

**IMPLEMENTASI DAN ANALISIS
PENGUNAAN *INTRUSION DETECTION SISTEM* GUNA
MENCEGAH DAN MENDETEKSI SERANGAN YANG
TERDAPAT DI JARINGAN LOKAL DENGAN
MENGUNAKAN *ROUTERBOARD*
MIKROTIK *RB951-2HND***

SKRIPSI



disusun oleh

Ahmad Pugu Setiawan

17.11.1188

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

**IMPLEMENTASI DAN ANALISIS
PENGUNAAN *INTRUSION DETECTION SISTEM* GUNA
MENCEGAH DAN MENDETEKSI SERANGAN YANG
TERDAPAT DI JARINGAN LOKAL DENGAN
MENGUNAKAN *ROUTERBOARD*
MIKROTIK *RB951-2HND***

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Informatika



disusun oleh

Ahmad Pugu Setiawan

17.11.1188

**PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2022**

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI DAN ANALISIS PENGGUNAAN INTRUSION
DETECTION SYSTEM GUNA MENCEGAH DAN MENDETEKSI
SERANGAN YANG TERDAPAT DI JARINGAN LOKAL DENGAN
MENGUNAKAN ROUTERBOARD MIKROTIK RB951-2HND**

yang dipersiapkan dan disusun oleh

Ahmad Pugu Setiawan

17.11.1188

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 25 april 2022

Dosen Pembimbing,

ANDIKA AGUS SLAMETO, M.KOM

NIK. 190302109

PENGESAHAN

SKRIPSI

**IMPLEMENTASI DAN ANALISIS
PENGUNAAN *INTRUSION DETECTION SISTEM* GUNA
MENCEGAH DAN MENDETEKSI SERANGAN YANG
TERDAPAT DI JARINGAN LOKAL DENGAN
MENGUNAKAN *ROUTERBOARD*
MIKROTIK *RB951-2HND***

yang dipersiapkan dan disusun oleh

Ahmad Pugu Setiawan

17.11.1188

Telah dipertahankan di depan Dewan Penguji
pada tanggal 19 Desember 2022

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

M. Rudyanto Arief, S.T, M.T

NIK. 190302098

Aggit Ferdita Nugraha, S.T., M.Eng

NIK. 190302480

Andika Agus Slameto, M.Kom

NIK. 190302109

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 3 Januari 2023

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom.,M.Kom.

