

Universitas Katolik Santo Thomas

Repositori Unika Santo Thomas

<http://eprints.ust.ac.id>

Fakultas Ilmu Komputer (FIKOM)
Program Studi Sistem Informasi

Undergraduate Theses

Sibuea, Lisa Margaretha

2024

Optimalisasi Keamanan Server Dan Jaringan Terhadap DDOS SYN FLOODING Dengan Metode Ddos Mitigation

<http://eprints.ust.ac.id/id/eprint/1213>

Downloaded from Repositori Institusi UST, Universitas Katolik Santo Thomas

**OPTIMALISASI KEAMANAN SERVER DAN JARINGAN
TERHADAP DDOS SYN FLOODING DENGAN
METODE DDOS MITIGATION**

SKRIPSI

**Diajukan Untuk Melengkapi dan Memenuhi Persyaratan
Memperoleh Gelar Sarjana Komputer Pada
Program Studi Teknik Informatika**

Oleh:

LISA MARGARETHA SIBUEA

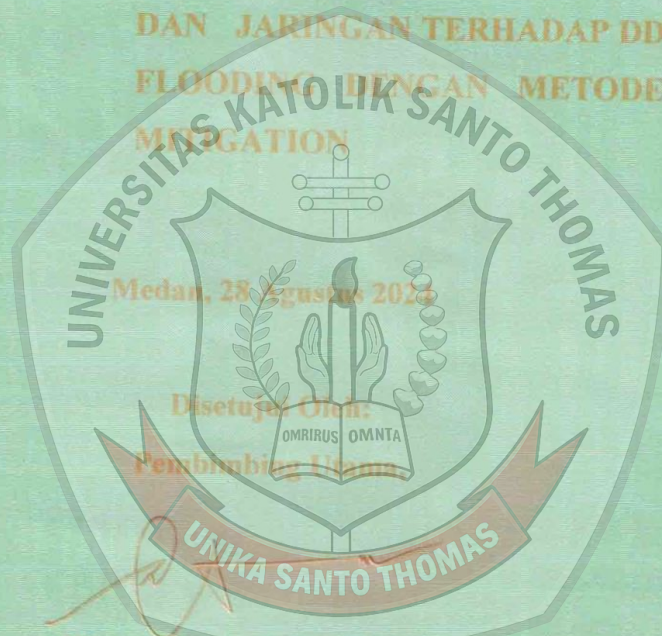
200840087



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS KATOLIK SANTO THOMAS
MEDAN
2024**

LEMBAR PENGESAHAN SKRIPSI

NAMA : LISA MARGARETHA SIBUEA
NPM : 200840087
PROGRAM STUDI : TEKNIK INFORMATIKA
JENJANG : SARJANA SATU (S-1)
JUDUL SKRIPSI : OPTIMALISASI KEAMANAN SERVER
DAN JARINGAN TERHADAP DDOS SYN
FLOODING DENGAN METODE DDOS
MITIGATION



Wasit Ginting, S.Kom., M.Kom
NIDN. 0529067401

Diketahui Oleh


Ketua Program Studi
Masdlana Sagala, S.Kom., M.Kom
NIDN. 0126088202


Dekan
Desinta Purba, ST., M.Kom
NIDN. 0111067801

SKRIPSI

OPTIMALISASI KEAMANAN SERVER DAN JARINGAN
TERHADAP DDOS SYN FLOODING DENGAN
METODE DDOS MITIGATION

Dipersiapkan dan Disusun Oleh:

