

**PROGRAM STUDI TEKNIK KOMPUTER**

**PENERAPAN KEAMANAN JARINGAN DARI SERANGAN SNIFFING DI  
DEPARTEMEN LAYANAN TI PT PUPUK SRIWIDJAJA (PUSRI)  
PALEMBANG**

**KARYA AKHIR**



**MUHAMAD ARY JANUARTA**

**211220011**

**PROGRAM DIPLOMA III  
FAKULTAS VOKASI  
UNIVERSITAS BINA DARMA  
PALEMBANG**

**2024**



**PENERAPAN KEAMANAN JARINGAN DARI SERANGAN SNIFFING DI  
DEPARTEMEN LAYANAN TI PT PUPUK SRIWIDJAJA  
(PUSRI)PALEMBANG**

**MUHAMAD ARY JANUARTA**

**211220011**

**Karya akhir ini diajukan sebagai salah satu syarat memperoleh gelar  
Ahli Madya (A.Md.)**

**PROGRAM STUDI TEKNIK KOMPUTER  
FAKULTAS VOKASI  
UNIVERSITAS BINA DARMA  
2024**

**HALAMAN PENGESAHAN**

**PENERAPAN KEAMANAN JARINGAN DARI SERANGAN  
SNIFFING DI DEPARTEMEN LAYANAN TI PT. PUPUK  
SRIWIDJAJA (PUSRI) PALEMBANG**

**MUHAMAD ARY JANUARTA  
211220011**

**Telah diterima sebagai salah satu syarat untuk memperoleh gelar Ahli  
Madya pada Program Studi Teknik Komputer**

Palembang, 10 Agustus 2024  
Fakultas Vokasi  
Universitas Bina Darma  
Dekan,

Pembimbing,



(Misinem, S.Köm., M.Si. )



(Prof. Dr. Edi Surya Negara, M.Kom.)

## HALAMAN PERSETUJUAN

Karya akhir Berjudul ” Penerapan Keamanan Jaringan Dari Serangan Sniffing Di Departemen Layanan TI PT. Pupuk Sriwidjaja (Pusri) Palembang ” oleh Muhamad Ary Januarta telah dipertahankan didepan komisi penguji pada hari senin tanggal 10 agustus 2024.

### KOMISI PENGUJI

1. Misinem, S.Kom., M.Si pembimbing
2. Tamsir Ariyadi, M.Kom. penguji I
3. Akhmad Khudri, M.Kom. penguji II

Palembang, 10 Agustus 2024

Program Studi Teknik Komputer

Fakultas Vokasi

Universitas Bina Darma

Ketua,



(Timur Dali Purwanto, S.Kom., M.Kom.)

## SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Muhamad Ary Januarta

Nim : 211220011

Dengan ini menyatakan bahwa :

1. Karya tulis saya ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (Sarjana/Diploma) di Universitas Bina Darma;
2. Karya tulis ini murni gagasan, rumusan dan penelitian saya sendiri dengan arahan dari tim pembimbing;
3. Di dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dikutip dengan mencantumkan nama pengarang dan memasukan dalam daftar rujukan atau daftar pustaka;
4. Saya bersedia karya tulis ini di cek keasliannya menggunakan *Plagiarism Checker* serta diunggah ke internet, sehingga dapat diakses *public* secara *online*;
5. Surat pernyataan ini saya tulis dengan sungguh – sungguh dan apabila terbukti melakukan penyimpangan atau ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi sesuai dengan peraturan perundang – undangan yang berlaku saat ini.

Dengan surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 10 Agustus 2024  
Yang Membuat Pernyataan,



Muhamad Ary Januarta  
NIM : 211220011

## MOTTO DAN PERSEMBAHAN

### MOTTO :

- “Memulai penuh keyakinan, menjalankan dengan penuh keikhlasan, menyelesaikan dengan penuh kebahagiaan”
- “ tidak ada mimpi yang gagal , yang ada hanyalah mimpi yang tertunda. Cuman sekiranya kalau teman-teman merasa gagal dalam mencapai mimpi, jangan khawatir, mimpi-mimpi lain bisa diciptakan”  
(Windah Basudara)

