

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP  
SERANGAN PACKET SNIFFING DENGAN IDS**

**SKRIPSI**

Untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi (S1-Informatika)



Disusun oleh :

**REZKY ADITYA PURNAMA PUTRA**

**19.11.3268**

Kepada

**Andika Agus Slameto, M.Kom**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**2023**

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP  
SERANGAN PACKET SNIFFING DENGAN IDS**

**SKRIPSI**

Untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi (S1-Informatika)



Disusun oleh :

**REZKY ADITYA PURNAMA PUTRA**

**19.11.3268**

Kepada

**Andika Agus Slameto, M.Kom**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS AMIKOM YOGYAKARTA**

**2023**

**HALAMAN PERSETUJUAN**

**SKRIPSI**

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN  
PACKET SNIFFING DENGAN IDS**

yang disusun dan diajukan oleh

**Rezky Aditya Purnama Putra**

**19.11.5268**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 19 Oktober 2023

Dosen Pembimbing,



**Andika Agus Slameta, M.Kom**  
**NIK. 190302109**

**HALAMAN PENGESAHAN**

**SKRIPSI**

**ANALISIS KEAMANAN JARINGAN (WIFI) TERHADAP SERANGAN  
PACKET SNIFFING DENGAN IDS**

yang disusun dan diajukan oleh

**Rezky Aditya Purnama Putra**

**19.11.3268**

Telah dipertahankan di depan Dewan Penguji  
pada tanggal 19 Oktober 2023

**Susunan Dewan Penguji**

**Nama Penguji**

**Tanda Tangan**

**Arif Akbarul Huda, S.Si, M.Eng**  
NIK. 190302287



**Yudi Sutanto, M.Kom**  
NIK. 190302039



**Andika Agus Slameto, M.Kom**  
NIK. 190302109



Skrripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 19 Oktober 2023

**DEKAN FAKULTAS ILMU KOMPUTER**



**Hanif Al Fatta, S.Kom., M.Kom.**  
NIK. 190302096

## HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rezky Aditya Purnama Putra  
NIM : 19.11.3268

Menyatakan bahwa Skripsi dengan judul berikut:

**Analisis Keamanan Jaringan (Wifi) Terhadap Serangan Packet Sniffing Dengan IDS**

Dosen Pembimbing : Andika Agus Slameto, 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, 19 Oktober 2023

Yang Menyatakan,



Signature and stamp of Rezky Aditya Purnama Putra, NIM: AA00548928753

Rezky Aditya Purnama Putra

## HALAMAN PERSEMBAHAN

Alhamdulillahirobbil'alamin, dengan mengucapkan rasa syukur atas karunia rahmat Allah SWT berikan. Dengan diselesaikannya skripsi ini, saya mempersembahkan kepada :

1. Kedua orang tua (Sugeng Purnomo dan Yulin Wahyu Estuti) yang tidak henti-hentinya selalu memberikan kasih sayang, mendoakan, dan memotivasi saya dalam segala hal apapun. Gelar ini saya persembahkan untuk orang tua saya yang mendidik saya mendapat gelar S1. Terima kasih untuk orang tua saya karna selalu ada disaat susah maupun senang. Terima kasih.
2. Untuk adik saya (Valena Maharani Purnama Putri) yang telah memotivasi saya untuk cepat menyelesaikan skripsi ini.
3. Terimakasih untuk dosen pembimbing saya bapak Andika Agus Slameto M.Kom, yang selalu membimbing saya dan mempermudah jalannya skripsi ini.
4. Untuk teman kontrakan saya yang tidak bisa saya sebut satu-satu yang telah mengajarkan saya tentang materi kuliah, membantu saya mengerjakan tugas selama kuliah, dan tempat saya untuk berdiskusi.
5. Untuk Aliaaaaaaa yang telah memberikan saya support dan membantu saya dalam mengerjakan skripsi.
6. Serta semua pihak yang telah mendukung saya yang tidak bisa saya sebutkan satu persatu.



## KATA PENGANTAR

Puji dan Syukur atas kehadiran Allah SWT, yang telah memberikan Rahmat, karunia, dan hidayahnya. Sholawat serta salam selalu tercurahkan kepada Nabi Muhammad SAW dan semoga kita semua mendapatkan syafa'atnya di hari akhir. Aaammiiiiinnn.

