

**DESAIN KEAMANAN JARINGAN MIKROTIK ROUTER OS  
MENGUNAKAN METODE PORT KNOCKING PADA  
BENGKEL JAYA PRATAMA**

**SKRIPSI**



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
INSTITUT SAINS DAN BISNIS ATMA LUHUR  
PANGKALPINANG**

**2023**

**DESAIN KEAMANAN JARINGAN MIKROTIK ROUTER OS  
MENGUNAKAN METODE PORT KNOCKING PADA  
BENGKEL JAYA PRATAMA**

**SKRIPSI**

**Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh  
Gelar Sarjana Komputer**



**Oleh:  
RIDHO TRIDAYANTO**

**1911500139**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INFORMASI  
INSTITUT SAINS DAN BISNIS ATMA LUHUR  
PANGKALPINANG**

**2023**

## SURAT PERNYATAAN ANTI PLAGIAT

Yang bertanda tangan di bawah ini

NIM : 1911500139

NAMA : Ridho Tridayanto

Judul Skripsi : **DESAIN KEAMANAN JARINGAN MIKROTIK ROUTER  
OS MENGGUNAKAN METODE PORT KNOCKING  
PADA BENGKEL JAYA PRATAMA**

Menyatakan bahwa Laporan Skripsi saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkal Pinang, 31 Januari 2023



Ridho Tridayanto

**LEMBAR PENGESAHAN SKRIPSI**

**DESAIN KEMAMAN JARINGAN MIKROTIK ROUTER OS  
MENGUNAKAN METODE PORT KNOCKING PADA  
BENGKEL JAYA PRATAMA**

Yang dipersiapkan dan disusun oleh  
**RIDHO TRIDAYANTO**  
1911500139

Telah dipertahankan di depan Dewan Penguji  
Pada tanggal 21 Juli 2023

**Susunan Dewan Penguji Anggota**

**Dosen Pembimbing**


  
**Rahmat Sulaiman, M.Kom**  
NIDN. 0208019401

  
**Dwi Yuny Sylfania, M.Kom**  
NIDN. 0207069301

**Kaprodi Teknik informatika**

**Ketua Penguji**

  
**Chandra Kirana, S.Kom, M.Kom**  
NIDN. 0228108501

  
**Yohanes Setiawan, M.Kom**  
NIDN. 0219068501

Skripsi ini telah diterima dan sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 07 Agustus 2023

**DEKAN FAKULTAS TEKNOLOGI INFORMASI**



**Ellya Helmiad, M.Kom**  
NIDN. 0201027901

## KATA PENGANTAR

Segala Puji syukur kehadiran Tuhan Yang Maha Esa yang telah melimpahkan Rahmat dan Cinta-Nya sehingga penulis dapat menyelesaikan penelitian Skripsi pada jurusan Informatika Institut Sains dan Bisnis Atma Luhur. Dalam penyusunan laporan skripsi ini mungkin tidak akan terlaksana tanpa dukungan, bimbingan dan petunjuk dari semua pihak yang telah membantu sehingga laporan dapat terselesaikan dengan baik. Untuk itu penulis ingin menyampaikan rasa terima kasih kepada :

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Orang tua tercinta, yang telah memberikan doa, semangat, dukungan, dan motivasi selama melakukan studi.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak prof. Dr. Moedjiono, M.Sc, Selaku Rektor ISB Atma Luhur.
5. Bapak Ellya Helmud, M.Kom, selaku Dekan FTI ISB Atma Luhur.
6. Bapak Chandra Kirana, M.Kom Selaku Kaprodi Teknik Informatika.
7. Ibu Dwi Yuny Sylfania, M.Kom. selaku Dosen Pembimbing Skripsi.
8. Saudara dan sahabat-sahabatku terutama Kawan-Kawan Angkatan 2019 yang telah memberikan dukungan moral untuk terus menyelesaikan skripsi ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, amin.