LISA MARGARETHA SIBUEA

20034000

Telah dipertahankan di depan Dewan Penguji

Pada Tanggal 04 September 2024

Susunan Dewan Penguji

OMITRUS OMINTA

Pembimbing Utama/Penguji I

Penguji II

Wasit Ginting, S.Kom., M.Kom
NIDN. 0529067401

Sorang Pakpahan, S.Kom., M.Kom
NIDN. 0122107901

Penguji III

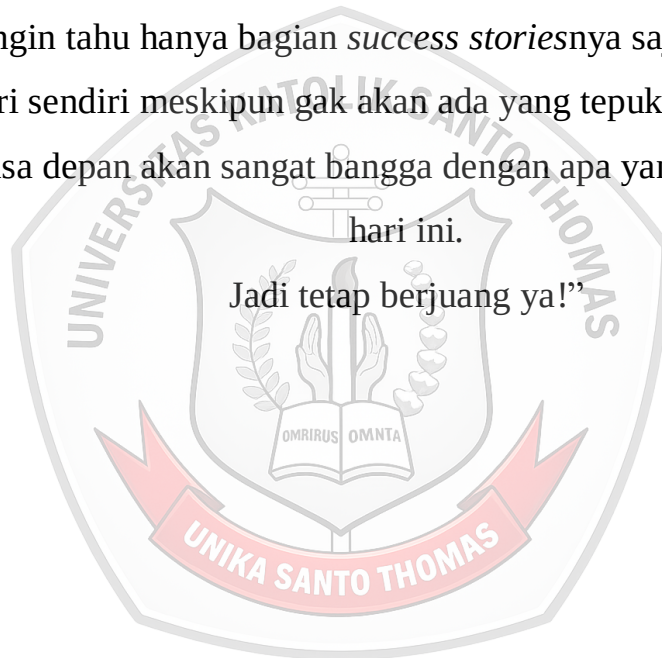
Andy Paul Harianja, ST., M.Kom
NIDN. 01081175

MOTTO

“God has perfect timing, never early, never late. It takes a little pattiience and it takes a lot of faith, but it’s a worth the wait.”

“Orang lain ga akan bisa paham *struggle* dan masa sulitnya kita, yang mereka ingin tahu hanya bagian *success stories*nya saja. Jadi berjuanglah untuk diri sendiri meskipun gak akan ada yang tepuk tangan. Kelak diri kita dimasa depan akan sangat bangga dengan apa yang kita perjuangkan hari ini.

Jadi tetap berjuang ya!”



LEMBAR PERSEMBAHAN

Dengan penuh rasa syukur dan kebahagiaan, skripsi ini saya persembahkan kepada mereka yang selalu hadir dan menjadi sumber kekuatan dalam perjalanan hidup saya.

“Tidak ada keberhasilan tanpa perjuangan, tidak ada pencapaian tanpa pengorbanan. Setiap langkah maju adalah wujud keberanian untuk menghadapi tantangan.”

Untuk kedua orang tua tercinta, yang dengan cinta dan pengorbanan tak terhingga telah membimbing dan mendukung setiap langkah saya. Untuk keluarga, sahabat, dan orang-orang terdekat yang senantiasa memberi semangat dan doa dalam setiap proses yang saya jalani.

“Mimpi besar membutuhkan ketekunan dan kerja keras, namun keyakinan dan doa adalah pilar yang menuntun kita menuju pencapaian yang lebih tinggi.”

Skripsi ini bukanlah akhir dari perjalanan, melainkan sebuah awal dari babak baru dalam kehidupan. Semoga segala ilmu dan pengalaman yang diperoleh dapat menjadi bekal untuk masa depan yang lebih baik.

PERNYATAAN PENULIS

Sebagai sivitas akademik Universitas Katolik Santo Thomas, saya yang bertanda tangan dibawah ini :

Nama : Lisa Margaretha Sibuea

NPM : 200840087

Program Studi : Teknik Informatika

Fakultas : Ilmu Komputer

Jenis Karya : Skripsi

1. Menyatakan dan bertanggungjawab dengan sebenarnya bahwa Skripsi ini adalah hasil karya saya sendiri, kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya. Jika pada waktu selanjutnya ada pihak lain yang mengklaim bahwa Skripsi ini sebagai karyanya, yang disertai dengan bukti-bukti yang cukup, maka saya bersedia untuk dibatalkan gelar Sarjana Komputer saya beserta segala hak dan kewajiban yang melekat pada gelar tersebut.
2. Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Katolik Santo Thomas Hak Bebas Royalti Nonesklusif (**Non Exclusive Royalty-Free Right**) atas karya ilmiah saya tersebut, beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Nonesklusif ini, Universitas Katolik Santo Thomas berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Universitas Katolik Santo Thomas