Dalam kata pengantar skripsi ini, saya ingin mengucapkan terima kasih kepada semua pihak yang telah ikut serta dalam penyelesaian skripsi ini. Tanpa bantuan, dorongan dan dukungan mereka, skripsi ini tidak akan dapat diselesaikan dengan baik. Saya tidak lupa mengucapkan terimakasih kepada :

1. Bapak dan Ibu saya yaitu Sugeng Purnomo dan Yulin Wahyu Estuti orang yang saya cintai yang telah memberikan segala kasih sayang, motivasi, dan support dalam segala hal.
2. Bapak Prof. Dr. M. Suyanto, M.M, selaku Rektor Universitas AMIKOM Yogyakarta.
3. Bapak Hanif Al Fatta, S. Kom., M. Kom, selaku Dekan Fakultas Ilmu Universitas AMIKOM Yogyakarta.
4. Bapak Andika Agus Slameto, M.Kom selaku Dosen Pembimbing saya yang telah memberikan bimbingan dalam proses skripsi saya.
5. Teman-teman 19-IF 11 atas segala hal bantuan.
6. Semua pihak yang telah membantu penulisan skripsi ini yang tidak bisa saya sebutkan satu persatu.

Saya sangat menyadari bahwa skripsi ini masih jauh dari kata kesempurnaan. Apabila terdapat kesalahan dan kekurangan mohon maaf sebesar besarnya.

Yogyakarta 19 Oktober 2023

Rezky Aditya Purnama Putra

## DAFTAR ISI

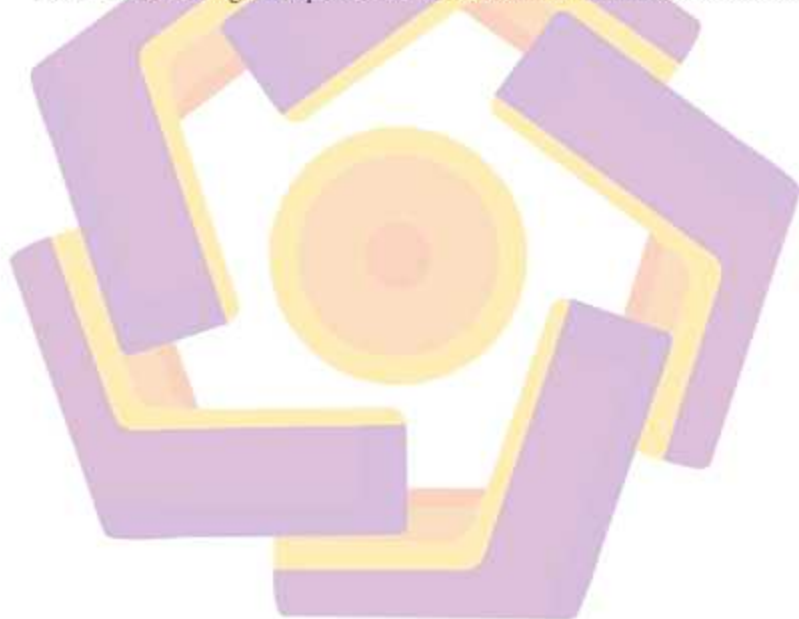
|   |     |
|---|-----|
| HALAMAN JUDUL.....                          | i   |
| HALAMAN PERSETUJUAN.....                    | ii  |
| HALAMAN PENGESAHAN.....                     | iii |
| HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....    | iv  |
| HALAMAN PERSEMBAHAN.....                    | v   |
| KATA PENGANTAR.....                         | vi  |
| DAFTAR ISI.....                             | vii |
| DAFTAR TABEL.....                           | ix  |
| DAFTAR GAMBAR.....                          | x   |
| INTISARI.....                               | xi  |
| ABSTRACT.....                               | xii |
| BAB I PENDAHULUAN.....                      | 1   |
| 1.1 Latar Belakang Masalah.....             | 2   |
| 1.1 Rumusan Masalah.....                    | 2   |
| 1.1 Batasan Masalah.....                    | 2   |
| 1.1 Tujuan Penelitian.....                  | 2   |
| 1.1 Manfaat Penelitian.....                 | 3   |
| 1.1 Sistematika Penulisan.....              | 3   |
| BAB II TINJAUAN PUSTAKA.....                | 5   |
| 2.1 Studi Literatur.....                    | 5   |
| 2.2 Dasar Teori.....                        | 11  |
| 2.2.1 Jaringan Komputer.....                | 11  |
| 2.2.2 Keamanan Jaringan.....                | 13  |
| 2.2.3 Jaringan Wireless.....                | 15  |
| 2.2.4 Intrusion Detection System (IDS)..... | 16  |
| 2.2.5 Jenis – jenis IDS.....                | 17  |
| 2.2.6 Packet Sniffing.....                  | 18  |
| 2.2.7 Ettercap.....                         | 18  |
| 2.2.8 Sistem Operasi.....                   | 19  |
| 2.2.9 Linux.....                            | 19  |



