

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN FILE
TRANSFER PROTOCOL (FTP) MENGGUNAKAN INTRUSION
PREVENTION SYSTEM (IPS) PADA MIKROTIK
SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana Program
Studi Informatika



disusun oleh

MUHAMMAD THORRIQ RIDHO BEY ALGHOZY
19.11.2640

Kepada

FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN FILE
TRANSFER PROTOCOL (FTP) MENGGUNAKAN INTRUSION
PREVENTION SYSTEM (IPS) PADA MIKROTIK
SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana Program
Studi Informatika



disusun oleh
MUHAMMAD THORRIQ RIDHO BEY ALGHOZY
19.11.2640

Kepada
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN FILE
TRANSFER PROTOCOL (FTP) MENGGUNAKAN INTRUSION
PREVENTION SYSTEM (IPS) PADA MIKROTIK**

yang disusun dan diajukan oleh

Muhammad Thorriq Ridho Bey Alhozy

19.11.2640

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Februari 2023

Dosen Pembimbing,

Andriyan Dwi Putra, M.Kom

NIK. 190302270

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN FILE
TRANSFER PROTOCOL (FTP) MENGGUNAKAN INTRUSION
PREVENTION SYSTEM (IPS) PADA MIKROTIK

yang disusun dan diajukan oleh

Muhammad Thorriq Ridho Bey Alhozy

19.11.2640

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Februari 2023

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Yudi Sutanto, M. Kom
NIK. 190302039

Mulia Sulistiyono, M.Kom
NIK. 190302248

Andriwan Dwi Putra, M.Kom
NIK. 190302270



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Februari 2023

DEKAN FAKULTAS ILMU KOMPUTER



Hanif Al Fatta, S.Kom., M.Kom.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : MUHAMMAD THORRIQ RIDHO BEY ALGHOZY
NIM : 19.11.2640

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS DAN IMPLEMENTASI KEAMANAN JARINGAN FILE TRANSFER PROTOCOL (FTP) MENGGUNAKAN INTRUSION PREVENTION SYSTEM (IPS) PADA MIKROTIK

Dosen Pembimbing : Andriyan Dwi Putra, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Februari 2023

Yang Menyatakan,



MUHAMMAD THORRIQ RIDHO BEY ALGHOZY

HALAMAN PERSEMBAHAN

Segala Puji syukur saya panjatkan kepada Allah Subhanahu wa ta'ala atas limpahan rahmat dan hidayat-Nya, serta support dan doa dari kedua orang tua tercinta serta keluarga besar, lalu teman – teman seperjuangan yang tak henti – hentinya memberikan semangat. Alhamdulillah penelitian skripsi dapat dilaksanakan dan diselesaikan tepat waktu dengan hasil yang baik. Dengan rasa bahagia saya ucapkan rasa syukur dan terima kasih kepada :

1. Allah SWT atas rahmat, karunia, dan anugrah yang telah diberikan kepada kita semua, lalu dengan atas izin Allah saya bisa menjadi seperti saat ini.
2. Skripsi ini saya persembahkan untuk dosen pembimbing saya bapak Andriyan Dwi Putra M.Kom yang telah memberikan bantuan, bimbingan dan waktu yang telah beliau berikan, sehingga peneliti dapat menyelesaikan karya skripsi ini.
3. Skripsi ini saya persembahkan kepada kedua orang tua saya bapak dan ibu yang telah memberikan support, semangat dan doa. Terutama ibu saya, saya bisa menyelesaikan salah satu cita – cita ibu saya yaitu menyelesaikan pendidikan saya.
4. Saya mempersembahkan skripsi ini kepada teman-teman saya Raha, Luky, Rahmat, Herjuno, Raynal, dan masih banyak lagi. Dengan menemani saya selama hampir tiga setengah tahun dan senantiasa memberi motivasi untuk menjadi lebih baik lagi.

KATA PENGANTAR

Segala puji syukur peneliti panjatkan kehadiran Allah SWT karena atas rahmat dan karunia-Nya, sehingga peneliti masih diberikan kesehatan, kemudahan dan kesempatan hingga penulisan naskah skripsi dapat berjalan dengan baik dan lancar.

Skripsi ini diajukan untuk memenuhi salah satu syarat kelulusan dalam jenjang perguruan tinggi program studi Strata I Informatika Universitas Amikom Yogyakarta serta meraih gelar Sarjana Komputer. Dibuatnya skripsi ini merupakan salah satu dari tujuan untuk memberikan informasi dan menambah pengetahuan kepada pembaca mengenai keamanan jaringan *File Transfer Protocol* (FTP) pada router MikroTik menggunakan *Intrusion Prevention System* (IPS) serta monitoring pada jaringan internet.