NIK. 190302096

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 29 Desember 2022



Ahmad Pugu Setiawan

17.11.1188

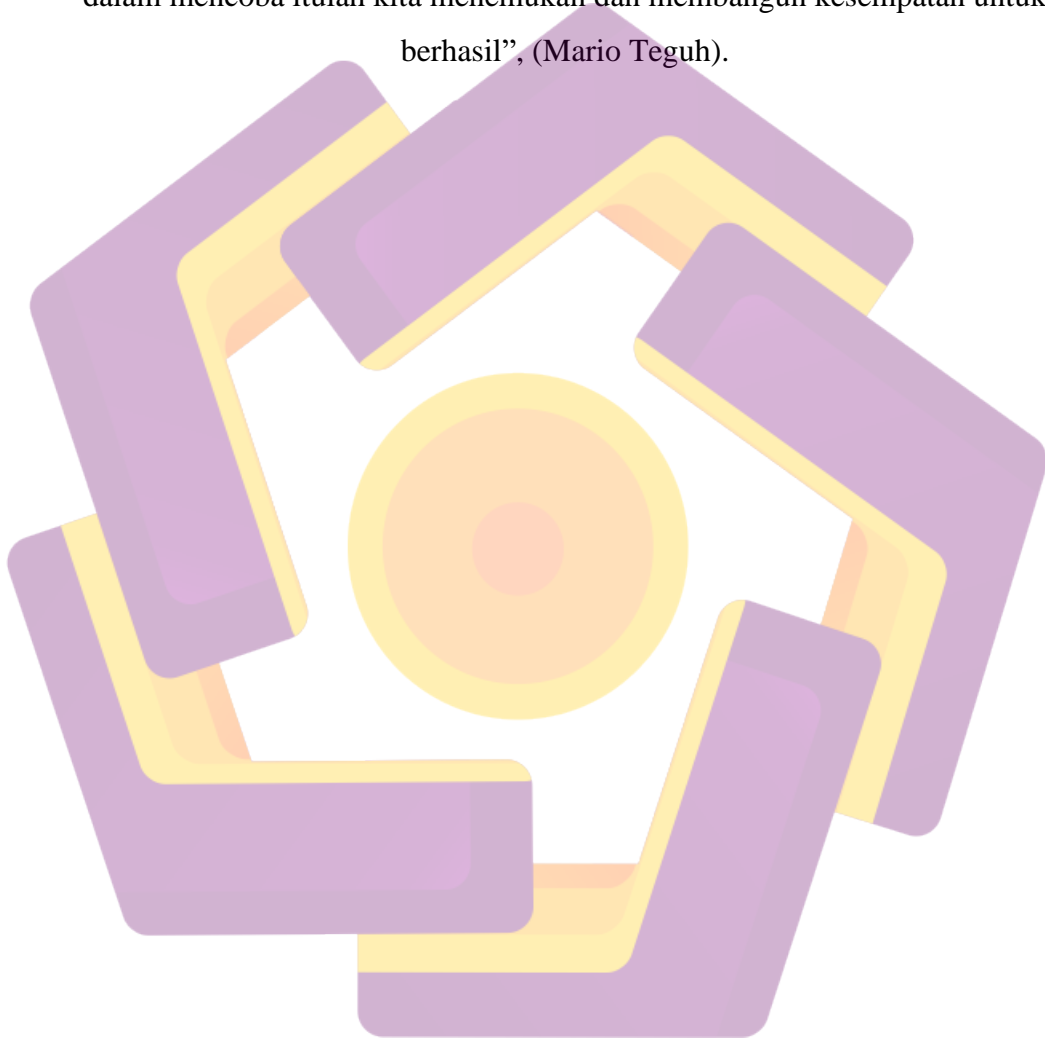
MOTTO

”kebahagian dan kebebasan dimulai dengan sebuah pemahaman yang jelas atas satu prinsip. Yaitu mana yang ada dalam kontrolmu dan mana yang bukan”

(Epictetus)

“Tugas kita bukanlah untuk berhasil, tugas kita adalah untuk mencoba, karena di dalam mencoba itulah kita menemukan dan membangun kesempatan untuk

berhasil”, (Mario Teguh).



PERSEMBAHAN

Segala puji syukur penulis panjatkan kepada Allah SWT yang telah memberikan rahmat dan hidayah-nya, sehingga penulis dapat menyelesaikan skripsi ini. Shalawat serta salam penulis panjatkan kepada Nabi Muhammad SAW yang telah membawa tauladan kepada kehidupan seluruh umat manusia dan membawa dunia dari zaman gelapnya ilmu pengetahuan sehingga zaman yang terang benderang seperti saat ini. Dalam penulisan naskah skripsi ini penulis akan mengucapkan rasa syukur dan terimakasih kepada :

1. Orang tua yang telah memberikan semangat dan motivasi penuh serta doa setiap hari agar berjalan dengan baik.
2. Bapak Andika Agus Slameto, M.Kom. selaku pembimbing skripsi ini yang telah banyak memberikan arahan skripsi ini.
3. Ibu dan Bapak Dosen Universitas AMIKOM Yogyakarta yang telah memberikan ilmu yang bermanfaat.
4. Teman-teman kos maupun teman-teman S1 Informatika 17-S1IF-04 yang telah *mensupport* skripsi ini.
5. Semua pihak yang telah membantu kelancaran dalam penyusunan naskah skripsi yang tidak dapat di tulis satu-pesatu.

KATA PENGANTAR

Puji dan syukur kehadiral Allah SWT, yang telah melimpakan rahmat seta hidayah-Nya dan salawat serta salam juga tidak lupa kita panjatkan kepada junjungan kita Nabi Muhammad SAW yang telah membawa kita kea lam yang gelap gulita ke menuju alam yang terang seperti yang kita nikmati saat ini.

Skripsi yang berjudul “Implementasi Dan Analisis Penggunaan *Intrusion Detection Sistem* Guna Mencegah Dan Mendeteksi Serangan Yang Terdapat Di Jaringan Lokal Dengan Menggunakan *Routerboard* Mikrotik *Rb951-2hnd*” yang disusun sebagai syarat untuk mendapatkan gelar sarjana di Universitas Amikom Yogyakarta.

