

LAPORAN AKHIR
MONITORING KEAMANAN JARINGAN MENGGUNAKAN IDS PADA
ROUTER MIKROTIK BERBASIS TELEGRAM
DI JURUSAN TEKNIK KOMPUTER



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

Oleh :

Intan Cahyani
061830701117

JURUSAN TEKNIK KOMPUTER
POLITEKNIK NEGERI SRIWIJAYA
PALEMBANG
2021

LEMBAR PERSETUJUAN LAPORAN AKHIR
MONITORING KEAMANAN JARINGAN MENGGUNAKAN IDS PADA
ROUTER MIKROTIK BERBASIS TELEGRAM
DI JURUSAN TEKNIK KOMPUTER



Oleh :

Intan Cahyani (0618 3070 1117)

Pembimbing I

Mustaziri, S.T., M.Kom
NIP. 196909282005011002

Palembang, Agustus 2021

Pembimbing II

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

Mengetahui,
Ketua Jurusan Teknik Komputer

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

**MONITORING KEAMANAN JARINGAN MENGGUNAKAN IDS PADA
ROUTER MIKROTIK BERBASIS TELEGRAM
DI JURUSAN TEKNIK KOMPUTER**



Telah diuji dan dipertahankan di depan dewan penguji pada sidang
Laporan Akhir pada Rabu, 28 Juli 2021

Ketua Dewan Penguji

Yulian Mirza, S.T., M.Kom
NIP. 196607121990031003

Anggota Dewan Penguji

Meiyi Darlies, S.Kom., M.Kom
NIP. 197805152006041003


Alan Novi Tompunu, S.T., M.T
NIP. 197611082000031002

Hartati Deviana, S.T., M.Kom
NIP. 197405262008122001

Rian Rahmanda Putra, S.Kom., M.Kom
NIP. 198901252019031013

Tanda Tangan


.....


.....


.....


.....


.....

**Mengetahui,
Ketua Jurusan Teknik Komputer**



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

MOTTO

*“Sesungguhnya sesudah kesulitan itu ada kemudahan”
(Q.S. Al-Insyirah : 6)*

*“Fall in love with the process of becoming the very best
version of yourself”
-Mau Belajar|Apa*

*“Bahagia itu bukanlah ketika kita nggak punya masalah,
tetapi ketika kita punya masalah dan berhasil
melaluinya!”
-@rahasiagadis*

Kupersembahkan kepada:

- ♡ Allah SWT dan Nabi Muhammad SAW
- ♡ My Family
- ♡ Dosen Pembimbingku Bapak Mustaziri, S.T., M.Kom dan Ikhthison Mekongga, S.T., M.Kom terima kasih banyak atas bimbingannya.
- ♡ Rekan-rekan Seperjuangan 6CF
- ♡ Almamaterku Politeknik Negeri Sriwijaya

ABSTRAK

“MONITORING KEAMANAN JARINGAN MENGGUNAKAN IDS PADA ROUTER MIKROTIK BERBASIS TELEGRAM DI JURUSAN TEKNIN KOMPUTER”

(Intan Cahyani, 2021: 65 Halaman)

IDS (*Intrusion Detection System*) merupakan suatu sistem yang dapat mendeteksi aktifitas mencurigakan dan memberikan laporan terhadap aktifitas jaringan komputer. 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. *Intrusion Detection System* yang diterapkan pada *router MikroTik* dapat mendeteksi berbagai aktifitas penyerangan sesuai dengan *rule* yang telah ditentukan seperti *Brute forces login* pada *MikroTik* menggunakan SSH, Telnet, FTP, dan *Winbox*, serta jenis serangan *port scanning*. Kemudian sistem akan memberikan laporan melalui Telegram secara *realtime* mengenai adanya serangan yang mencoba masuk kedalam sistem.

Kata Kunci : IDS (*Intrusion Detection System*), MikroTik, Deteksi Serangan, Telegram.

ABSTRACT

"MONITORING NETWORK SECURITY USING IDS ON MICROTIC ROUTER BASED ON TELEGRAM IN COMPUTER ENGINEERING DEPARTMENT"

(Intan Cahyani, 2021: 65 Pages)

IDS (Intrusion Detection System) is a system that can detect suspicious activity and provide reports on computer network activity. On a MicroTic router that provides several facilities to support network security and access, a system can be applied to detect if an attack occurs on a computer network. The Intrusion Detection System applied to MicroTic routers can detect various attack activities according to predetermined rules such as Brute forces login on MicroTic using SSH, Telnet, FTP, and Winbox, as well as types of port scanning. Then the system will provide reports via Telegram in real time regarding any attacks that try to enter the system.