### PERSEMBAHAN :

- Allah subhanahu wa ta'ala.
- Kedua orang tua saya tercinta bapak syamsiar dan ibu Nailah, orang tua yang hebat yang selalu menjadi penyemangat saya sebagai sandaran terkuat dari kerasnya dunia. Yang tak henti-hentinya mendo'akan mencurahkan kasih sayang, perhatian, motivasi, nasihat, serta dukungan baik secara moral maupun finansial.
- Kedua adikku, Fitri Julianti dan Naysa Juliantary. Terima kasih sudah ikut serta dalam proses penulis menempuh pendidikan selama ini, terima kasih atas support nya.
- Kepada pembimbing saya Misinem, S.Kom.,M.Si.. Terima kasih atas bimbingannya, kritik, dan saran, dan selalu meluangkan waktu disela kesibukan.
- Seluruh Dosen Universitas Bina Darma Palembang
- Kepada semua grup teknik komputer 2021, dan grup D3 Akatsuki yang telah memberikan support sehingga saya bisa menyelesaikan karya akhir ini.

## ABSTRACT

Network security is a crucial aspect in maintaining the integrity, confidentiality, and availability of data in an organization. Sniffing attacks, a type of attack in which the perpetrator intercepts and monitors data transmitted over the network, pose a significant threat to data security. This research aims to analyze the performance of network security in the IT Services Department of PT Pupuk Sriwidjaja (PUSRI) Palembang from the threat of sniffing attacks. The research methods used include evaluation of existing security systems, testing against potential sniffing attacks, as well as implementation and analysis of the effectiveness of various security mechanisms such as encryption, network segmentation, and intrusion detection. The results show that with the implementation of appropriate security mechanisms, the risk of sniffing attacks can be minimized. In addition, this research also provides recommendations for further development in improving network security, including training for IT staff on best security practices and improving real-time network monitoring.

*Keywords: Network security, sniffing attack, PT Pupuk Sriwidjaja, encryption, network segmentation, intrusion detection.*

## ABSTRAK

Keamanan jaringan merupakan aspek krusial dalam menjaga integritas, kerahasiaan, dan ketersediaan data pada sebuah organisasi. Serangan sniffing, yaitu jenis serangan di mana pelaku mengintersepsi dan memantau data yang dikirimkan melalui jaringan, menjadi ancaman signifikan terhadap keamanan data. Penelitian ini bertujuan untuk menganalisis kinerja keamanan jaringan di Departemen Layanan TI PT. Pupuk Sriwidjaja (PUSRI) Palembang dari ancaman serangan sniffing. Metode penelitian yang digunakan meliputi evaluasi sistem keamanan yang ada, pengujian terhadap potensi serangan sniffing, serta implementasi dan analisis efektivitas berbagai mekanisme keamanan seperti enkripsi, segmentasi jaringan, dan deteksi intrusi. Hasil penelitian menunjukkan bahwa dengan penerapan mekanisme keamanan yang tepat, risiko terhadap serangan sniffing dapat diminimalkan. Selain itu, penelitian ini juga memberikan rekomendasi bagi pengembangan lebih lanjut dalam meningkatkan keamanan jaringan, termasuk pelatihan bagi staf TI mengenai praktik keamanan terbaik dan peningkatan pemantauan jaringan secara real-time.

*Kata kunci: Keamanan jaringan, serangan sniffing, PT. Pupuk Sriwidjaja, enkripsi, segmentasi jaringan, deteksi intrusi.*



# DAFTAR RIWAYAT HIDUP

## *CURICULUM VITAE*

---

### **MUHAMAD ARY JANUARTA, A.Md.**

Fresh Graduate, Computer Engineering of Universitas Bina Darma

---

**PALEMBANG, SOUTH SUMATERA 30259 • 083160466346 • Email :**  
aryjanuarta30@gmail.com

---

#### **PERSONAL INFORMATION**

---

Date of Birth : Palembang, January, 30<sup>th</sup>, 2001  
Address : Jl, Mayor Jend. Satibi Darwis RT 029 RW 007  
Kel keramasan kec kertapati Palembang.