Pada Tanggal : 04 September 2024

Yang Menyatakan

Lisa Margaretha Sibuea

Penulis

ABSTRAK

Universitas Katolik Santo Thomas Sumatera Utara disingkat UNIKA Santo Thomas didirikan pada tahun 1984 di Jl. S. Parman 107, Medan. Pada dekade pertama, pertumbuhan dan perkembangan UNIKA sangat pesat sehingga dibutuhkan lokasi kampus baru yang lebih luas. Pada tahun 1994, kampus baru di Tanjung Sari Medan diresmikan dan seluruh kegiatan Pengajaran, Penelitian dan Pengabdian Masyarakat dipusatkan dan dirancang di kampus Tanjung Sari. Serangan Distributed Denial of Service (DDoS) Syn Flooding adalah salah satu ancaman terbesar terhadap keamanan server dan jaringan komputer. Serangan ini memanfaatkan kelemahan dalam protokol Transmisi Kontrol Protokol (TCP) untuk membanjiri server dengan permintaan koneksi palsu, sehingga mengganggu kinerja dan ketersediaan layanan. Penelitian ini bertujuan untuk mengoptimalkan keamanan server dan jaringan terhadap serangan DDoS Syn Flooding dengan menggunakan metode mitigasi DDoS berbasis perangkat Mikrotik Metode yang digunakan melibatkan konfigurasi dan pengaturan perangkat Mikrotik untuk mendeteksi dan memitigasi serangan DDoS Syn Flooding secara efisien. Penelitian ini meliputi analisis pola serangan, implementasi aturan firewall, dan pemanfaatan fitur keamanan Mikrotik seperti Connection Limiting dan Syn Cookie. Hasil dari penelitian ini menunjukkan bahwa metode mitigasi DDoS yang diterapkan mampu secara signifikan mengurangi dampak serangan Syn Flooding, meningkatkan kinerja server dan jaringan, serta memastikan ketersediaan layanan yang optimal.

Kata Kunci : Mikrotik, DDOS Mitigation, Synflood attack, TCP, Jaringan Komputer, Server

ABSTRACT

Catholic University of Santo Thomas, North Sumatra, abbreviated as UNIKA Santo Thomas, was established in 1984 on Jl. S. Parman 107, Medan. In the first decade, the growth and development of UNIKA was very rapid so that a new, larger campus location was needed. In 1994, the new campus in Tanjung Sari Medan was inaugurated and all Teaching, Research and Community Service activities were centered and designed on the Tanjung Sari campus. Distributed Denial of Service (DDoS) Syn Flooding attacks are one of the biggest threats to server and computer network security. This attack exploits weaknesses in the Transmission Control Protocol (TCP) protocol to flood the server with fake connection requests, thereby disrupting service performance and availability. This study aims to optimize server and network security against DDoS Syn Flooding attacks using a DDoS mitigation method based on Mikrotik devices. The method used involves configuring and setting up Mikrotik devices to efficiently detect and mitigate DDoS Syn Flooding attacks. This study includes analysis of attack patterns, implementation of firewall rules, and utilization of Mikrotik security features such as Connection Limiting and Syn Cookie. The results of this study indicate that the applied DDoS mitigation method is able to significantly reduce the impact of Syn Flooding attacks, improve server and network performance, and ensure optimal service availability.

Keywords: Mikrotik, DDOS Mitigation, Synflood attack, TCP, Computer Network, Server

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Tuhan Yang Maha Esa, atas segala berkat-Nya sehingga penulis dapat menyelesaikan Skripsi dengan Judul “OPTIMALISASI KEAMANAN SERVER DAN JARINGAN TERHADAP DDOS SYN FLOODING DENGAN METODE DDOS MITIGATION” yang diajukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Katolik Santo Thomas.