Kata Kunci : IDS (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 **“Monitoring Keamanan Jaringan Menggunakan IDS Pada Router MikroTik 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. Bapak Mustaziri, S.T., M.Kom. selaku Pembimbing I.
7. Bapak Ikhtison Mekongga, S.T., 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, Agustus 2021

Penulis

Intan Cahyani

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
MOTTO	iv
ABSTRAK	v
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR.....	xii
DAFTAR TABEL	xv
I PENDAHULUAN	
1.1. Latar Belakang	1
1.2. RumusanMasalah	2
1.3. BatasanMasalah.....	2
1.4. Tujuan dan Manfaat	3
1.4.1. Tujuan.....	3
1.4.2. Manfaat.....	3
II TINJAUAN PUSTAKA	
2.1. Penelitian Terdahulu	4
2.2. Sistem Jaringan di Jurusan Teknik Komputer	6
2.3. <i>Monitoring</i>	6
2.4. Jaringan Komputer	6
2.4.1. Jenis – jenis jaringan.....	7
2.5. <i>IDS (Intrusion Detection System)</i>	8
2.6. <i>Router</i>	9
2.7. <i>MikroTik Router OS</i>	9
2.8. Winbox	10
2.9. Media Transmisi Jaringan Komputer (<i>Wire Network</i>)	11
2.9.1. Jaringan Berkabel (<i>Wired Network</i>)	11
2.9.2. Jaringan Nirkabel (Wi-Fi)	13
2.10.Topologi Jaringan	13
2.10.1. Jenis – jenis Topologi Jaringan	14

2.11. Firewall.....	17
2.12. Jenis Serangan pada Jaringan Komputer	17
2.12.1. Port Scanning(Nmap).....	17
2.12.2. Brute Force	17
2.12.3. Telnet Brute Force	18
2.12.4. SSH Brute Force	18
2.12.5. FTP Brute Force.....	18
2.13. Perl	18
2.14. Telegram	19
2.15. Linux Ubuntu.....	19
2.16. Flowchart.....	20

III METODE PENELITIAN

3.1. Perancangan Sistem.....	23
3.2. Diagram Alir Rancang Bangun Sistem	24
3.3. Metode Pengumpulan Data	25
3.4. Perancangan Sistem.....	25
3.4.1. Perangkat Keras(Hardware)	25
3.4.2. Perangkat Lunak(Software).....	25
3.5. Rancang Bangun Jaringan	25
3.6. Rancangan Pengalamatan IP	26
3.7. Konfigurasi.....	26
3.7.1. Konfigurasi MikroTik	27
3.7.1.1. Konfigurasi DHCP Client	27
3.7.1.2. Konfigurasi IP Address	28
3.7.1.3. Konfigurasi DHCP Server.....	29
3.7.1.4. Mengatur DNS	32
3.7.1.5. Mengatur Firewall NAT	33
3.7.2. Konfigurasi Wlan	35
3.7.3. Konfigurasi IDS	37
3.7.3.1. SSH Brute Force	38
3.7.3.2. Telnet Brute Force	41
3.7.3.3. FTP Brute Force	41

3.7.3.4. <i>Winbox Brute Force</i>	42
3.7.3.6. <i>Port Scanning</i>	42
3.8. Bot Telegram.....	43
3.9. Mengkoneksikan <i>MikroTik</i> ke Telegram	47
3.10. Skenario Pengujian.....	48
3.11. Rancangan Notifikasi Telegram.....	50

IV HASIL DAN PEMBAHASAN

4.1. Pengujian Koneksi Internet	51
4.2. Pengujian IDS (<i>Intrusion Detection System</i>)	51
4.2.1. Pengujian SSH <i>Brute Force</i>	53
4.2.2. Pengujian Telnet <i>Brute Force</i>	54
4.2.3. Pengujian <i>Winbox Brute Force</i>	55
4.2.4. Pengujian FTP <i>Brute Force</i>	56
4.2.6. Pengujian <i>Port Scanning</i>	57
4.3. Notifikasi Telegram.....	58
4.2.1. Notifikasi SSH <i>Brute Force</i>	59
4.2.2. Notifikasi Telnet <i>Brute Force</i>	60
4.2.3. Notifikasi <i>Winbox Brute Force</i>	61
4.2.4. Notifikasi FTP <i>Brute Force</i>	62
4.2.6. Notifikasi <i>Port Scanning</i>	62
4.4. Hasil Pengujian	63
4.5. Cara Kerja IDS (<i>Intrusion Detection System</i>) Pada <i>MikroTik</i>	64