Nationality : Indonesia  
Material Status : Single

#### **EDUCATION BACKGROUND**

---

**2021 – 2024**                      **Universitas Bina Darma**  
Faculty of Vokasi  
Computer Engineering  
Associate's degree

## KATA PENGANTAR

*Assalamu'alaikum Wr. Wb*

Puji dan syukur atas kehadiran Allah SWT yang telah memberikan Nikmat, Hidayah, dan Karunia-Nya sehingga penulis menyelesaikan Karya Akhir dengan judul “ **PENERAPAN KEAMANAN JARINGAN DARI SERANGAN SNIFFING DI DEPARTEMEN LAYANAN TI PT. PUPUK SRIWIDJAJA (PUSRI) PALEMBANG.**”

Dalam penulisan karya akhir ini, penulis telah banyak menerima bantuan, baik sumbangan pemikiran, fasilitas, maupun tenaga yang tak ternilai harganya bagi penulis, Untuk itu penulis menyampaikan ucapan terima kasih kepada semua pihak yang telah membantu dalam pembuatan karya akhir ini, khususnya kepada yang terhormat :

1. Prof. Dr. Sunda Ariana, M.Pd., M.M Selaku Rektor Universitas Bina Darma Palembang.
2. Prof. Dr. Edi Surya Negara, M.Kom. Selaku Dekan Fakultas Vokasi .
3. Timur Dali Purwanto, M.Kom Selaku Ketua Program Studi Teknik Komputer.
4. Misinem, S.Kom.,M.Si Selaku Dosen Pembimbing Karya Akhir Sekaligus Pembimbing Akademik yang telah memberikan arahan dan bimbingan dalam proses menyelesaikan karya akhir.
5. Kepada kedua orang tua saya, keluarga besar yang senantiasa selalu memberikan dukungan dan do'a dalam penulisan karya akhir ini.

6. Seluruh dosen dan staf pengajar program Studi Teknik Komputer Universitas Bina Darma Palembang.
7. Teman teman seperjuangan angkatan 21 Teknik Komputer yang banyak memberikan masukan serta bantuan dalam menyelesaikan karya akhir.
8. Seluruh mahasiswa KP di kantor Mitra Bisnis dan Layanan TI PSP.

Penulis menyadari bahwa di dalam penulisan karya akhir ini masih banyak kekurangan. Segala kekurangan yang terjadi, merupakan keterbatasan dari penulis, untuk itu atas segala kekurangan yang terdapat dalam tugas akhir ini, penulis mengharapkan informasi , kritik dan saran yang membangun pembaca.

Akhir kata penulis mengucapkan terima kasih.

*Wassalamu'alaikum Wr.Wb*

Palembang, 10 Agustus 2024

Muhamad Ary Januarta

## DAFTAR ISI

<b>PROGRAM STUDI TEKNIK KOMPUTER .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>ii</b>
<b>HALAMAN PERSETUJUAN.....</b>	<b>iii</b>
<b>SURAT PERNYATAAN .....</b>	<b>iv</b>
<b>MOTTO DAN PERSEMBAHAN .....</b>	<b>v</b>
<b>ABSTRACT .....</b>	<b>vi</b>
<b>ABSTRAK .....</b>	<b>vii</b>
<b>DAFTAR RIWAYAT HIDUP.....</b>	<b>viii</b>
<b>KATA PENGANTAR.....</b>	<b>ix</b>
<b>DAFTAR ISI.....</b>	<b>xi</b>
<b>DAFTAR TABEL.....</b>	<b>xiii</b>
<b>DAFTAR GAMBAR.....</b>	<b>xiv</b>
<b>DAFTAR LAMPIRAN .....</b>	<b>xv</b>
<b>BAB I PENDAHULUAN .....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian .....	4
1.6 Penelitian Terdahulu.....	5
<b>BAB II METODOLOGI PENELITIAN .....</b>	<b>9</b>
2.1 Gambaran Objek Penelitian.....	9
2.1.1 Sejarah Singkat PT Pupuk Sriwidjaja (PUSRI) .....	9
2.1.2 Visi dan misi .....	9
2.1.3 Makna Logo Perusahaan .....	11
2.1.4 Nilai utama perusahaan.....	12
2.1.5 Struktur organisasi PT Pupuk Sriwidjaja Palembang .....	15
2.1.6 Struktur organisasi Departemen Mitra Bisnis dan Layanan TI.....	15