Penulis menyadari bahwa dalam penyusunan skripsi ini telah banyak mendapat bimbingan, motivasi, nasihat serta dukungan dari berbagai pihak. Untuk itu dengan segala kerendahan hati penulis mengucapkan terima kasih kepada:

1. Secara khusus, dengan penuh cinta dan rasa hormat, saya ingin menyampaikan rasa terima kasih yang mendalam kepada kedua orang tua saya, Bapak Liston Sibuea dan Ibu Evi Lenni Br.Sitorus. Terima kasih atas doa, kasih sayang, serta dukungan moral dan materi yang tak pernah berhenti kalian berikan. Setiap nasihat dan semangat dari kalian menjadi motivasi terbesar saya untuk terus maju dan menyelesaikan tugas ini. Segala pengorbanan yang kalian berikan menjadi inspirasi dalam setiap langkah saya. Skripsi ini adalah wujud kecil dari rasa terima kasih saya atas semua yang telah kalian lakukan, dan semoga ini bisa menjadi sesuatu yang membanggakan untuk kalian. Semoga Tuhan senantiasa melimpahkan berkah-Nya kepada kalian, serta memberikan kebahagiaan dan kesehatan. Terima kasih telah menjadi orang tua yang luar biasa.
2. Bapak Prof. Dr. Maidin Gultom, SH, M.Hum selaku Rektor Universitas Katolik Santo Thomas.
3. Ibu Desinta Purba, S.T.,M.Kom selaku Dekan Fakultas Ilmu Komputer.
4. Ibu Masdiana Sagala, S.Kom.,M.Kom selaku Kepala Program Studi Teknik Informatika.
5. Bapak Wasit Ginting, S.Kom.,M.Kom selaku dosen Pembimbing Skripsi yang dengan penuh kesabaran, ketelitian, dan perhatian telah memberikan

bimbingan serta saran-saran yang sangat berarti. Berkat arahan dan bantuan beliau, saya dapat menyelesaikan skripsi ini dengan baik dan tepat waktu.

6. Kepada Keluarga saya tercinta, terima kasih atas cinta, dukungan, dan doa yang tak pernah putus selama perjalanan panjang ini. Setiap langkah yang saya ambil dalam penyusunan skripsi ini selalu didampingi dengan kasih sayang dan perhatian yang tulus dari kalian.
7. Kepada sahabat-sahabat terbaik saya, Silvia Tri Eviyanti Simamora, Stevani Anggita Ginting, Kristin Sinaga, dan Heni Silaban. Kalian semua telah menjadi pilar penting dalam perjalanan panjang yang penuh tantangan ini. Kepada sahabat-sahabatku, terima kasih atas kebersamaan, dukungan, dan canda tawa yang selalu menemani di setiap langkah. Kalian selalu hadir saat saya membutuhkan semangat, menjadi pendengar yang baik saat saya mengalami kesulitan, dan memberikan tawa di saat-saat paling lelah. Persahabatan kita adalah salah satu hal terindah yang saya syukuri, dan tanpa kalian, mungkin perjalanan ini akan terasa lebih berat.
8. Dan terakhir tak lupa saya ucapkan teruntuk diriku sendiri yang telah berjuang tanpa henti, Aku ingin mengucapkan terima kasih atas ketekunan, kesabaran, dan dedikasi yang telah aku berikan dalam proses panjang menyelesaikan skripsi ini. Terima kasih telah terus berusaha meski sering merasa lelah, tertekan, dan hampir menyerah. Meski jalan ini tak selalu mudah, aku telah membuktikan bahwa dengan keyakinan dan kerja keras, semuanya dapat tercapai. Aku bangga pada diriku yang mampu melewati berbagai rintangan, bertahan di saat-saat sulit, dan terus melangkah maju. Terima kasih telah menjaga semangat dan keyakinan bahwa segala usaha ini akan membuahkan hasil. Skripsi ini adalah bukti dari perjalanan panjang penuh pembelajaran, dan aku berterima kasih kepada diriku sendiri karena telah menjalaninya dengan keberanian dan kesungguhan.