|  |                                     |           |
|--|-------------------------------------|-----------|
| 2.2.10                                   | Flowchart Analisis .....            | 20        |
| <b>BAB III METODE PENELITIAN.....</b>    |                                     | <b>22</b> |
| 3.1                                      | Metode Penelitian.....              | 22        |
| 3.2                                      | Alur Penelitian .....               | 24        |
| 3.3                                      | Alat dan Bahan.....                 | 25        |
| <b>BAB IV HASIL DAN PEMBAHASAN .....</b> |                                     | <b>27</b> |
| 4.1                                      | Perancangan Penelitian .....        | 27        |
| 4.1.1                                    | Rancangan Sistem .....              | 27        |
| 4.1.2                                    | Rancangan Jaringan .....            | 28        |
| 4.1.3                                    | Rancangan Proses dan Pengujian..... | 29        |
| 4.2                                      | Implementasi.....                   | 31        |
| 4.3                                      | Pengujian Packet Sniffing.....      | 33        |
| <b>BAB V PENUTUP.....</b>                |                                     | <b>45</b> |
| 5.1                                      | Kesimpulan .....                    | 45        |
| 5.2                                      | Saran.....                          | 46        |
| <b>DAFTAR PUSTAKA .....</b>              |                                     | <b>47</b> |

## DAFTAR TABEL

|   |    |
|---|----|
| Tabel 2. 1 Tabel Keaslian Penelitian.....               | 8  |
| Tabel 2. 2 Simbol – Simbol Flowchart .....              | 20 |
| Tabel 3. 1 Analisis SWOT .....                          | 22 |
| Tabel 4.1 Daftar Website HTTP yang akan diserang .....  | 29 |
| Tabel 4.2 Daftar Website HTTPS yang akan diserang ..... | 30 |
| Tabel 4.3 Hasil Packet Sniffing Website HTTP .....      | 43 |
| Tabel 4.4 Hasil Packet Sniffing Website HTTPS .....     | 43 |
| Tabel 4.5 Perbandingan Burpsuite dan Wireshark.....     | 44 |



## DAFTAR GAMBAR

|  |    |
|--|----|
| Gambar 2. 1 Local Area Network .....         | 11 |
| Gambar 2. 2 Metropolitan Area Network .....  | 12 |
| Gambar 2. 3 Wide Area Network .....          | 13 |
| Gambar 3. 1 Diagram Alur Penelitian.....     | 24 |
| Gambar 4. 1 Cara Kerja IDS .....             | 27 |
| Gambar 4. 2 Cara Kerja Packet Sniffing ..... | 28 |
| Gambar 4. 3 Topologi Jaringan .....          | 29 |
| Gambar 4. 4 Update Repository .....          | 32 |
| Gambar 4. 5 Cek IP Address .....             | 32 |
| Gambar 4. 6 Intercept is Off .....           | 33 |
| Gambar 4. 7 Daftar Interface Wireshark ..... | 33 |
| Gambar 4. 8 Tampilan Awal Wireshark .....    | 34 |
| Gambar 4. 9 Start Ettercap .....             | 34 |
| Gambar 4. 10 Tampilan Awal Ettercap.....     | 35 |
| Gambar 4. 11 Tampilan Host List.....         | 35 |
| Gambar 4. 12 ARP Poisoning .....             | 36 |
| Gambar 4. 13 Popup MITM.....                 | 36 |
| Gambar 4. 14 Proses Login Website HTTP.....  | 36 |
| Gambar 4. 15 Sniffing di Ettercap .....      | 37 |
| Gambar 4. 16 Capture Wireshark.....          | 37 |
| Gambar 4. 17 Cek IP Website.....             | 37 |
| Gambar 4. 18 TCP Stream .....                | 38 |
| Gambar 4. 19 Menu Proxy Setting.....         | 39 |
| Gambar 4. 20 Browser Burpsuite.....          | 39 |
| Gambar 4. 21 Login Page Waskita .....        | 40 |
| Gambar 4. 22 Tampilan Awal Waskita .....     | 40 |
| Gambar 4. 23 Capture Packet Burpsuite .....  | 41 |
| Gambar 4. 24 List API .....                  | 41 |
| Gambar 4. 25 Tampilan Site Map .....         | 42 |