V PENUTUP

5.1. Kesimpulan.....	65
5.2. Saran.....	65

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1.	Router MikroTik	9
Gambar 2.2.	Winbox.....	10
Gambar 2.3.	Kabel <i>Coaxial</i>	12
Gambar 2.4.	Kabel UTP.....	12
Gambar 2.5.	Kabel STP	13
Gambar 2.6.	Jenis - jenis Topologi	14
Gambar 3.1.	Blok Diagram	23
Gambar 3.2.	Diagram Alir	24
Gambar 3.3.	Rancangan Jaringan	26
Gambar 3.4.	DHCP <i>Client</i>	27
Gambar 3.5.	<i>New DHCP Client</i>	27
Gambar 3.6.	<i>Ether1</i> dari DHCP <i>Client</i>	28
Gambar 3.7.	<i>Address list</i>	28
Gambar 3.8.	<i>Add Address</i>	29
Gambar 3.9.	Tampilan setelah ditambah IP	29
Gambar 3.10.	DHCP <i>Server</i>	30
Gambar 3.11.	DHCP <i>Server interface</i>	30
Gambar 3.12.	DHCP <i>Address Space</i>	30
Gambar 3.13.	<i>Gateway for DHCP Network</i>	31
Gambar 3.14.	<i>Address to Give Out</i>	31
Gambar 3.15.	DNS <i>Servers</i>	31
Gambar 3.16.	<i>Lease Time</i>	32
Gambar 3.17.	Tampilan DHCP <i>Server</i>	32
Gambar 3.18.	DNS <i>Settings</i>	32
Gambar 3.19.	<i>Firewall NAT</i>	33
Gambar 3.20.	General NAT <i>Rule</i>	33
Gambar 3.21.	Action NAT <i>Rule</i>	34
Gambar 3.22.	Tampilan <i>Firewall NAT</i>	34
Gambar 3.23.	Cek <i>internet MikroTik</i>	35
Gambar 3.24.	<i>Wi-fi Interface</i>	35
Gambar 3.25.	<i>Wireless</i>	36

Gambar 3.26.	<i>Address Wlan1</i>	36
Gambar 3.27.	<i>DHCP Server Wlan</i>	37
Gambar 3.28.	<i>Filter Rule</i>	37
Gambar 3.29.	<i>IP Service List</i>	38
Gambar 3.30.	<i>SSH General</i>	38
Gambar 3.31.	<i>SSH Advanced</i>	39
Gambar 3.32.	<i>Action SSH</i>	39
Gambar 3.33.	<i>Advanced SSH Blacklist</i>	40
Gambar 3.34.	<i>Action SSH add src address list</i>	40
Gambar 3.35.	<i>BotFather</i>	43
Gambar 3.36.	<i>Add Bot</i>	44
Gambar 3.37.	<i>Newbot</i>	44
Gambar 3.38.	<i>Token Telegram</i>	45
Gambar 3.39.	<i>Search ID bot</i>	45
Gambar 3.40.	<i>Chat ID</i>	46
Gambar 3.41.	<i>Tes Bot</i>	46
Gambar 3.42.	<i>Halaman Chat bot</i>	47
Gambar 3.43.	<i>Logging Action</i>	47
Gambar 3.44.	<i>Rules Info Logging</i>	48
Gambar 3.45.	<i>Rules Warning Logging</i>	48
Gambar 3.46.	<i>Rules Logging</i>	48
Gambar 3.47.	<i>Schedule</i>	49
Gambar 3.48.	<i>Install hydra</i>	49
Gambar 3.49.	<i>File Wordlist Password</i>	50
Gambar 3.50.	<i>Rancangan Notifikasi</i>	50
Gambar 4.1.	<i>Tes Ping</i>	51
Gambar 4.2.	<i>Konfigurasi IDS</i>	52
Gambar 4.3.	<i>Tes Ping Linux</i>	52
Gambar 4.4.	<i>Cek IP Gateway Target</i>	52
Gambar 4.5.	<i>Wordlist Password</i>	53
Gambar 4.6.	<i>Pengujian Brute Force SSH</i>	53
Gambar 4.7.	<i>Peringatan Brute Force SSH</i>	54

Gambar 4.8.	Pengujian <i>Brute Force</i> Telnet	54
Gambar 4.9.	Peringatan <i>Brute Force</i> Telnet	55
Gambar 4.10.	Percobaan <i>Login Winbox</i>	55
Gambar 4.11.	Peringatan <i>Login Winbox</i>	56
Gambar 4.12.	Peringatan <i>Brute Force Winbox</i>	56
Gambar 4.13.	Pengujian FTP di Linux	57
Gambar 4.14.	Peringatan <i>Brute Force</i> FTP	57
Gambar 4.15.	<i>Port Scanning</i>	58
Gambar 4.16.	Peringatan <i>Port Scanning</i>	58
Gambar 4.17.	<i>Scheduler MikroTik</i>	59
Gambar 4.18.	Notifikasi SSH <i>Brute Force</i>	60
Gambar 4.19.	Notifikasi Telnet <i>Brute Force</i>	60
Gambar 4.20.	<i>Login Failure Winbox</i>	61
Gambar 4.21.	Notifikasi <i>Winbox Brute Force</i>	61
Gambar 4.22.	Notifikasi FTP <i>Brute Force</i>	62
Gambar 4.23.	Notifikasi <i>Port Scanning</i>	62
Gambar 4.24.	<i>Rule IDS</i>	64

DAFTAR TABEL

Tabel 2.1. Penelitian Terdahulu.....	5
Tabel 2.2. Simbol <i>Flowchart</i>	20
Tabel 2.3. <i>Processing Symbols</i> (Simbol Proses)	21
Tabel 2.4. <i>Input/Output Symbols</i> (Masukan/Keluaran).....	22
Tabel 3.1. Daftar Perangkat Keras yang Digunakan	25
Tabel 3.2. Daftar Perangkat Lunak yang Digunakan	25
Tabel 3.3. Alokasi Alamat IP	26
Tabel 4.1. Pengujian Serangan	63
Tabel 4.2. Pengujian Notifikasi Telegram.....	63