Penulis menyadari bahwa dalam penulisan skripsi ini masih terdapat kekurangan, baik dari segi isi maupun penyajian. Oleh karena itu, dengan segala kerendahan hati, penulis membuka diri untuk menerima saran dan kritik yang membangun guna penyempurnaan skripsi ini. Penulis juga berharap semoga skripsi ini dapat memberikan manfaat bagi para pembaca. Akhir kata penulis ucapkan terimakasih.

Medan, 04 September 2024

Penulis,

Lisa Margaretha Sibuea



DAFTAR ISI

	Halaman
LEMBAR PENGESAHAN SKRIPSI	Error! Bookmark not defined.
MOTTO	i
LEMBAR PERSEMBAHAN	iv
PERNYATAAN PENULIS.....	v
ABSTRAK.....	vi
ABSTRACT	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	xi
DAFTAR TABEL	xv
DAFTAR GAMBAR.....	xvi
BAB I.....	1
PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Rumusan Masalah.....	3
I.3 Batasan Masalah	3
I.4 Maksud dan Tujuan.....	4
I.4.1 Maksud.....	4
I.4.2 Tujuan	4
I.5 Metodologi Penelitian	4
I.6 Sistematika Penulisan.....	6
BAB II	7
LANDASAN TEORI.....	7
II.1 Jaringan Wi-fi	7
II.2 Monitoring Jaringan.....	9
II.3 Keamanan Jaringan.....	10
II.3.1 Konsep Keamanan Jaringan.....	14
II.3.2 Aspek-Aspek Keamanan Jaringan.....	16
II.4 OSI Layer	17
II.5 Topologi Jaringan	20
II.5.1 Physical Topology	20

II.5.2 Point to Point Topology	21
II.5.3 Topologi Bus (Bus Topology)	21
II.5.4 Topologi Bintang (Star Topology)	23
II.5.5 Topologi Cincin (Ring Topology).....	24
II.5.6 Topologi Acak (Mesh Topology).....	25
II.5.7 Topologi Pohon (Tree Topology)	27
II.6 Jenis-Jenis Ancaman Keamanan Jaringan.....	28
II.6.1 Packet Sniffing	28
II.6.2 ARP Spoofing / ARP Poisoning.....	28
II.6.3 Probe	29
II.6.4 Scan.....	29
II.6.5 Account Compromise	29
II.6.6 Root Compromise.....	29
II.6.7 Denial of service (Dos).....	30
II.7 Distributed Denial Of Service (DDOS)	30
II.8 Wireshark	31
II.9 NMAP	32
II.10 Winbox	32
II.11 Mikrotik.....	33
II.11.1 Sejarah Mikrotik.....	33
II.11.2 Jenis-Jenis Mikrotik.....	34
II.11.3 Fitur Mikrotik	36
II.12 Flowchart.....	37
BAB III	39
GAMBARAN UMUM	39
UNIVERSITAS KATOLIK SANTO THOMAS	39
III.1 Profil Universitas Katolik Santo Thomas	39
III.2 Sejarah Universitas Katolik Santo Thomas	39
III.3 Visi Dan Misi Universitas Katolik Santo Thomas	40
III.3.1 Visi	40
III.3.2 Misi.....	40
III.4 Logo Universitas Katolik Santo Thomas	41
III.5 Tujuan Universitas Katolik Santo Thomas	42
III.6 Sasaran Universitas Katolik Santo Thomas	42

