

**LAPORAN AKHIR**

**IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) PADA  
KEAMANAN JARINGAN DENGAN NOTIFIKASI BERBASIS  
TELEGRAM DI JURUSAN TEKNIK KOMPUTER**



**Laporan ini disusun untuk memenuhi syarat menyelesaikan  
Pendidikan Diploma III Jurusan Teknik Komputer  
Politeknik Negeri Sriwijaya**

**Oleh :**

**Azzahra Rahmatillah  
061830701113**

**JURUSAN TEKNIK KOMPUTER  
POLITEKNIK NEGERI SRIWIJAYA  
PALEMBANG  
2021**

**LEMBAR PERSETUJUAN LAPORAN AKHIR**

**IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) PADA  
KEAMANAN JARINGAN DENGAN NOTIFIKASI BERBASIS  
TELEGRAM DI JURUSAN TEKNIK KOMPUTER**



Oleh :

Azzahra Rahmatillah (061830701113)

Palembang, Agustus 2021

Pembimbing I

Ema Laila, S.Kom., M.Kom  
NIP. 197703292001122002

Pembimbing II

Ali Firdaus, S.Kom, M.Kom  
NIP. 197010112001121001

Mengetahui,

Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T  
NIP. 197005232005011004

IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) PADA  
KEAMANAN JARINGAN DENGAN NOTIFIKASI BERBASIS  
TELEGRAM DI JURUSAN TEKNIK KOMPUTER



Telah diuji dan dipertahankan di depan dewan penguji pada sidang  
Laporan Akhir pada Senin, 26 Juli 2021

Ketua Dewan Penguji

Ema Laila, S.Kom., M.Kom  
NIP. 197703292001122002

Anggota Dewan Penguji

Slamet Widodo, S.Kom., M.Kom  
NIP. 197305162002121001

Isnainy Azro, S.Kom., M.Kom  
NIP. 197310012002122002

Ikhtison Mekongga, S.T., M.Kom  
NIP. 197705242000031002

Adi Sutrisman, S.Kom., M.Kom  
NIP. 197503052001121005

Tanda Tangan

Mengetahui,  
Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T  
NIP. 197005232005011004

## MOTTO

*“Tidaklah mungkin bagi matahari mengejar bulan dan malampun tidak dapat mendahului siang. Masing-masing beredar pada garis edarnya”*

*(Q.S. Yasin : 40)*

Kupersembahkan kepada:

- Keluargaku
- Dosen Pembimbingku Ibu  
Ema Laila, S. Kom., M.Kom dan Pak Ali  
Firdaus, S. Kom., M.Kom terima kasih  
banyak atas bimbingannya.
- Rekan-rekan Seperjuangan 6CF
- Almamaterku Politeknik Negeri  
Sriwijaya

## ABSTRAK

### “IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) PADA KEAMANAN JARINGAN DENGAN NOTIFIKASI BERBASIS TELEGRAM DI JURUSAN TEKNIK KOMPUTER”

---

---

(Azzahra Rahmatillah, 2021: 79 Halaman)

*Intrusion Prevention System (IPS)* adalah perangkat lunak yang berkerja untuk mendeteksi aktifitas yang mencurigakan dan melakukan pencegahan terhadap intrusi pada jaringan. Pada router *MikroTik* yang menyediakan beberapa fasilitas untuk mendukung keamanan dan akses jaringan dapat diterapkan sebuah sistem untuk mendeteksi jika terjadi penyerangan pada jaringan komputer. Serangan atau penyusupan dapat dicegah dengan menerapkan *Intrusion Prevention System* dan serangan dapat terdeteksi tergantung pada pola serangan yang ada di dalam rule IPS. Administrator *system* dapat mengetahui serangan yang terjadi pada *server internet* melalui pesan notifikasi yang memuat informasi jenis serangan dan kapan terjadinya yang dikirim oleh *system* yang dibuat melalui *Telegram*.

