



**Oleh:**

**Putri Rosayanti Silalahi  
180210034**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK DAN KOMPUTER  
UNIVERSITAS PUTERA BATAM  
2024**

## SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya:

Nama : Putri Rosayanti Silalahi  
NPM : 180210034  
Fakultas : Teknik dan Komputer  
Program Studi : Teknik Informatika

Menyatakan bahwa “**Skripsi**” yang saya buat dengan judul:

**“ANALISIS KEAMANAN JARINGAN WIFI TERHADAP SERANGAN SNIFFING”**

Ini bukan “duplikasi” karya orang lain; itu sepenuhnya ciptaanmu sendiri. Sepanjang pengetahuan saya, karya ilmiah atau pendapat yang dimuat dalam naskah skripsi ini hanyalah yang dikutip secara tertulis dan dicantumkan dalam daftar pustaka dan sumber kutipan. Semua karya dan opini lainnya telah ditulis atau diterbitkan oleh orang lain.

Apabila terbukti naskah tesis saya mengandung unsur PLAGIASI, maka saya setuju untuk dibatalkan dan gelar akademik saya dicabut, sesuai dengan peraturan perundang-undangan yang berlaku.

Oleh karena itu saya sungguh-sungguh membuat pernyataan ini bebas dari segala tekanan pihak luar.

Batam, 23 Februari 2024



**Putri Rosayanti Silalahi**

**180210034**

**ANALISIS KEAMANAN JARINGAN PADA FASILITAS *WIFI*  
TERHADAP SERANGAN *SNIFFING***

**SKRIPSI**

**Untuk memenuhi salah satu syarat  
guna memperoleh gelar Sarjana**

**Oleh  
Putri Rosayanti Silalahi  
180210034**

**Telah disetujui oleh Pembimbing pada tanggal  
Seperti tertera di bawah ini**

**Batam, 23 Februari 2024**



**Sunarsan Sitohang, S.Kom., M.TI.  
Pembimbing**

## ABSTRAK

Perkembangan teknologi dan ketergantungan pada jaringan *WiFi* memberikan manfaat besar dalam dunia bisnis, termasuk di YAMAHA, PT ALFA SCORPII Tembesi. Namun, kekhawatiran terhadap keamanan jaringan semakin meningkat, terutama dengan serangan cyber yang semakin kompleks. Salah satu ancaman yang muncul adalah serangan *sniffing*, di mana penyerang berusaha mencuri data sensitif melalui jaringan *WiFi*. Wireshark, sebagai alat peretasan *WiFi*, memainkan peran krusial dalam mengidentifikasi dan mengatasi potensi ancaman keamanan jaringan. Alat ini memiliki kemampuan untuk mendeteksi sinyal nirkabel terbuka, menganalisis protokol jaringan, dan mengaudit keamanan jaringan. Selain itu, Wireshark dapat melakukan tindakan lebih lanjut seperti memblokir lalu lintas di jaringan *LAN*, mencuri kata sandi, dan melakukan penyadapan aktif pada protokol umum. Penelitian ini dilakukan dalam dua tahap. Tahap pertama adalah mengidentifikasi keberadaan dan keamanan jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi. Sementara itu, tahap kedua melibatkan serangan paket *sniffing* menggunakan perangkat lunak Wireshark. Penelitian ini bertujuan untuk melakukan analisis mendalam terhadap keamanan jaringan *WiFi* di perusahaan tersebut terhadap serangan *sniffing*. Hasil penelitian ini memberikan wawasan lebih mendalam tentang tingkat keamanan jaringan *WiFi* di YAMAHA, PT ALFA SCORPII Tembesi. Selain itu, diharapkan penelitian ini membantu perusahaan mengidentifikasi dan mengatasi potensi kerentanan keamanan yang dapat dieksploitasi oleh serangan *sniffing*. Dengan meningkatkan keamanan jaringan, YAMAHA, PT ALFA SCORPII Tembesi dapat memastikan bahwa data sensitif pelanggan dan informasi perusahaan tetap aman dari ancaman serangan *sniffing*.