III.7 Nilai-Nilai di Universitas Katolik Santo Thomas	43
III.8 Motto Universitas Katolik Santo Thomas.....	43
III.9 Struktur Organisasi Universitas Katolik Santo Thomas	43
III.10 Pimpinan Universitas Katolik Santo Thomas	45
III.11 Pembagian Tugas-Tugas Struktur Organisasi	45
BAB IV	51
ANALISIS DAN PERANCANGAN.....	51
IV.1 Analisis Sistem.....	51
IV.1.1 Analisis Penyedia Layanan Bandwidth.....	51
IV.1.2 Analisis Topologi.....	52
IV.1.3 Pengembangan Topologi.....	52
IV.1.4 Skema Web Server yang Berjalan	53
IV.1.5 Skema Jaringan Hotspot.....	54
IV.2 Kesimpulan Analisis.....	55
IV.2.1 Hasil Analisis.....	55
IV.2.2 Analisis Permasalahan	56
IV.3 Perancangan	56
IV.3.1 Rancangan IP Address	57
IV.3.2 Rancangan DDOS Mitigation.....	57
BAB V IMPLEMENTASI DAN PENGUJIAN	61
V.1 Spesifikasi Hardware dan Software.....	61
V.2 Tahap Implementasi.....	62
V.2.1 Instalasi Perangkat Keras.....	62
V.2.2 Basic Konfigurasi Mikrotik	62
V.2.2.1 Konfigurasi Identity dan Interface.....	64
V.2.2.2 Konfigurasi IP Address dan DHCP Client	65
V.2.2.3 Konfigurasi Bridge Port dan IP Address	67
V.2.2.4 Konfigurasi DNS	69
V.2.2.5 Konfigurasi NAT.....	69
V.2.2.6 Testing Koneksi Mikrotik	71
V.2.3 Instalasi Hping3	71
V.2.4 DDOS Mitigation	73
V.3 Tahap Implementasi DDoS dengan Simulasi.....	74
V.3.1 Skema Tanpa DDoS Mitigation.....	76

V.3.1.1 Syn Flood Terhadap Server.....	76
V.3.1.2 Syn Flood Terhadap Mikrotik.....	78
V.3.2 Skema dengan DDoS Mitigation	80
V.3.2.1 Syn Flood Terhadap Server.....	81
V.3.2.2 Syn Flood Terhadap Server Jaringan.....	82
V.3.3 Evaluasi Berdasarkan Simulasi	84
V.4 Uji Relevansi Penelitian.....	84
V.4.1 Relevansi Terhadap Spesifikasi Hardware	85
V.4.2 Uji Relevansi Penelitian	87
V.4.2.1 Syn Flood Terhadap Server Jaringan.....	89
V.4.2.2 Syn Flood Terhadap IBM-Lenovo System X3500.....	90
V.4.2.3 Uji Relevansi DDoS Mitigation.....	91
V.4.3 Evaluasi Uji Relevansi.....	94
BAB VI PENUTUP.....	96
VI.1 Kesimpulan	96
VI.2 Saran.....	97
DAFTAR PUSTAKA.....	98
LAMPIRAN	

DAFTAR TABEL

	Halaman
Tabel II.1 Keamanan Jaringan Wifi.....	7
Tabel II.2 Keamanan Jaringan	11
Tabel II.3 Konsep Keamanan Jaringan	15
Tabel II.4 Aspek-Aspek Keamanan Jaringan	16
Tabel II.5 Level dan Features Mikrotik	35
Tabel II. 6 Simbol Flowchart.....	37
Tabel IV.1 Web Server Universitas	54
Tabel IV.2 Rancangan IP Address.....	57
Tabel V.1 Spesifikasi Hardware dan Software	61
Tabel V.2 Software Yang Digunakan	62
Tabel V.3 Simulasi Perbandingan DDOS Mitigation	84
Tabel V.4 Data Hardware Yang Digunakan Dalam Uji Relevansi.....	86
Tabel V.5 Perbandingan Spesifikasi Hardware	87
Tabel V.6 Perbandingan Data CPU Load Terhadap Server Apps	89
Tabel V.7 Data Persentase CPU Load.....	91
Tabel V.8 Uji Relevansi Terhadap CPU	94
Tabel V.9 Uji Reaksi Perubahan Server Terhadap Serangan DDOS.....	94