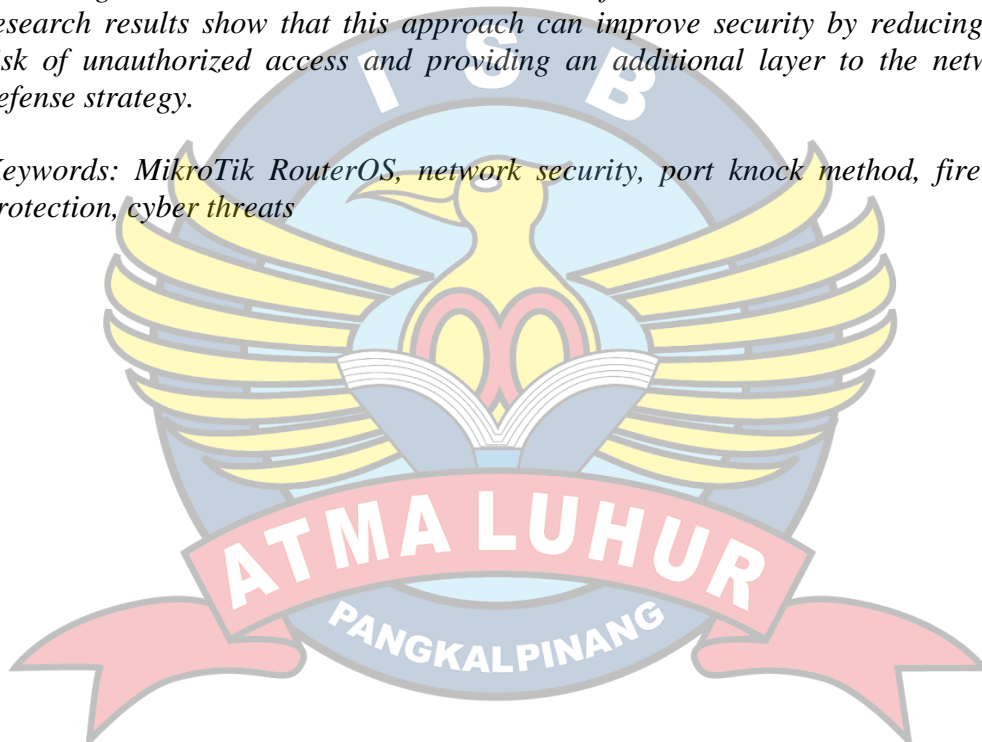
Pangkalpinang, Agustus 2023

Penulis

## ABSTRACT

*This thesis discusses the design and implementation of network security by typing ports on the MikroTik RouterOS platform. Cybersecurity is a major concern in today's digital era, and the port knocking method has been recognized as an effective approach to mitigating cyberthreats. This study focuses on integrating the port knocking concept into the MikroTik RouterOS firewall configuration to enhance the network protection layer. This method requires a series of connection requests on a specific port before granting the desired access. Experiments and tests were carried out to evaluate the effectiveness of the port knock method in protecting the MikroTik RouterOS network from unauthorized access. The research results show that this approach can improve security by reducing the risk of unauthorized access and providing an additional layer to the network defense strategy.*