Saya menyadari bahwa dalam proses pembuatan laporan skripsi ini tidak pernah lepas dari dorongan dan bantuan serta motivasi dari semua pihak yang terlibat. Dalam kesempatan ini saya mengucapkan banyak terima kasih kepada pihak-pihak yang telah banyak membantu dalam pelaksanaan dan penyusunan laporan skripsi ini. Oleh karena itu dengan segala hormat dan kerendahan hati, penekanan penulis mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. Suyanto, M.M., selaku rektor Universitas Amikom Yogyakarta.
2. Bapak Andriyan Dwi Putra, M.Kom selaku dosen pembimbing yang telah memberikan bimbingan, saran dan masukannya dalam menyelesaikan naskah skripsi ini.
3. Hanif Al Fatta, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta.
4. Ibu Windah Mega Pradnya D, M.Kom selaku ketua Program Studi Informatika Universitas Amikom Yogyakarta.
5. Dosen Universitas Amikom Yogyakarta yang telah memberikan ilmu, dan pengalaman selama masa perkuliahan.
6. Kedua Orang tua yang telah memberikan bantuan dukungan serta doa.

7. Teman-teman dan sahabat yang telah memberikan motivasi dan semangat kepada saya hingga saya bisa menyelesaikan penelitian ini.

peneliti menyadari bahwa dalam pembuatan skripsi ini masih jauh dari kata sempurna dan masih banyak kekurangan, baik dari segi bahasa, penulisan ataupun penyajian materi.

Oleh karena itu, penulis sangat mengharapkan para pembaca untuk memberikan saran dan kritik yang membangun. Semoga naskah skripsi ini bisa bermanfaat bagi penulis dan semua pembaca serta dapat digunakan sebagai referensi untuk penelitian kedepanya



Klaten, 29 Januari 2023

Muh. Thorriq Ridho Bey Alghozy
NIM. 19.11.2640

DAFTAR ISI

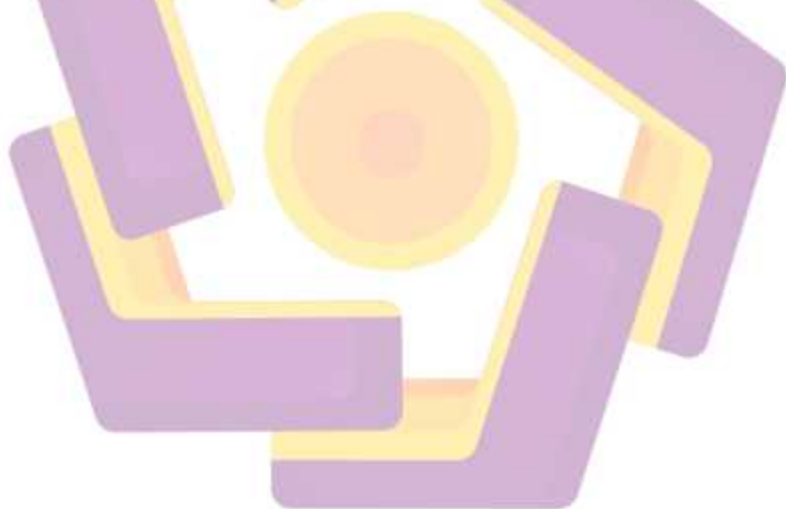
SKRIPSI.....	1
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN.....	Error! Bookmark not defined.
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	Error! Bookmark not defined.
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN	xiv
INTISARI	xv
ABSTRACT.....	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA.....	6
2.1 Studi Literatur	6
2.2 Dasar Teori.....	15
2.1.1 Keamanan Jaringan.....	15
2.1.2 <i>Firewall</i>	15
2.1.3 <i>FTP (File Transfer Protocol)</i>	16
2.1.4 MikroTik.....	16
2.1.5 Router.....	17
2.1.6 Intrusion Prevition System (IPS).....	18