Kata kunci: Analisis Keamanan, *Sniffing*, *Wireshark*

## **ABSTRACT**

*The integration of technology and reliance on WiFi networks has yielded substantial advantages in the business domain, including at YAMAHA, PT ALFA SCORPII Tembesi. Nevertheless, concerns over network security are escalating, particularly in the face of growing cyber threats. One such potential menace is sniffing attacks, where perpetrators seek to pilfer sensitive data transmitted across WiFi networks. Wireshark, functioning as a WiFi hacking tool, assumes a pivotal role in pinpointing and mitigating potential security risks to the network. This tool possesses the capability to identify open wireless signals, scrutinize network protocols, and audit network security. Moreover, Wireshark can execute actions like obstructing traffic on LAN networks, pilfering passwords, and actively eavesdropping on common protocols. The research unfolds in two phases – the initial phase encompasses recognizing the existence and security of WiFi networks at YAMAHA, PT ALFA SCORPII Tembesi. Simultaneously, the second phase involves executing packet sniffing attacks using Wireshark software. The primary objective of this research is to undertake a thorough analysis of WiFi network security at the company concerning sniffing attacks. The results of this research provide deeper insight into the security level of the WiFi network at YAMAHA, PT ALFA SCORPII Tembesi. Furthermore, the research is poised to aid the company in detecting and rectifying potential security vulnerabilities susceptible to exploitation via sniffing attacks. Through fortifying network security, YAMAHA, PT ALFA SCORPII Tembesi can ensure the safeguarding of customer-sensitive data and company information from the looming threat of sniffing attacks.*

*Keyword: Security Analysis ,Sniffing,Wireshark*

## KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa , atas segala limpahan nikmat dan karunia-Nya yang tak terhingga, sehingga penulis dapat melakukan dan menyelesaikan penelitian di YAMAHA, PT ALFA SCORPII Tembesi serta dapat menyelesaikan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika Universitas putera batam.

selanjutnya penulis mengucapkan terimakasih kepada pihak-pihak yang telah mendukung secara langsung maupun tidak langsung dalam kelancaran skripsi ini, antara lain:

1. Rektor Universitas Putera Batam, Ibu Nur Elfi Husda, S.Kom.,M.SI.
2. Dekan Fakultas Teknik dan Komputer, Bapak Welly Sugianto, S.T.,M.Mm.
3. Ketua Program Studi Teknik Informatika Universitas Putera Batam, Bapak Andi Maslan, S.T.,M.SI.
4. Bapak Sunarsan Sitohang, S.Kom., M.TI. selaku pembimbing skripsi, yang telah bersedia memberikan masukan, nasehat dan dukungannya kepada penulis. Terima kasih, Pak.
5. Bapak Elbert Hutabri, S.Kom., M.Kom. Selaku dosen pembimbing akademik.
6. Dosen dan Staff Universitas Putera Batam.
7. Orang Tua Tercinta, Yang selalu memberikan kasih sayang, dukungan, semangat, moril dan materil yang tak terhingga serta doa. Terima kasih atas jasa yang tak terhingga.
8. Teman, Kakak, Abang, sahabat penulis yang selalu memberi semangat dan dukungan kepada penulis untuk menyelesaikan sripsi.
9. Teman-teman sekelas Teknik Informatika Kelas *Shift*, Teman-teman Teknik Informatika Angkatan 2018 Universitas Putera Batam. Terima kasih untuk segala dukungan dan doa.
10. Kepada pihak-pihak yang telah banyak membantu, mohon maaf apabila tak disebut nama, dan mohon maaf apabila tak disebut gelar. Terima kasih.

Semoga Allah membalas segala kebaikan, memudahkan segala urusan serta mencurahkan rahmat-Nya. Aamiin.

Batam, 23 Februari 2024

A handwritten signature in black ink, appearing to read 'Putri Rosayanti Silalahi'.

Putri Rosayanti Silalahi



## DAFTAR ISI

<b>ANALISIS KEAMANAN JARINGAN PADA FASILITAS <i>WIFI</i> TERHADAP SERANGAN <i>SNIFFING</i> .....</b>	<b>i</b>
<b>ANALISIS KEAMANAN JARINGAN PADA FASILITAS <i>WIFI</i> TERHADAP SERANGAN <i>SNIFFING</i> .....</b>	<b>i</b>
<b>SURAT PERNYATAAN ORISINALITAS .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>ii</b>
<b>ABSTRAK .....</b>	<b>iii</b>
<b><i>ABSTRACT</i> .....</b>	<b>iv</b>
<b>KATA PENGANTAR.....</b>	<b>v</b>
<b>DAFTAR ISI.....</b>	<b>vii</b>
<b>DAFTAR GAMBAR.....</b>	<b>ix</b>
<b>DAFTAR TABEL .....</b>	<b>x</b>
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar belakang .....	1
1.2 Identifikasi masalah.....	4
1.3 Batasan Masalah.....	4
1.4 Rumusan Masalah .....	5
1.5 Tujuan penelitian .....	5
1.6 Manfaat penelitian .....	5
1.6.1 Secara teoritis .....	5
1.6.2 Secara praktis .....	6
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>7</b>
2.1 Teori dasar .....	7