**Kata Kunci:** IPS (Intrusion Prevention System), MikroTik, Deteksi Serangan, Telegram.

## **ABSTRACT**

### **" IMPLEMENTATION OF INTRUSION PREVENTION SYSTEM (IPS) IN NETWORK SECURITY WITH NOTIFICATION-BASED TELEGRAM IN COMPUTER ENGINEERING"**

---

---

**(Azzahra Rahmatillah, 2021: 79 Pages)**

Intrusion Prevention System (IPS) is software that works to detect suspicious activity and prevent intrusion on the network. On MikroTik routers that provide several facilities to support security and network access can be applied a system to detect in case of attacks on computer networks. Attacks or intrusions can be prevented by implementing the Intrusion Prevention System and attacks can be detected depending on the pattern of attacks contained in the IPS rules. System administrators can know the attacks that occur on internet servers through notification messages containing information on the type of attack and when it occurred sent by the system created through Telegram.

**Key Words : IPS (Intrusion Detection System), MicroTic, Attack Detection, Telegram.**

## KATA PENGANTAR

Assalamu'alaikum Warramatullahi Wabarakatuh.

Puji syukur penulis ucapkan atas kehadiran Allah Subhanahu Wata'ala. yang telah memberikan rahmat dan hidayah-nya sehingga penulis dapat menyelesaikan laporan akhir dengan judul **“Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram di Jurusan Teknik Komputer”**.

Laporan akhir ini disusun dalam rangka melengkapi persyaratan kurikulum untuk menyelesaikan Pendidikan Diploma III Teknik Komputer di Politeknik Negeri Sriwijaya Palembang.

Pada kesempatan ini penulis ingin mengucapkan terima kasih kepada berbagai pihak yang telah memberikan bantuan kepada penulis dalam penyelesaian laporan akhir ini, khususnya kepada:

1. Allah SWT Yang telah memberikan kemudahan dan kelancaran untukku sehingga dapat menyelesaikan laporan akhir ini.
2. Orangtua dan saudara tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar selama ini.
3. Bapak Dr. Ing Ahmad Taqwa, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
4. Bapak Azwardi, S.T., M.T. selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
5. Bapak Yulian Mirza, S.T., M.Kom. selaku Sekretaris Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
6. Ibu Ema Laila, S.Kom., M.Kom selaku Pembimbing I.
7. Bapak Ali Firdaus, S.Kom, M.Kom selaku Pembimbing II.
8. Seluruh Bapak/Ibu Dosen Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.

9. Staff administrasi Jurusan Teknik Komputer yang telah membantu segala kepentingan perihal administrasi dan akademik selama proses penyusunan laporan akhir ini hingga selesai.
10. Teman-teman seperjuangan 6CF Teknik Komputer 2018.
11. Seluruh Rekan-rekan Mahasiswa Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.

Semoga laporan akhir ini dapat dipahami dan diterima, agar selanjutnya dapat mengerjakan sepenuhnya bahwa banyak terdapat kekurangan baik dalam penyajian ataupun isi dari laporan ini, mengingat kurangnya pengetahuan dan pengalaman penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang bersifat membangun guna penyempurnaan penulisan berikutnya.

Palembang, Juli 2021

Penulis

Azzahra Rahmatillah

## DAFTAR ISI

<b>HALAMAN JUDUL .....</b>	<b>i</b>
<b>HALAMAN PENGESAHAN .....</b>	<b>ii</b>
<b>MOTTO .....</b>	<b>iv</b>
<b>ABSTRAK .....</b>	<b>v</b>
<b>KATA PENGANTAR .....</b>	<b>vii</b>
<b>DAFTAR ISI .....</b>	<b>ix</b>
<b>DAFTAR GAMBAR.....</b>	<b>xii</b>
<b>DAFTAR TABEL .....</b>	<b>xvii</b>
<b>I PENDAHULUAN</b>	
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah .....	2
1.3. Batasan Masalah.....	2
1.4. Tujuan dan Manfaat .....	3
1.4.1. Tujuan.....	3
1.4.2. Manfaat.....	3
<b>II TINJAUAN PUSTAKA</b>	
2.1. Penelitian Terdahulu.....	4
2.2. Jaringan Komputer.....	5
2.3. Jenis – jenis jaringan .....	5
2.4. Topologi Jaringan .....	8
2.4.1. Topologi Jaringan Bus.....	8
2.4.2. Topologi Jaringan Ring .....	8
2.4.3. Topologi Jaringan Start .....	9
2.4.4. Topologi Jaringan Tree.....	9