2.1.7 Waktu dan Pelaksanaan Penelitian .....	16
2.2 Bahan dan Alat .....	16
2.3 Metode Penelitian .....	22
2.3.1 Metode Pengumpulan Data .....	25
<b>BAB III .....</b>	<b>27</b>
<b>HASIL DAN PEMBAHASAN .....</b>	<b>27</b>
3.1 Pengujian Port Scanning .....	27
3.2 Melakukan Capture Jaringan .....	28
3.3 Pengujian Sniffing Tanpa Firewall .....	30
3.4 Konfigurasi firewall layer 7 protocol .....	32
3.5 Konfigurasi Filter Rules .....	35
3.5.1 Scanning port dalam keadaan Mode port knocking .....	40
3.5.2 pengujian serangan sniffing menggunakan firewall .....	40
3.5.3 Grafik before jaringan .....	43
3.5.4 Grafik after jaringan .....	44
3.6 Hasil pengujian .....	45
<b>BAB IV KESIMPULAN DAN SARAN .....</b>	<b>48</b>
4.1 Kesimpulan .....	48
4.2 Saran .....	49
<b>DAFTAR PUSTAKA .....</b>	<b>50</b>
<b>LAMPIRAN .....</b>	<b>.....</b>

## DAFTAR TABEL

<b>Tabel 2.1</b> Pengalamatan Ip Address .....	24
<b>Tabel 3.1</b> Hasil Aktivitas Serangan Sniffing Sebelum Diterapkan Firewall .....	43
<b>Tabel 3.2</b> Hasil Aktivitas Sniffing Serangan Setelah Diterapkan Firewall .....	44



## DAFTAR GAMBAR

<b>Gambar 2. 1</b> Logo Perusahaan .....	11
<b>Gambar 2. 2</b> Logo Akhlak .....	13
<b>Gambar 2. 3</b> Struktur Organisasi PT.Pupuk Sriwidjaja Palembang.....	15
<b>Gambar 2. 4</b> Struktur Organisasi Departemen Layanan Ti Pt.Pusri Palembang .....	16
<b>Gambar 2. 5</b> Laptop .....	17
<b>Gambar 2. 6</b> Mikrotik Hap Lite.....	18
<b>Gambar 2. 7</b> Tampilan Wireshark yang sedang Aktif .....	19
<b>Gambar 2. 8</b> Tampilan Ettercap .....	19
<b>Gambar 2. 9</b> Tahapan NMap .....	22
<b>Gambar 2. 10</b> Tahapan Penelitian .....	22
<b>Gambar 2. 11</b> Topologi Star .....	23
<b>Gambar 3. 1</b> Scanning Menggunakan Tools Zenmap .....	27
<b>Gambar 3. 2</b> Capture Jaringan Wireshark .....	28
<b>Gambar 3. 3</b> Menampilkan Informasi Hasil Wireshark .....	29
<b>Gambar 3. 4</b> Tampilan Web Login Mikrotik Di Browser .....	29
<b>Gambar 3. 5</b> Proses Serangan Sniffing Pada Ettercap .....	30
<b>Gambar 3. 6</b> Menampilkan User Pass Korban .....	31
<b>Gambar 3. 7</b> Lalu Lintas Di Wireshark Ketika Terjadi Serangan.....	31
<b>Gambar 3. 8</b> Firewall Rules.....	33
<b>Gambar 3. 9</b> Firewall Layer 7.....	33
<b>Gambar 3. 10</b> Tampilan <i>Action Drop</i> .....	34
<b>Gambar 3. 11</b> Tampilan Blokir Mikrotik .....	35
<b>Gambar 3. 12</b> Konfigurasi Firewall Rules .....	36
<b>Gambar 3. 13</b> Knock IP .....	37
<b>Gambar 3. 14</b> Hasil Konfigurasi Firewall Rules .....	38
<b>Gambar 3. 15</b> Tampilan Setelah Diterapkan Firewall.....	39
<b>Gambar 3. 16</b> Hasil scanning Nmap Setelah Diterapkan Firewall .....	40
<b>Gambar 3. 17</b> proses serangan sniffing.....	41
<b>Gambar 3. 18</b> Hasil Serangan Sniffing Menggunakan Firewall .....	42
<b>Gambar 3. 19</b> Grafik before jaringan.....	43
<b>Gambar 3. 20</b> Grafik after jaringan .....	44

## DAFTAR LAMPIRAN

- Lampiran 1.** Logbook Magang
- Lampiran 2.** Nilai Magang
- Lampiran 3.** Permohonan pengajuan judul Karya Akhir
- Lampiran 4.** SK pembimbing Karya Akhir
- Lampiran 5.** Lembar konsultasi Karya Akhir
- Lampiran 6.** Lembar perbaikan Karya Akhir
- Lampiran 7.** Nilai Karya Akhir