2.1.1	Jaringan komputer.....	7
2.1.2	Standar Jaringan Komputer .....	8
2.1.2.1	Serangkaian standar IEEE802.....	9
2.1.3	Jenis Jaringan Komputer.....	10
2.1.4	Keamanan jaringan komputer.....	13
2.1.5	Jenis Ancaman Jaringan Komputer .....	13
2.1.6	Model OSI layer.....	14
2.2	Teori Khusus .....	20
2.2.1	<i>WiFi</i> .....	21
2.2.2	<i>Sniffing</i> .....	21
2.3	<i>Tools</i> .....	22
2.3.1	<i>Kali Linux</i> .....	22
2.3.1	<i>Wireshark</i> .....	23
2.4	Penelitian Terdahulu.....	24
2.5	Kerangka Pemikiran .....	30
<b>BAB III DESAIN PENELITIAN.....</b>		<b>31</b>
3.1	Desain Penelitian .....	31
3.2	Analisis jaringan.....	32
3.3	Rancangan Jaringan yang Dibangun/Diusulkan.....	34
3.4	Lokasi dan Jadwal Penelitian .....	36
<b>BAB IV HASIL PENELITIAN DAN PEMBAHASAN.....</b>		<b>38</b>
4.1	Hasil Penelitian.....	38
4.1.1	Persiapan Tools.....	38
4.2	Pembahasan .....	44
4.2.1.	Hasil Analisis Jaringan <i>WiFi</i> .....	44

4.2.2. Packet <i>Sniffing</i> .....	46
<b>BAB V KESIMPULAN DAN SARAN .....</b>	<b>54</b>
5.1 Kesimpulan.....	54
5.2 Saran.....	55
<b>DAFTAR PUSTAKA .....</b>	<b>57</b>

## DAFTAR GAMBAR

	Halaman
<b>Gambar 2. 1</b> LAN (Local Area Network) .....	11
<b>Gambar 2. 2</b> MAN (Metropolitan Area Network).....	12
<b>Gambar 2. 3</b> WAN (Wide Area Network).....	12
<b>Gambar 2. 4</b> Internet (Interconnected Network) .....	13
<b>Gambar 2. 5</b> Model OSI Layer .....	15
<b>Gambar 2. 6</b> Physical layer .....	16
<b>Gambar 2. 7</b> Data link layer.....	17
<b>Gambar 2. 8</b> Network layer .....	17
<b>Gambar 2. 9</b> Transport layer .....	18
<b>Gambar 2. 10</b> Session layer .....	19
<b>Gambar 2. 11</b> Presentation layer.....	19
<b>Gambar 2. 12</b> Application layer .....	20
<b>Gambar 2. 13</b> Wireshark versi 3.0.2 .....	24
<b>Gambar 2. 14</b> Kerangka Pemikiran .....	30
<b>Gambar 3. 1</b> Disain Penelitian .....	31
<b>Gambar 3. 2</b> Jaringan yang sedang berjalan .....	33
<b>Gambar 3. 3</b> Topologi Jaringan yang Diusulkan.....	35
<b>Gambar 4. 1</b> Tampilan Login .....	39
<b>Gambar 4. 2</b> Tampilan Dekstop Kali Linux Undercover Mode .....	40
<b>Gambar 4. 3</b> Melakukan Update.....	41
<b>Gambar 4. 4</b> TampilanTerminal Saat Menginstal Wireshark.....	42
<b>Gambar 4. 5</b> Memeriksa Utilitas Wireshark Disistem.....	43
<b>Gambar 4. 6</b> Membuka Wireshark .....	43
<b>Gambar 4. 7</b> Tampilan Interface pada Wireshark.....	44
<b>Gambar 4. 8</b> Monitoring Jaringan WiFi Hari 1 .....	45
<b>Gambar 4. 9</b> Monitoring Jaringan WiFi Hari 2 .....	45
<b>Gambar 4. 10</b> Skenario Serangan Menggunakan Metode Follow Stream .....	47
<b>Gambar 4. 11</b> Jaringan yang Sedang di Sniffing .....	48
<b>Gambar 4. 12</b> TCP Stream.....	49

## DAFTAR TABEL

Halaman

<b>Tabel 3. 1</b> Perangkat keras yang sedang berjalan.....	33
<b>Tabel 3. 2</b> Perangkat Keras yang Diusulkan .....	35
<b>Tabel 4. 1</b> Website yang akan di sniffing .....	<b>Error! Bookmark not defined.</b>
<b>Tabel 4. 2</b> Hasil Aktifitas <i>Sniffing</i> Menggunakan wireshark.....	49