Penyelesaian skripsi ini tidak lepas juga dari keterlibatan orang orang dibawah ini maka dari itu penulis pada kesempatan ini ingin menyampaikan rasa hormat saya kepada :

1. Allah SWT yang telah memberikan kekuatan serta ridhonya kepada kami sehingga dapat menyelesaikan skripsi ini.
2. Prof. Dr. M. Suyanto, MM. Selaku Rektor Universitas AMIKOM Yogyakarta
3. Bapak Hanif Al Fatta, S.Kom., M.Kom. Selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta.
4. Ibu Windha Mega Pradnya Dhuhita, M.Kom. Selaku Ketua Program Studi Informatika Universitas AMIKOM Yogyakarta.
5. Bapak Andika Agus Slameto, M.Kom. Selaku Dosen Pembimbing yang selalu bijaksana memberikan Bimbingan, nasehat serta waktunya selama penulisan skripsi ini.

Skripsi ini masih jauh dari kata sempurna, maka dari itu kritik dan saran yang membangun serta teguran dari semua pihak dikarenakan keterbatasan pengetahuan oleh penulis. Semoga skripsi ini bermanfaat bagi penulis dan pembaca, Khususnya dalam bidang keamanan jaringan

Yogyakarta, ---

Ahmad Pugu Sertiawan

17.11.1188

DAFTAR ISI

Judul	i
Persetujuan	ii
Pengesahan	iii
Pernyataan	iv
Motto	v
Persembahan.....	vi
Kata Pengantar.....	vii
Daftar Isi.....	viii
Daftar Gambar.....	xii
Daftar Tabel.....	xiv
Intisari.....	xv
Abstract.....	xvi
BAB I PENDAHULUAN	1
1.1. Latar Belakang.....	1
1.2. Rumusan Masalah	3
1.3. Batasan masalah	3
1.4. Maksud dan Tujuan	4
1.5. Manfaat penelitian	4
1.6. Metodologi Penelitian	5
1.1.1. <i>Metode</i> Pengumpulan Data.....	5
1.1.2. <i>Metode</i> Analisa dan Perancangan.....	5
1.7. Sistematika Penulisan.....	7
BAB II LANDASAN TEORI	9

2.1.	Tinjauan Pustaka	9
2.2.	Dasar Teori	13
2.2.1.	<i>Mikrotik</i>	14
2.2.2.	<i>RouterOS</i>	15
2.2.3.	<i>Server</i>	16
2.2.3.1.	Cara kerja <i>Server</i>	16
2.2.4.	NMAP (<i>Network Mapper</i>).....	17
2.2.5.	Sistem Operasi.....	18
2.2.5.1.	Fungsi Adanya Sistem Operasi	18
2.2.6.	<i>firewall</i>	20
2.2.6.1.	Beberapa Tipe <i>Firewall</i>	20
2.2.7.	<i>DHCP Server</i>	23
2.2.7.1.	Fungsi dari <i>DHCP Server</i>	23
2.2.8.	<i>DHCP Client</i>	24
2.2.9.	<i>Hacker</i> (peretas)	24
2.2.9.1.	Jenis-jenis peretas (<i>Hacker</i>)	25
2.2.10.	<i>Router</i>	28
2.2.10.1.	Fungsi <i>router</i>	28
2.2.11.	DOS (<i>denial of service</i>).....	30
2.2.12.	<i>DDOS</i> (<i>Distributed Denial Of Service</i>).....	30
2.2.13.	Protokol jaringan	32
2.2.13.1.	DNS (<i>domain name sistem</i>).....	33
2.2.13.2.	<i>TCP/IP</i>	33
2.2.14.	<i>Telnet</i> (<i>telecommunication Network</i>).....	35