2.1.7	<i>Host Based Intrusion Prevention System (HIPS)</i>	19
2.1.8	<i>Network Intrusion Prevention System (NIPS)</i>	19
2.1.9	<i>TCP/IP (Transmission Control Protocol / Internet Protocol)</i>	21
2.1.10	<i>Port Scanning</i>	21
2.1.12	<i>ICMP Flood</i>	22
2.1.13	<i>WinBox</i>	22
2.1.14	<i>Zenmap/Nmap</i>	22
2.1.15	<i>Kali Linux</i>	23
2.1.16	<i>Ncrack</i>	23
2.1.17	<i>xHydra</i>	24
2.1.18	<i>Hping3</i>	24
2.1.19	<i>Monitoring Jaringan</i>	24
2.1.20	<i>Open System Interconnection (OSI)</i>	24
2.1.21	<i>VM Virtual Box</i>	25
2.1.22	<i>Network Development Life Cycle (NDLC)</i>	25
2.1.23	<i>Sampel (Sampling)</i>	27
BAB III METODE PENELITIAN		28
3.1	<i>Objek Penelitian</i>	28
3.2	<i>Alur Penelttan</i>	29
3.2.1	<i>Alur Penelitian skripsi</i>	29
3.2.2	<i>Alur Sistem Kerja Serangan Dan Pencegahan</i>	31
3.3	<i>Alat dan Bahan</i>	32
3.3.1	<i>Perangkat Keras (Hardware)</i>	32
3.3.2	<i>Perangkat Lunak (Software)</i>	35
BAB IV HASIL DAN PEMBAHASAN		36
4.1	<i>Implementasi</i>	36

4.1.1	Konfigurasi Awal	36
4.1.2	Implementasi Rules IPS Pada <i>Firewall</i> Router MikroTik.....	39
4.2	Flowchart Penyerangan	41
4.2.1	Flowchart Serangan <i>Port Scanning</i>	41
4.2.2	Flowchart Serangan <i>Brute Force</i> FTP	42
4.2.3	Flowchart Serangan <i>ICMP flood</i>	43
4.3	Hasil Pengujian Serangan.....	44
4.3.1	Pengujian Serangan <i>Port Scanning</i> Dengan Tools Zenmap.....	44
4.3.2	Pengujian Serangan <i>Bruteforce</i> FTP Dengan Tools Ncrack.....	49
4.3.3	Pengujian Serangan <i>Brute force</i> FTP Dengan xHydra.....	54
4.3.4	Pengujian Serangan <i>ICMP Flood</i> Dengan Tools Hping3.....	58
BAB IV PENUTUP		65
5.1	Kesimpulan	65
5.2	Saran	66
REFERENSI.....		67
LAMPIRAN.....		70
Lampiran 1 Konfigurasi Dasar MikroTik.....		70
Lampiran 2 Konfigurasi Rules IPS pada firewall.....		72
Lampiran 3 Konfigurasi Scheduler.....		80
Lampiran 4 Dokumentasi Percobaan Serangan Dengan User Lain		83

DAFTAR TABEL

Tabel 2. 1 Keaslian Penelitian	10
Tabel 3. 1 Spesifikasi Perangkat Laptop	33
Tabel 3. 2 Spesifikasi Perangkat Router MikroTik	34
Tabel 3. 3 Software Dan Spesifikasi Yang Dipakai.....	35
Tabel 4. 1 Pengujian Serangan <i>Port Scanning</i> Memakai Zmap.....	47
Tabel 4. 2 Pengujian Serangan <i>Brute force</i> FTP Dengan Ncrack	51
Tabel 4. 3 Pengujian Serangan <i>Brute force</i> Dengan Tools xHydra	56
Tabel 4. 4 Pengujian Serangan ICMP Flood Sebelum Penerapan IPS.....	61
Tabel 4. 5 Pengujian Serangan ICMPFlood Sesudah Penerapan IPS	62