DAFTAR GAMBAR

	Halaman
Gambar II.1 OSI Layer	18
Gambar II.2 Topologi Bus.....	22
Gambar II.3 Topologi Star	23
Gambar II.4 Topologi Ring	24
Gambar II.5 Topologi Mesh	25
Gambar II.6 Fully Connected Mesh Topology.....	26
Gambar II.7 Partially Connected.....	26
Gambar II.8 Topologi Tree	27
Gambar III.1 Rektorat.....	39
Gambar III.2 Logo Universitas Katolik	41
Gambar III.3 Struktur Organisasi	44
Gambar IV.1 Logo PT. Mora Telematika Indonesia Tbk	51
Gambar IV.2 Topologi Jaringan	52
Gambar IV.3 Pengembangan Topologi.....	53
Gambar IV.4 Skema Jaringan Hotspot.....	55
Gambar IV.5 Perancangan dengan Metode DDOS Mitigation	57
Gambar IV.6 SYN Flood Attack	58
Gambar IV.7 Flowchart Algoritma DDOS Mitigation	59
Gambar V.1 Tampilan Login Winbox.....	63
Gambar V.2 Tampilan Awal Winbox.....	64
Gambar V.3 Indentity Mikrotik	65
Gambar V.4 Interface Internet	65
Gambar V.5 Konfigurasi IP pada Interface	66
Gambar V.6 Konfigurasi DHCP Client	66
Gambar V.7 Add Bridge Interface	67
Gambar V.8 Bridge Port	68
Gambar V.9 Add IP Address Bridge Port.....	68

Gambar V.10	Konfigurasi DNS	69
Gambar V.11	Konfigurasi NAT Rule	70
Gambar V.12	Konfigurasi NAT Action	70
Gambar V.13	Test PING	71
Gambar V.14	Source Code HPING3	72
Gambar V. 15	Perintah Update	73
Gambar V.16	Source Code Menginstall.....	73
Gambar V.17	Interface Raw pada Firewall	73
Gambar V.18	Skema Awal Pada Sistem Operasi Windows Tanpa Serangan...	75
Gambar V.19	Sistem Operasi Ubuntu Tanpa Serangan	75
Gambar V.20	Sistem Operasi Router Os Mikrotik Tanpa Serangan	76
Gambar V.21	SYN Flood Terhadap Server Windows	77
Gambar V.22	Hasil Pengujian SYN Flood Terhadap Server	77
Gambar V.23	SYN Flood Terhadap Server Ubuntu	78
Gambar V.24	Sistem Operasi Ubuntu Setelah Diserang	78
Gambar V.25	SYN Flood Terhadap Mikrotik	79
Gambar V.26	Hasil Pengujian SYN Flood Terhadap Mikrotik.....	79
Gambar V.27	Hasil Test PING Terhadap SYN Flood Attack.....	80
Gambar V.28	DDOS Mitigation Terhadap Server.....	81
Gambar V.29	Hasil Pengujian DDOS Mitigation Terhadap Server	81
Gambar V.30	DDOS Mitigation Terhadap Server Jaringan.....	82
Gambar V.31	Hasil Pengujian DDOS Mitigation Terhadap Server Jaringan ...	83
Gambar V.32	Test PING DDOS Mitigation Terhadap Server Jaringan	83
Gambar V.33	Standby Server Jaringan pada Mikrotik Rb1100ahx4.....	88
Gambar V.34	Standby Server Apps IBM-Lenovo System X3500	88
Gambar V.35	Reaksi Dari Server Jaringan Ketika Dilakukan Syn Flood.....	90
Gambar V.36	Reaksi Dari Server Apps Ketika Dilakukan Syn Flood.....	91
Gambar V.37	Uji Relevansi DDoS Mitigation	92
Gambar V.38	Konfigurasi DDos Mitigation pada Mikrotik Rb1100	92
Gambar V.39	Cek Terhadap IP Publik setelah Forwarding	93
Gambar V.40	Serangan ke Server Menggunakan IP Publik.....	93