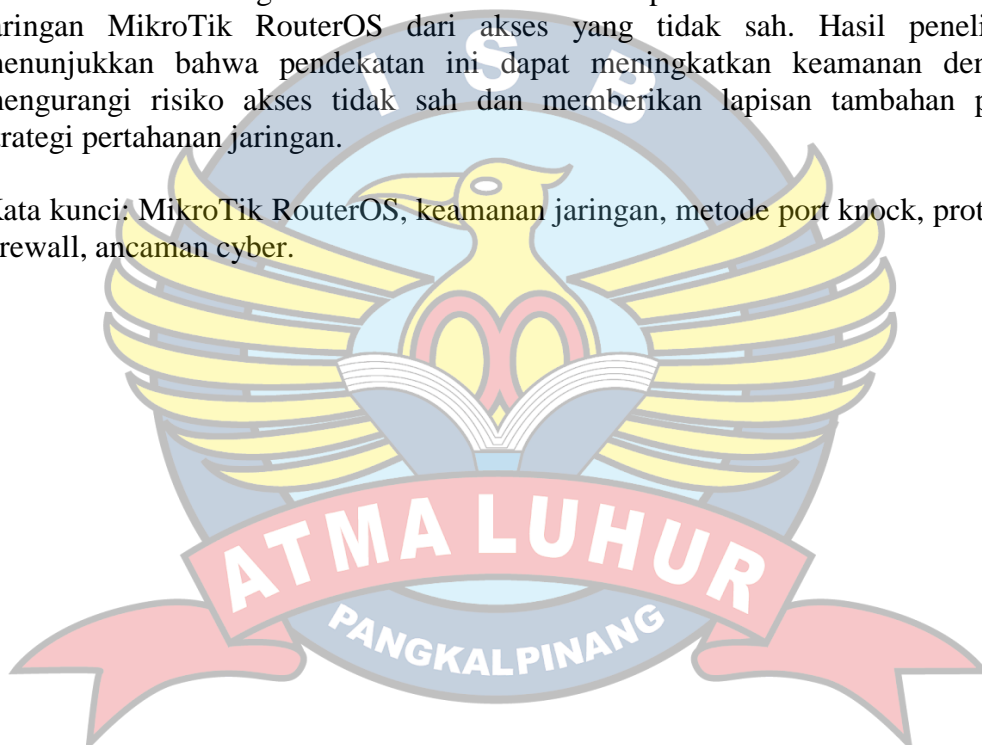
*Keywords: MikroTik RouterOS, network security, port knock method, firewall protection, cyber threats*



## ABSTRAK

Skripsi ini membahas tentang desain dan implementasi keamanan jaringan dengan menyetorkan port pada platform MikroTik RouterOS. Keamanan siber menjadi perhatian utama di era digital saat ini, dan metode port knocking telah diakui sebagai pendekatan yang efektif untuk memitigasi ancaman siber. Studi ini berfokus pada pengintegrasian konsep port knocking ke dalam konfigurasi firewall MikroTik RouterOS untuk meningkatkan lapisan perlindungan jaringan. Metode ini memerlukan serangkaian permintaan koneksi pada port tertentu sebelum memberikan akses yang diinginkan. Eksperimen dan pengujian dilakukan untuk mengevaluasi keefektifan metode port knock dalam melindungi jaringan MikroTik RouterOS dari akses yang tidak sah. Hasil penelitian menunjukkan bahwa pendekatan ini dapat meningkatkan keamanan dengan mengurangi risiko akses tidak sah dan memberikan lapisan tambahan pada strategi pertahanan jaringan.

Kata kunci: MikroTik RouterOS, keamanan jaringan, metode port knock, proteksi firewall, ancaman cyber.



## DAFTAR ISI

<b>LEMBAR PENYATAAN ANTI PLAGIAT</b> .....	<b>ii</b>
<b>LEMBAR PENGESAHAN SKRIPSI</b> .....	<b>iii</b>
<b>KATA PENGANTAR</b> .....	<b>iv</b>
<b>ABSTRACT</b> .....	<b>v</b>
<b>ABSTRAK</b> .....	<b>vi</b>
<b>DAFTAR ISI</b> .....	<b>vii</b>
<b>DAFTAR GAMBAR</b> .....	<b>x</b>
<b>DAFTAR TABEL</b> .....	<b>xi</b>
<b>BAB I PENDAHULUAN</b> .....	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian.....	3
1.4.1 Tujuan.....	3
1.4.2 Manfaat.....	3
1.5 Sistematika Penulisan.....	4
<b>BAB II LANDASAN TEORI</b> .....	<b>5</b>
2.1 Mikrotik.....	5
2.2 Port Knocking.....	6
2.3 Firewall.....	6
2.4 Hacking.....	7
2.5 Router .....	7
2.6 Jaringan Komputer .....	7
2.6.1 Topologi Jaringan.....	7
2.7 Keamanan Jaringan.....	10
2.7.1 Bentuk Ancaman Jaringan Komputer.....	11
2.7.2 Metode Penyerang Jaringan Komputer .....	12