2.4.5. Topologi Jaringan Mesh .....	10
2.5. Intrusion Prevention Sistem (IPS) .....	10
2.5.1. Host Based IPS (HIPS).....	11
2.5.2. Network Based IPS (NIPS) .....	12
2.6. <i>Firewall</i> .....	14
2.7. <i>Router</i> .....	14
2.7.1. Jenis router.....	15
2.7.2. Fungsi <i>Router</i> .....	16
2.8. <i>Mikrotik RouterOS</i> .....	16
2.9. Aplikasi Winbox.....	19
2.9.1. Fungsi Winbox .....	19
2.10. Jenis Serangan pada Jaringan Komputer .....	19
2.10.1. Port Scanning(Nmap).....	19
2.10.2. Telnet Brute Force.....	19
2.10.3. SSH Brute Force.....	20
2.10.4. FTP Brute Force .....	20
2.11. Perl .....	20
2.12. Telegram .....	21
2.13. Flowchart .....	21
2.13.1. Simbol-simbol Flowchart .....	21

### **III RANCANG BANGUN**

3.1. Perancangan Sistem.....	26
3.2. Diagram Alir Rancang Bangun Sistem .....	27
3.3. Rancang Bangun Jaringan .....	28
3.3.1 Skema Penyerangan .....	28
3.4. Rancangan Pengalamanan IP .....	29
3.5. Konfigurasi.....	30

3.5.1. Konfigurasi Wlan .....	30
3.5.2. Konfigurasi Mikrotik .....	33
3.5.2.1. Konfigurasi DHCP ( <i>Dynamic Host Configuration Protocol</i> ).....	33
3.6. Konfigurasi IPS .....	43
3.6.1. Brute force SSH .....	44
3.6.2. Brute force FTP .....	46
3.6.3. Brute force Telnet.....	49
3.6.4. Port Scanner .....	51
3.7. Bot Telegram.....	54
3.8. Mengkoneksikan Mikrotik ke Bot Telegram .....	58
3.9. Komponen Pengujian .....	61
<b>IV HASIL DAN PEMBAHASAN</b>	
4.1. Koneksi Internet .....	63
4.2. IPS (Intrusion Prevention System) dan Notifikasi Telegram.....	63
4.2.1. Brute force SSH .....	64
4.2.2. Brute force FTP .....	68
4.2.3. Brute force Telnet.....	73
4.2.4. Port Scanner .....	77
4.3. Hasil Pengujian System.....	81
<b>V PENUTUP</b>	
5.1. Kesimpulan.....	74
5.2. Saran.....	74

## DAFTAR PUSTAKA

## LAMPIRAN

## DAFTAR GAMBAR

<b>Gambar 2.1.</b>	PAN ( <i>Personal Area Network</i> ) .....	6
<b>Gambar 2.2.</b>	MAN ( <i>Metropolitan Area Network</i> ) .....	6
<b>Gambar 2.3.</b>	LAN ( <i>Local Area Network</i> ) .....	7
<b>Gambar 2.4.</b>	WAN ( <i>Wide Area Network</i> ) .....	7
<b>Gambar 2.5.</b>	Topologi <i>Bus</i> .....	8
<b>Gambar 2.6.</b>	Topologi <i>Ring</i> .....	9
<b>Gambar 2.7.</b>	Topologi <i>Star</i> .....	9
<b>Gambar 2.8.</b>	Topologi <i>Tree</i> .....	10
<b>Gambar 2.9.</b>	Topologi <i>Mesh</i> .....	10
<b>Gambar 2.10.</b>	<i>Router</i> .....	14
<b>Gambar 2.11.</b>	<i>MikroTik</i> .....	17
<b>Gambar 3.1.</b>	Blok Diagram .....	24
<b>Gambar 3.2.</b>	Diagram Alir .....	25
<b>Gambar 3.3.</b>	Rancangan Jaringan .....	26
<b>Gambar 3.4.</b>	Skema Penyerangan .....	27
<b>Gambar 3.5.</b>	<i>Wifi Interface</i> .....	28
<b>Gambar 3.6.</b>	<i>Wireless</i> .....	28
<b>Gambar 3.7.</b>	<i>IP Address</i> .....	28
<b>Gambar 3.8.</b>	Pengalamatan <i>WLAN</i> .....	28
<b>Gambar 3.9.</b>	<i>Menu Setup</i> .....	28
<b>Gambar 3.10.</b>	<i>DHCP Server Interface</i> .....	29
<b>Gambar 3.11.</b>	<i>DHCP Address Space</i> .....	29
<b>Gambar 3.12.</b>	<i>Gateway for DHCP Network</i> .....	29
<b>Gambar 3.13.</b>	<i>Address to Give Out</i> .....	29
<b>Gambar 3.14.</b>	<i>DNS Server</i> .....	30
<b>Gambar 3.15.</b>	<i>Lease Time</i> .....	30