## INTISARI

Jaringan nirkabel merupakan suatu teknologi yang dapat menghubungkan dua perangkat atau lebih untuk berkomunikasi tanpa harus menggunakan kabel sebagai media transmisi data. koneksi nirkabel menggunakan gelombang elektromagnetik seperti (gelombang radio dan gelombang *microwave*). Jaringan nirkabel biasa ditemukan dalam produk layanan komunikasi seperti telepon (suara), radio, wifi, dan layanan televisi. *Packet Sniffing* adalah teknik pencurian data pada sebuah jaringan yang ditransmisikan dari komputer *client* ke *server web*. Berdasarkan penjetlasan diatas maka rumusan masalah yang terjadi adalah : bagaimana cara mendeteksi serangan *sniffing attack* dan meningkatkan keamanan jaringan nirkabel

Dalam penelitian ini peneliti mencoba untuk menganalisis masalah utama yang terjadi dan memberi pengetahuan tentang dampak atau resiko jaringan nirkabel tanpa menggunakan fitur keamanan. penelitian ini membahas pendeteksi serangan *Packet Sniffing* pada wifi dengan menggunakan sistem *IDS*. *Intrusion Detection System (IDS)* adalah sebuah sistem yang melakukan pengawasan terhadap kegiatan-kegiatan yang mencurigakan dalam sebuah sistem jaringan.

Hasil dari penelitian ini adalah pada *protokol HTTP*, *tools ettercap* mampu merekam aktivitas jaringan internet dan mampu menangkap *user* dan *password* pada saat *login* menggunakan *protokol HTTP*, sedangkan pada *protokol HTTPS* tidak dapat melakukan aktivitas internet karena *protokol HTTPS* memiliki *security*. ketika *IDS snort* dijalankan, *IDS* akan memonitoring jaringan internet dan akan memberi *alert* berupa *text "Overwrite Attack"* ketika terdapat serangan *sniffing attack* dengan indikasi *arp spoofing*

Kata kunci : Jaringan Nirkabel, *IDS*, *Packet Sniffing*

## ABSTRACT

A wireless network is a technology that can connect two or more devices to communicate without having to use cables as a data transmission medium. Wireless connection uses electromagnetic waves such as (radio waves and microwave waves). Wireless networks are commonly found in communication service products such as telephone (voice), radio, wifi, and television services. Packet Sniffing is a data theft technique on a network that is transmitted from a client computer to a web server. Based on the explanation above, the formulation of the problem that occurs is: how to detect sniffing attacks and improve wireless network security.

In this study, the researcher tries to analyze the main problems that occur and provide knowledge about the impact or risk of wireless networks without using security features. This study discusses detecting packet sniffing attacks on wifi using an IDS system. Intrusion Detection System (IDS) is a system that monitors suspicious activities in a network system.

The results of this study are the HTTP protocol, ettercap tools can record internet network activity and can capture users and passwords when logging in using the HTTP protocol, while the HTTPS protocol cannot perform internet activities because the HTTPS protocol has security. when IDS snort is run, the IDS will monitor the internet network and will give an alert in the form of the text "Overwrite Attack" when there is a sniffing attack with an indication of arp spoofing.

Keywords : Wireless Network, IDS, Packet Sniffing