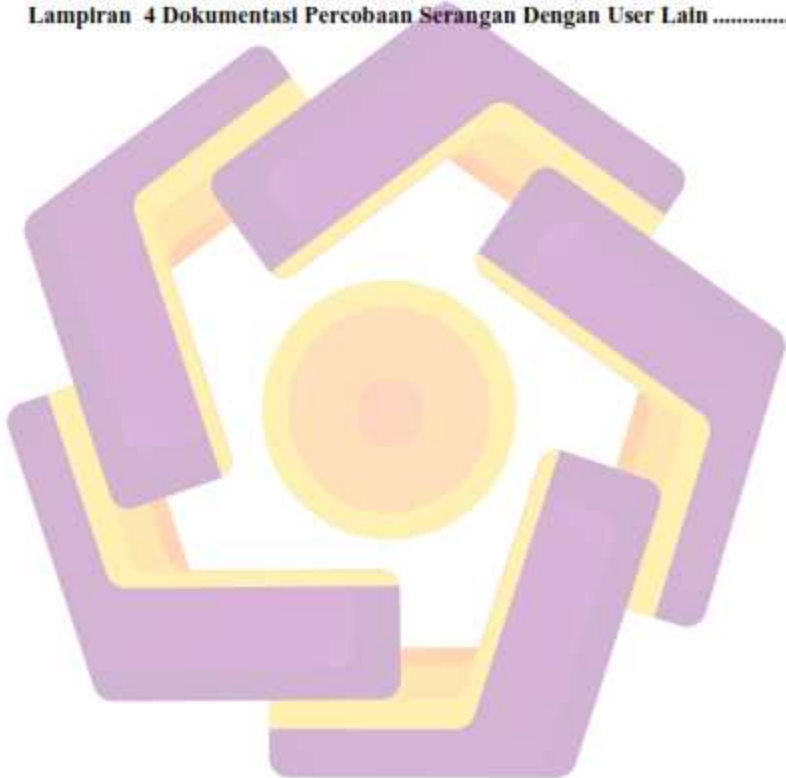
DAFTAR GAMBAR

Gambar 2. 1 Bentuk Topologi <i>Firewall</i> Dalam Jaringan	15
Gambar 2. 2 Router RB951UI-2HND.....	18
Gambar 2. 3 Logo WinBox.....	22
Gambar 2. 4 Logo Zenmap/Nmap.....	22
Gambar 2. 5 Logo Kali Linux Distro	23
Gambar 2. 6 Logo Virtual Box	25
Gambar 2. 7 Metode NDLC	26
Gambar 3. 1 Tahapan Metode Penelitian NDLC.....	29
Gambar 3. 2 Tahapan Alur Penelitian Skripsi.....	29
Gambar 3. 3 Alur Sistem Serangan Dan Pencegahan	31
Gambar 3. 4 Laptop Asus ROG STRIX G.....	33
Gambar 3. 5 Router Mikrotik RB951UI-2HND.....	34
Gambar 4. 1 IP Address	36
Gambar 4. 2 Akun MikroTik.....	37
Gambar 4. 3 Keamanan Google Akun	37
Gambar 4. 4 <i>Scheduler Alert</i> MikroTik.....	38
Gambar 4. 5 <i>Scheduler On Event</i>	38
Gambar 4. 6 List Password Untuk Penelitian	39
Gambar 4. 7 Rules <i>Port Scanning</i>	39
Gambar 4. 8 Rules <i>Brute force FTP</i>	40
Gambar 4. 9 Rules ICMP <i>Flood</i>	40
Gambar 4. 10 Flowchart Serangan <i>Port Scanning</i>	41
Gambar 4. 11 Flowchart Serangan <i>Brute force FTP</i>	42
Gambar 4. 12 Flowchart Serangan ICMP <i>Flood</i>	43
Gambar 4. 13 Serangan <i>Port scanning</i>	45
Gambar 4. 14 Rules <i>Port Scanning</i>	45
Gambar 4. 15 <i>Address list Port Scanning</i>	45
Gambar 4. 16 Log Sistem MikroTik	46
Gambar 4. 17 Monitoring Serangan Pada Gmail	46

Gambar 4. 18 Grafik Durasi Penyerangan <i>Port Scanning</i>	48
Gambar 4. 19 Grafik Rentang Waktu Alert Monitoring Gmail	49
Gambar 4. 20 Serangan <i>Brute force</i> FTP menggunakan Ncrack	50
Gambar 4. 21 Rules IPS Pada <i>Firewall</i> Berjalan.....	50
Gambar 4. 22 <i>Address list Brute Force</i> FTP.....	50
Gambar 4. 23 Log Sistem MikroTik	51
Gambar 4. 24 Monitoring Serangan Pada Gmail	51
Gambar 4. 25 Grafik Durasi Penyerangan Pada Ncrack.....	53
Gambar 4. 26 Grafik Rentang Waktu Alert Monitoring Gmail	53
Gambar 4. 27 Serangan <i>Brute force</i> FTP Menggunakan xHydra.....	54
Gambar 4. 28 Rules IPS Pada <i>Firewall</i> Berjalan.....	55
Gambar 4. 29 <i>Address list Brute Force</i> FTP.....	55
Gambar 4. 30 Log Sistem MikroTik	55
Gambar 4. 31 Monitoring Serangan Pada Gmail	56
Gambar 4. 32 Grafik Durasi Penyerangan Pada xHydra.....	58
Gambar 4. 33 Grafik Rentang Waktu Alert Monitoring Gmail	58
Gambar 4. 34 CPU Load Sebelum Dan Sesudah Terjadi Serangan	59
Gambar 4. 35 Pengujian Serangan ICMP <i>Flood</i> 300.000 Paket.....	59
Gambar 4. 36 Rules Pada IPS Berjalan	60
Gambar 4. 37 Kondisi CPU Load Saat Serangan.....	60
Gambar 4. 38 <i>Address list</i> DDoS ICMP <i>Flood</i>	60
Gambar 4. 39 Monitoring Serangan pada Gmail	61
Gambar 4. 40 Grafik CPU Load Sebelum Penerapan IPS	62
Gambar 4. 41 Grafik CPU Load Setelah Penerapan IPS	64
Gambar 4. 42 Grafik Rentang Waktu Alert Monitoring Gmail	64