2.2.15.	<i>SSH (secure shell)</i>	36
2.2.16.	<i>OSI Layer</i>	36
2.2.17.	<i>Topologi jaringan</i>	38
2.2.18.	<i>IDS</i>	45
2.2.19.	<i>Port knocking</i>	46
2.2.20.	<i>Limit Ping flood</i>	46
2.2.21.	<i>Port Scan Detection</i>	46
BAB III METODE PENELITIAN		48
3.1.	Gambaran umum penelitian.....	48
3.2.	Analisa	49
3.2.1.	Analisa kebutuhan fungsional	49
3.2.2.	Analisa Kebutuhan nonfungsional	50
3.3.	Alat dan bahan penelitian	50
3.3.1.	Alat	50
3.3.2.	Bahan	51
3.4.	Alur penelitian	53
3.5.	Desain	54
3.5.1.	Rancangan <i>Metode</i>	54
3.6.	<i>Topologi Jaringan</i>	56
BAB IV HASIL DAN PEMBAHASAN		63
4.1	Implementasi	63
4.1.1	<i>Port Knocking</i>	64
4.1.2	Membuat target <i>port knocking</i>	64
4.1.3	Memberlakukan akses terpercaya.....	65

4.1.4	Menangkap akses dengan <i>IP</i> terlarang	66
4.1.5	<i>Blocking access</i> pada label dilarang	67
4.1.6	<i>Limit ping Flooding</i>	68
4.1.7	<i>Port Scan Detection</i>	69
4.1.8	Menangkap <i>IP port Scanner</i>	69
4.1.9	<i>Blocking IP port Scanner</i>	71
4.2	Pengujian.....	72
4.2.1	Pengujian <i>port knocking</i>	72
4.2.2	<i>Blocking port 1000</i>	73
4.2.3	Melakukan akses pada <i>port 22</i>	74
4.2.4	Simulasi akses <i>port 22</i> tanpa <i>knocking</i>	76
4.2.5	<i>Limit ping Flooding</i>	77
4.2.6	<i>Port Scan Detection</i>	79
4.3	Hasil dan Pembahasan	81
4.3.1	Hasil pengujian fitur	81
4.3.2	Hasil berdasarkan penerapan fitur secara langsung.....	84
BAB V PENUTUP		86
5.1	Kesimpulan	86
5.2	Saran.....	86
LAMPIRAN 1		91
LAMPIRAN 2		92