2.8	Winbox .....	13
2.9	Secure Shell (SSH) .....	13
2.10	Cisco Packet Tracer .....	13
2.11	Penelitian Terdahulu.....	14
<b>BAB III METODOLOGI PENELITIAN .....</b>		<b>19</b>
3.1	Model Penelitian.....	19
3.2	Tahapan PPDIOO .....	19
3.3	Teknik Pengumpulan Data .....	20
3.4	Alat Bantu Pengujian Jaringan .....	21
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>		<b>22</b>
4.1	Latar Belakang Organisasi.....	23
4.2	Struktur Organisasi .....	23
4.3	Visi dan Misi .....	23
4.3.1	Visi Bengkel Jaya Pratama .....	23
4.3.2	Misi Bengkel Jaya Pratama .....	23
4.4	Analisis Sistem Yang Berjalan .....	24
4.4.1	Pemecahan Masalah .....	24
4.4.2	Analisis Kebutuhan Sistem Usulan.....	26
4.5	Rancangan Sistem.....	26
4.5.1	Activity Diagram .....	26
4.5.2	Deployment Diagram .....	26
4.5.3	Rancangan Aplikasi .....	27
4.5.4	Manajemen Jaringan Usulan .....	27
4.5.5	Pemecahan Masalah .....	28
4.6	Konfigurasi Hardware .....	28
4.6.1	Konfigurasi Mikrotik Sebagai Router Gateway Internet.....	28
4.6.2	Konfigurasi Metode Port Knocking Pada Mikrotik .....	30
4.7	Pengujian Sistem Implementasi.....	35

<b>BAB V KESIMPULAN DAN SARAN</b> .....	<b>37</b>
5.1 Kesimpulan.....	37
5.2 Saran.....	37
<b>DAFTAR PUSTAKA</b> .....	<b>38</b>
<b>LAMPIRAN</b> .....	<b>40</b>



## DAFTAR GAMBAR

Gambar 2.1 Gambaran PPDIOO .....	5
Gambar 2,2 Mikrotik RB750 .....	7
Gambar 2.3 Firewall .....	8
Gambar 2.4 Topologi Bus.....	10
Gambar 2.5 Topologi Star.....	11
Gambar 2.6 Topologi Ring .....	11
Gambar 2.7 Topologi Mesh .....	12
Gambar 4.1 Struktur.....	25
Gambar 4.2 Activity Diagram Jaringan Awal .....	27
Gambar 4.3 Activity Diagram Usulan .....	28
Gambar 4.4 Deployment Diagram.....	29
Gambar 4.5 Add IP Address .....	31
Gambar 4.6 Penambahan DNS Mikrotik .....	32
Gambar 4.7 Tampilan NAT .....	32
Gambar 4.8 Tampilan Firewall General Rule 1 .....	33
Gambar 4.9 Tampilan Action Rule 1 .....	33
Gambar 4.10 Tampilan Firewall General Rule 2 .....	34
Gambar 4.11 Tampilan Advance Rule 2.....	34
Gambar 4.12 Tampilan Action Rule 2.....	35
Gambar 4.13 Tampilan Firewall General Rule 3 .....	35
Gambar 4.14 Tampilan Advance Rule 3.....	36
Gambar 4.15 Tampilan Action Rule 3 .....	36
Gambar 4.16 Tampilan Firewall General Rule 4.....	37
Gambar 4.17 Tampilan Advanced Rule 4.....	37
Gambar 4.18 Tampilan Action Rule 4.....	37
Gambar 4.19 Hasil Pengujian PING ke Router .....	38
Gambar 4.20 Hasil Pengujian Pertama .....	38
Gambar 4.21 Hasil Pengujian Kedua.....	39
Gambar 4.22 Hasil Pengujian Ketiga.....	39

## DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu .....	16
Tabel 4.1 Kebutuhan Perangkat Keras .....	28
Tabel 4.2 Kebutuhan Perangkat Lunak .....	28
Tabel 4.3 Spesifikasi Hardware.....	29
Tabel 4.4 Spesifikasi Software.....	30