<b>Gambar 3.16.</b> DHCP Setup berhasil .....	30
<b>Gambar 3.17.</b> Wlan1 pada DHCP server .....	30
<b>Gambar 3.18.</b> DHCP Client .....	31
<b>Gambar 3.19.</b> Tampilan Menu DHCP Client.....	31
<b>Gambar 3.20.</b> New DHCP Client.....	32
<b>Gambar 3.21.</b> DHCP Client ether1 .....	32
<b>Gambar 3.22.</b> Address List.....	33
<b>Gambar 3.23.</b> Pengalamatan Interface.....	33
<b>Gambar 3.24.</b> DHCP Sever pada Menu IP.....	33
<b>Gambar 3.25.</b> DHCP Setup pada DHCP Server .....	34
<b>Gambar 3.26.</b> DHCP Server Interface .....	34
<b>Gambar 3.27.</b> DHCP Address Space.....	34
<b>Gambar 3.28.</b> Gateway for DHCP Network.....	34
<b>Gambar 3.29.</b> Addresses to Give Out.....	35
<b>Gambar 3.30.</b> DNS Servers.....	35
<b>Gambar 3.31.</b> Lease Time .....	35
<b>Gambar 3.32.</b> DHCP Setup berhasil .....	35
<b>Gambar 3.33.</b> DHCP Server.....	36
<b>Gambar 3.34.</b> Menu DNS.....	36
<b>Gambar 3.35.</b> DNS Settings.....	37
<b>Gambar 3.36.</b> Menu Firewall pada IP.....	37
<b>Gambar 3.37.</b> Menu NAT .....	37
<b>Gambar 3.38.</b> General pada New NAT Rule.....	38
<b>Gambar 3.39.</b> Action pada New NAT Rule.....	38
<b>Gambar 3.40.</b> Tampilan NAT .....	39
<b>Gambar 3.41.</b> Cek koneksi internet.....	39
<b>Gambar 3.42.</b> Menu Firewall.....	40
<b>Gambar 3.43.</b> Filter Rules.....	40

<b>Gambar 3.44.</b> <i>General Brute force SSH</i> .....	40
<b>Gambar 3.45.</b> <i>Advanced Brute force SSH</i> .....	41
<b>Gambar 3.46.</b> <i>Action Brute Force SSH</i> .....	41
<b>Gambar 3.47.</b> <i>General Brute Force FTP</i> .....	42
<b>Gambar 3.48.</b> <i>Advanced Brute force FTP</i> .....	43
<b>Gambar 3.49.</b> <i>Action Brute Force FTP</i> .....	43
<b>Gambar 3.50.</b> <i>General Brute Force Telnet</i> .....	44
<b>Gambar 3.51.</b> <i>Advanced Brute Force Telnet</i> .....	45
<b>Gambar 3.52.</b> <i>Action Brute Force Telnet</i> .....	45
<b>Gambar 3.53.</b> <i>General Port Scanner</i> .....	46
<b>Gambar 3.54.</b> <i>Advanced Port Scanner</i> .....	47
<b>Gambar 3.55.</b> <i>Action Port Scanner</i> .....	47
<b>Gambar 3.56.</b> <i>Search akun BotFather</i> .....	48
<b>Gambar 3.57.</b> <i>Tampilan akun BotFather</i> .....	49
<b>Gambar 3.58.</b> <i>Menentukan nama bot</i> .....	49
<b>Gambar 3.59.</b> <i>Balasan setelah membuat bot</i> .....	50
<b>Gambar 3.60.</b> <i>Bot pada kolom search</i> .....	50
<b>Gambar 3.61.</b> <i>Mulai percakapan</i> .....	50
<b>Gambar 3.62.</b> <i>Tampilan ID chat</i> .....	51
<b>Gambar 3.63.</b> <i>Balasan dari bot</i> .....	51
<b>Gambar 3.64.</b> <i>Logging Action</i> .....	52
<b>Gambar 3.65.</b> <i>Rules Info Logging</i> .....	52
<b>Gambar 3.66.</b> <i>Rules Warning Logging</i> .....	53
<b>Gambar 3.67.</b> <i>Rules Logging</i> .....	53
<b>Gambar 3.68.</b> <i>Schedule</i> .....	54
<b>Gambar 3.69.</b> <i>Schedule IPS</i> .....	55
<b>Gambar 4.1.</b> <i>Tes Koneksi Internet</i> .....	56
<b>Gambar 4.2.</b> <i>Password list SSH</i> .....	57