DAFTAR LAMPIRAN

Lampiran 1 Konfigurasi Dasar MikroTik.....	70
Lampiran 2 Konfigurasi Rules IPS pada firewall.....	72
Lampiran 3 Konfigurasi Scheduler	80
Lampiran 4 Dokumentasi Percobaan Serangan Dengan User Lain	83



INTISARI

Saat ini perkembangan teknologi pada bidang komunikasi dan informasi mengalami peningkatan yang pesat, dampak dari kemajuan ini terlihat didalam pengolahan data. Pengolahan data dilakukan melalui media transmisi elektronik, media tersebut dikenal dengan *File Transfer Protocol (FTP)*, FTP digunakan sebagai media transfer data atau file dalam lingkup suatu jaringan. FTP merupakan salah satu pilihan yang tepat dalam penyimpanan file, karena proses *upload* dan *download* bisa digunakan secara cepat dan efektif. Namun dengan perkembangan teknologi yang pesat ini banyak alat atau tools yang dapat digunakan untuk melakukan tindakan kejahatan seperti *brute force FTP*, *port scanning*, dan DDoS (*ICMP flood*).

Maka dibutuhkan sebuah sistem yang mampu melakukan tindakan *prevention* dan digunakanlah metode *Intrusion Prevention System (IPS)*. IPS mempunyai fungsi untuk mengamati, mengidentifikasi tindakan mencurigakan, dan melakukan *monitoring* serta pencegahan serangan dengan memblokir semua ancaman secara otomatis. Karena itu IPS bisa disebut sebagai gabungan dari IDS yang melakukan *moniroting* dan *prevention* layaknya *firewall*. Maka dari itu IPS dapat diterapkan pada router MikroTik sebagai metode keamanannya untuk mencegah serangan ke FTP server yang terdapat di router MikroTik.

Dari percobaan serangan seperti *bruteforce FTP*, *port scanning*, dan DDoS (*ICMP flood*). Didapat hasil yaitu serangan *Brute Force FTP* tidak mampu membobol akses akun FTP dengan tingkat keberhasilan 0, *Port Scanning* juga tidak mampu melanjutkan serangan, walaupun pada port 21 beberapa kali terscan karena IPS mendrop serangan. Pada serangan *ICMP Flood* dapat membebani server pada saat belum menerapkan IPS dengan tingkat CPU load 63%-100% dan setelah menerapkan IPS CPU load hanya 13%-36% yang membuat server tetap stabil.

Kata kunci: *brute force FTP*, *ICMP flood*, *port scanning*, *Intrusion Prevention System (IPS)*, *File Transfer Protocol (FTP)*.

ABSTRACT

Currently, the development of technology in the field of communication and information has increased rapidly, the impact of this progress can be seen in the processing of data. Data processing is carried out through electronic transmission media, the media is known as File Transfer Protocol (FTP), FTP is used as a data or file transfer medium within the scope of a network. FTP is one of the right choices in file storage, because the upload and download processes can be used quickly and effectively. However, with the rapid development of technology, there are many tools that can be used to commit crimes such as FTP brute force, port scanning, and DDoS (ICMP flood).

A system that is able to perform prevention actions is needed and the Intrusion Prevention System (IPS) method is used. IPS has a function to observe, identify suspicious actions, and perform monitoring and prevention of attacks to block all threats automatically. Therefore, IPS can be referred to as a combination of IDS that performs monitoring and prevention like a firewall. Therefore, IPS can be applied to MikroTik routers as a security method to prevent attacks on FTP servers on the MikroTik router.

From attack attempts such as bruteforce FTP, port scanning, and DDoS (ICMP flood). The results obtained are the attack Brute Force FTP is not able to break into the FTP account access with a success rate of 0, Port Scanning is also not able to continue the attack, although on port 21 some terscan because IPS drop attacks. On the ICMP Flood attack can overload the server when not implementing IPS with a CPU load level of 63%-100% and after implementing IPS CPU load is only 13%-36% which keeps the server stable.

Keywords: *brute force FTP, ICMP flood, port scanning, Intrusion Prevention System (IPS), File Transfer Protocol (FTP)*