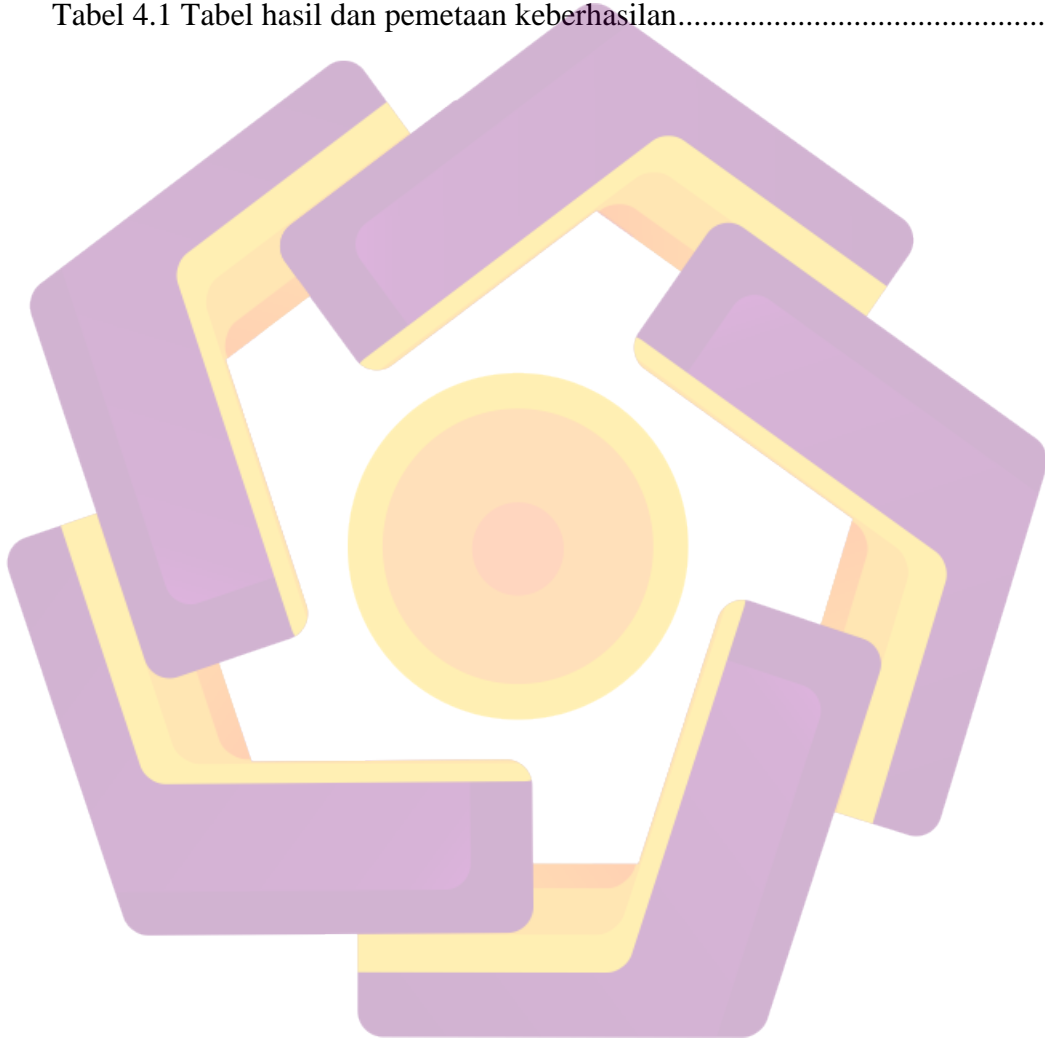
DAFTAR GAMBAR

Gambar 2.1 <i>Routerboard</i> RB941-2nD (sumber : mikrotik.co.id).....	14
Gambar 2.2 Contoh tampilan TERMINAL sistem operasi <i>routerOS</i>	15
Gambar 2.3 <i>server</i> (sumber : mskglobal.net).....	16
Gambar 2.4 <i>logo</i> NMAP	17
Gambar 2.5 contoh sistem oprasi yang paling terkenal	18
Gambar 2.6 <i>firewall</i> (sumber : calesmart.com).....	20
Gambar 2.7 contoh <i>router</i> 24 port (sumber : dlink.co.id).....	28
Gambar 2.8 Contoh mekanisme penggunaan DNS (Sumber : binus.ac.id).....	33
Gambar 2.9 Contoh mekanisme penggunaan <i>telnet</i>	35
Gambar 2.10 Cara kerja OSI <i>Layer</i> (sumber: komputerNetworkingnotes.co.id)	36
Gambar 2.11 <i>topologi</i> Bus (sumber : jetorbit.com)	39
Gambar 2.12 <i>Topologi</i> ring (sumber : pelampil.com)	40
Gambar 2.13 <i>Topologi</i> star (sumber : jetorbit.com).....	41
Gambar 2.14 <i>Topologi</i> mesh (sumber : dOSen pendidikan.co.id).....	42
Gambar 2.15 <i>Topologi</i> tree (sumber : dOSen pendidikan.co.id)	43
Gambar 2.16 <i>topologi</i> peer to peer (sumber : maxmanroe.com)	44
Gambar 3.1 Alur flowchart <i>metode</i> penelitian.....	53
Gambar 3.2 <i>Topologi</i> Penelitian	57
Gambar 4.1 Gambar <i>Prototype</i>	63
Gambar 4.2 Membuat akses target <i>port knocking</i>	65
Gambar 4.3 Penambahan label <i>SAFE-IP</i>	66
Gambar 4.4 Menambahkan label Dilarang pada <i>IP</i> attacker	67
Gambar 4.5 <i>Drop</i> pada access <i>IP</i> terkecuali <i>SAFE IP</i>	67

Gambar 4.6 <i>Limitasi Paket ICMP</i>	68
Gambar 4.7 <i>Blocking</i> paket yang tidak normal.....	69
Gambar 4.8 Menangkap <i>IP</i> pelaku <i>port Scanner</i>	70
Gambar 4.9 <i>Blocking</i> access pada <i>IP</i> attacker	72
Gambar 4.10 Mekanisme <i>rules port knocking</i>	72
Gambar 4.11 Proses <i>blocking port</i> 1000 dengan aplikasi <i>putty.exe</i>	74
Gambar 4.12 Akses sementara pada mekanisme <i>knocking port</i> 1000.....	74
Gambar 4.13 Akses <i>IP router</i> dengan menggunakan <i>port</i> 22.....	75
Gambar 4.14 Penambahan <i>IP</i> pada " <i>SAFE-ip</i> "	75
Gambar 4.15 Contoh kasus akses <i>port</i> 22 tanpa <i>knocking</i>	76
Gambar 4.16 <i>Drop connection</i> pada <i>IP</i> penyusup	76
Gambar 4.17 CPU over load	77
Gambar 4.18 <i>Router</i> mati secara otomatis	78
Gambar 4.19 <i>Byte</i> paket yang di <i>drop</i>	78
Gambar 4.20 CPU tidak over load.....	79
Gambar 4.21 Proses <i>Scanning port</i>	80
Gambar 4.22 <i>WinBox</i> otomatis <i>disconnecting</i>	80
Gambar 4.23 <i>IP attacker</i> yang tertangkap <i>router</i>	81