<b>Gambar 4.3.</b>	Brute Force SSH menggunakan Kali Linux .....	57
<b>Gambar 4.4.</b>	SSH gagal diakses .....	57
<b>Gambar 4.5.</b>	<i>Port dan Action Brute Force SSH</i> .....	58
<b>Gambar 4.6.</b>	Serangan SSH yang berhasil diblokir .....	58
<b>Gambar 4.7.</b>	<i>Brute Force SSH di Log</i> .....	59
<b>Gambar 4.8.</b>	<i>IP Attacker Brute Force SSH</i> .....	59
<b>Gambar 4.9.</b>	SSH pada <i>Putty</i> .....	60
<b>Gambar 4.10.</b>	SSH tidak bisa diakses .....	60
<b>Gambar 4.11.</b>	Brute Force SSH .....	61
<b>Gambar 4.12.</b>	Password List FTP .....	62
<b>Gambar 4.13.</b>	Brute Force FTP menggunakan Kali Linux .....	62
<b>Gambar 4.14.</b>	FTP gagal diakses .....	62
<b>Gambar 4.15.</b>	<i>Port dan Action Brute Force FTP</i> .....	63
<b>Gambar 4.16.</b>	Serangan FTP yang berhasil diblokir.....	63
<b>Gambar 4.17.</b>	Brute Force FTP di Log .....	63
<b>Gambar 4.18.</b>	Address List Brute Force FTP.....	64
<b>Gambar 4.19.</b>	FTP pada <i>FileZilla</i> .....	64
<b>Gambar 4.20.</b>	FTP tidak bisa diakses.....	64
<b>Gambar 4.21.</b>	Notifikasi Brute Force FTP.....	65
<b>Gambar 4.22.</b>	<i>Password List Telnet</i> .....	65
<b>Gambar 4.23.</b>	<i>Brute Force Telnet menggunakan Kali Linux</i> .....	66
<b>Gambar 4.24.</b>	Telnet gagal diakses .....	66
<b>Gambar 4.25.</b>	<i>Port dan Action Brute Force Telnet</i> .....	66
<b>Gambar 4.26.</b>	Serangan <i>Telnet</i> yang berhasil diblokir.....	67
<b>Gambar 4.27.</b>	<i>Brute Force Telnet di Log</i> .....	67
<b>Gambar 4.28.</b>	<i>IP Attacker Brute Force Telnet</i> .....	68
<b>Gambar 4.29.</b>	Telnet pada <i>Putty</i> .....	68
<b>Gambar 4.30.</b>	Telnet tidak bisa diakses .....	69

<b>Gambar 4.31.</b> Notifikasi <i>Brute Force Telnet</i> .....	69
<b>Gambar 4.32.</b> <i>Port Scanner</i> menggunakan <i>Nmap</i> .....	70
<b>Gambar 4.33.</b> Proses <i>Port Scanning</i> dengan <i>Nmap</i> .....	70
<b>Gambar 4.34.</b> Informasi Port .....	70
<b>Gambar 4.35.</b> <i>Port Scanner</i> di Log.....	71
<b>Gambar 4.36.</b> IP Attacker <i>Port Scanner</i> .....	71
<b>Gambar 4.37.</b> Notifikasi <i>Port Scanner</i> di <i>Telegram</i> .....	72

## DAFTAR TABEL

<b>Tabel 2.1.</b> <i>Flow Direction Symbols</i> (Simbol Penghubung/alur) .....	20
<b>Tabel 2.2.</b> Processing Symbols (Simbol Proses) .....	21
<b>Tabel 2.3.</b> Input/Output Symbols (Masukan/Keluaran) .....	22
<b>Tabel 3.1.</b> Alokasi Alamat IP .....	27
<b>Tabel 3.2.</b> Komponen Pengujian .....	55
<b>Tabel 4.1.</b> Hasil Pengujian.....	72