DAFTAR PUSTAKA

- Aprilianto, D., Fadila, T., & Muslim, M. A. (2017). Sistem pencegahan UDP DNS Flood dengan filter Firewall pada router Mikrotik. *Techno. com*, 16(2), 114-119.
- Cahyadi, M. Sistem Pencegahan Serangan Ddos Tcp Flood Menggunakan Algoritma Ingress/Egress Filtering.
- Dharma, S., & Thamrin. (2020a). Analisis Kinerja Jaringan WIFI. *Jurnal Vocational Teknik Elektronika Dan Informatika*.
<http://ejournal.unp.ac.id/index.php/voteknika/>
- Erlangga, M. F. E., Fahriani, N., & Tantri, A. H. (2023). Deteksi Serangan Syn Flood Pada Server Menggunakan Metode Algoritma K-Nearest Neighbor. In *SEMASTER: Seminar Nasional Teknologi Informasi & Ilmu Komputer* (Vol. 2, No. 1, pp. 68-72).
- Erlangga, M. F. E., Fahriani, N., & Tantri, A. H. (2023). Deteksi Serangan Syn Flood Pada Server Menggunakan Metode Algoritma K-Nearest Neighbor. In *SEMASTER: Seminar Nasional Teknologi Informasi & Ilmu Komputer* (Vol. 2, No. 1, pp. 68-72).
- Fakhmi, M., & Gultom, LM (2021, Desember). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw (Studi kasus: Sekolah Menengah Kejuruan Negeri 3 Bengkalis). Dalam *Seminar Nasional Industri dan Teknologi* (hlm. 260-277).
- Hariyadi, C. (2009). Graf Dalam Topologi Jaringan. *Ilmu Komput. Dan Teknologi Inf*, 3(10).
- Ibrahim, M. M. (2020). Analisis Keamanan Jaringan pada Fasilitas Internet (Wifi) Kantor Pemerintahan Kota Batam terhadap Serangan Packet Sniffing (Doctoral dissertation, Prodi Teknik Informatika).
- Jaya, B., Yuhandri, Y., & Sumijan, S. (2020). Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS). *Jurnal Sistim Informasi dan Teknologi*, 115-123.

- Kurniawan, T. A. (2020). Analisa Keamanan Jaringan Wifi Terhadap Serangan Packet Sniffing. *Jurnal Ilmiah Fakultas Teknik LIMIT'S Vol*, 16(2), 11.
- Kurniawan, R. (2021). *Analisis Keamanan Fasilitas Jaringan (Wifi) Terhadap Serangan Packet Sniffing Pada Protocol Http Dan Https* (Doctoral dissertation, Universitas Islam Riau).
- Nugroho, B. A. (2012). *Analisis Keamanan Jaringan Pada Fasilitas Internet (WiFi) Terhadap Serangan Packet Sniffing* (Doctoral dissertation, Universitas Muhammadiyah Surakarta).
- Panduan Proyek Perangkat Lunak, Fikom Unika St.Thomas, 2021
- Reynaldi, T. (2022). Implementasi Keamanan Jaringan Terhadap Serangan Syn Flood Dengan Menggunakan Firewall Raw Berbasis Routerboard Mikrotik (Doctoral Dissertation, Isb Atma Luhur).
- Romadhon, F. (2021). Implementasi Asi Ddos Mitigation Sebagai Filter Paket Pada Keamanan Jaringan Komputer Rumah Sakit Bhayangkara Tk. I Puskokkes Polri.
- Rosaly, R., & Prasetyo, A. (2019). Pengertian Flowchart Beserta Fungsi dan Simbol-simbol Flowchart yang Paling Umum Digunakan. *Program Studi Teknik Informatika Politeknik Purbaya*.
- Sahren, S. (2021). Implementasi Teknologi Firewall Sebagai Keamanan Server Dari Syn Flood Attack. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi)*, 7(2), 159-164.
- Suherdi, D. (2021). Pemanfaatan Firewall Pada Jaringan Menggunakan Mikrotik RB951Ui â€“2HnD. *Jurnal Teknologi Sistem Informasi dan Sistem Komputer TGD*, 4(2), 173-179.