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka.....	12
Tabel 3.1 Tabel Analisa Kebutuhan Fungsional.....	49
Tabel 3.2 Tabel Spesifikasi Alat yang Digunakan pada Penelitian	51
Tabel 3.3 Tabel Bahan yang Digunakan pada Penelitian	51
Tabel 4.1 Tabel hasil dan pemetaan keberhasilan.....	82



INTISARI

Banyak sekali cara yang ditempuh untuk menghalangi seseorang/perusahaan untuk dapat memberikan layanan yang optimal. Salah satunya adalah layanan pada jaringan internet. Cara yang digunakan adalah melakukan penyerangan terhadap *router* internet yang digunakan. Umumnya serangan yang dilakukan berupa serangan *DDOS*[1] *pingflood*[2] yang dapat membanjiri lalu lintas jaringan dan membuat *router overload* dalam bekerja serta dapat menimbulkan kerusakan. Berdasarkan hal tersebut, keamanan *router* adalah salah satu hal yang sangat penting dilakukan oleh seorang *administrator* jaringan pada sebuah perusahaan atau lembaga yang menggunakan internet.

Salah satu teknik keamanan jaringan pada *router* adalah menggunakan *Intruccion Detection Sistem (IDS)*[3]. *IDS* ini akan melakukan analisa terhadap *request ICMP* yang masuk ke *router*, apabila *request* yang diminta terlalu berlebihan (*pingflood*), maka *IDS* akan melakukan *block* terhadap request tersebut, Secara sistem, *IDS* yang digunakan diharapkan dapat mendeteksi dan menolak serangan *DDOS ping flood* dan membatasi adanya paket yang dikirim oleh *client* ke *Routerboard mikrotik*.

Pada penerapan fitur fitur yang telah dilakukan hasil menunjukan bahwa semua berhasil melakukan identifikasi dan *blocking* kepada parameter yang sudah di tentukan serta dapat melakukan identifikais *IP* yang dianggap sebagai atteker yang dibuktikan pada tabel hasil pengujian, dan dapat di terangkan bahwasanya *IDS* merupakan langkah yang mudah digunakan dan juga tidak membutuhkan *source* yang banyak atau langkah yang rumit dalam penerapannya, sehingga *metode* ini sudah cukup untuk menghindari kemungkinan sebuah jaringan dapat di retas atau di salah gunakan.

Kata Kunci : *DDOS, Pingflood, IDS, Router Mikrotik, Port Knocking,*

ABSTRACT

There are various methods to stop a person or business from being able to offer the best service. The internet network service is one of them. Attacking the internet router is the technique utilized. The most common types of assaults are DDOS[1] and pingflood[2] attacks, which may flood networks with traffic, overwhelm routers, and harm systems. On the basis of this, a network administrator at a business or establishment that uses the internet must prioritize router security.

Utilizing an Instruction Detection System (IDS) on routers is one of the network security strategies [3]. This IDS will analyze the ICMP requests that come into the router; if the request is excessive (such as a pingflood), the IDS will block it. Systematically, it is desired that the IDS be able to restrict any packets delivered by the client to the Mikrotik Routerboard and identify and reject DDOS ping flood attempts.

As evidenced in the test results table, the results of the implementation of the features show that all have been successful in identifying and blocking the parameters that have been determined and can identify IPs that are thought to be attackers. This can be explained by the fact that IDS is an easy step to use and also does not require a lot of sources or complicated steps in its application, so this method is sufficient to prevent the possibility that a network be compromised.

Keywords: *DDOS, Ping flood, IDs, Mikrotik Router, Port Knocking*