IMPLEMENTASI DAN ANALISIS MITIGASI SERANGAN DDOS PADA APLIKASI WEB MENGGUNAKAN ROUTER MIKROTIK

Untuk Memenuhi Sebagian Persyaratan Mencapai Derajat Sarjana S-1 Program Studi Informatika

Disusun Oleh : ALFATHUL ABROR

NIM. 20106050072

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2025

HALAMAN PENGESAHAN

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1804/Un.02/DST/PP.00.9/08/2025

Tugas Akhir dengan judul : Implementasi dan Analisis Mitigasi Serangan DDoS Pada Aplikasi Web menggunakan Router Mikrotik

yang dipersiapkan dan disusun oleh:

Nama : ALFATHUL ABROR
Nomor Induk Mahasiswa : 20106050072
Telah diujikan pada : Jumat, 15 Agustus 2025
Nilai ujian Tugas Akhir : A-

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
SIGNED
Valid ID: 68a4d97f2820a

Penguji I

Ir. Muhammad Didik Rohmad Wahyudi, S.T., M.T.
SIGNED
Valid ID: 68a48727d7691

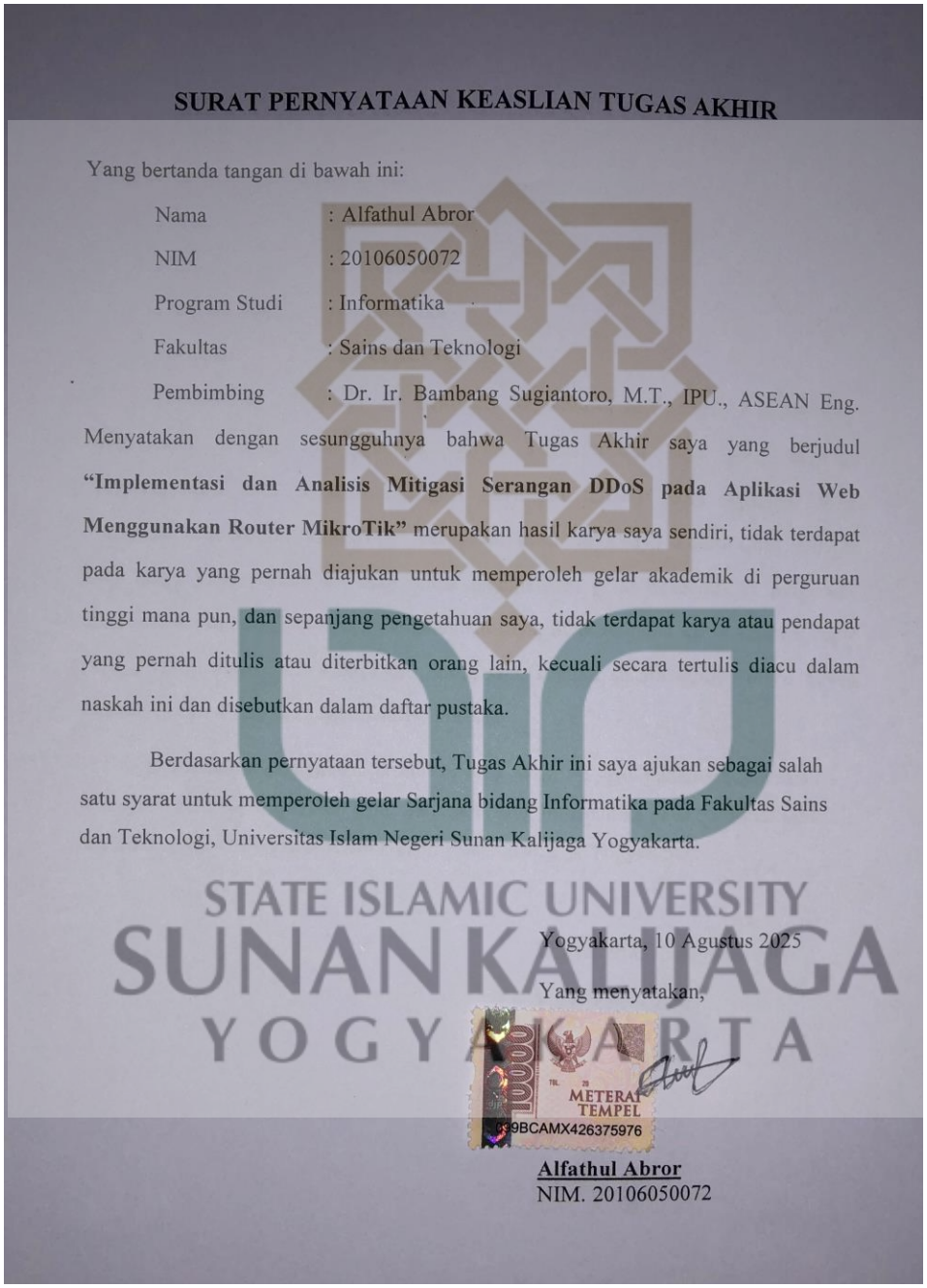
Penguji II

Eko Hadi Gunawan, M.Eng.
SIGNED
Valid ID: 68a479e384277

Yogyakarta, 15 Agustus 2025
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Prof. Dr. Dra. Hj. Khurul Wardati, M.Si.
SIGNED
Valid ID: 68a54b6aca7da

PERNYATAAN KEASLIAN SKRIPSI



SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	: Alfathul Abror
NIM	: 20106050072
Program Studi	: Informatika
Fakultas	: Sains dan Teknologi
Pembimbing	: Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.

Menyatakan dengan sesungguhnya bahwa Tugas Akhir saya yang berjudul **"Implementasi dan Analisis Mitigasi Serangan DDoS pada Aplikasi Web Menggunakan Router MikroTik"** merupakan hasil karya saya sendiri, tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar akademik di perguruan tinggi mana pun, dan sepanjang pengetahuan saya, tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Berdasarkan pernyataan tersebut, Tugas Akhir ini saya ajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana bidang Informatika pada Fakultas Sains dan Teknologi, Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Yogyakarta, 10 Agustus 2025

Yang menyatakan,

Alfathul Abror
NIM. 20106050072

SURAT PERSETUJUAN SKRIPSI / TUGAS AKHIR

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi / Tugas Akhir
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
Di Yogyakarta

Assalammu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka saya selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	:	Alfathul Abror
NIM	:	20106050072
Judul Skripsi	:	Implementasi dan Analisis Mitigasi Serangan DDoS pada Aplikasi Web Menggunakan Router MikroTik

sudah dapat diajukan kembali kepada Program Studi Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Program Studi Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudari dapat segera dimunaqasyahkan. Atas perhatiannya saya ucapkan terima kasih.

Wassalammu'alaikum wr. wb.

Yogyakarta, 12 agustus 2025
Pembimbing

Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng.
NIP. 19751024 200912 1 002

MOTTO

"Allah mengabulkan doa-doa ketika kita sudah siap, bukan ketika kita menginginkannya"

-KH. Ahmad Bahauddin Nursalim

"Barang siapa keluar untuk mencari sebuah ilmu, maka ia akan berada di jalan Allah hingga ia kembali."

- HR Tirmidzi

HALAMAN PERSEMBAHAN

Bismillahirrahmaanirrahiim, Dengan rahmat Allah yang Maha Pengasih Lagi Maha Penyayang. Dengan ini penulis persembahkan skripsi ini kepada :

1. Papa dan Mama, dua sosok yang menjadi pondasi hidupku. Papa, dengan keteguhan dan kesederhanaan, mengajarkanku arti tanggung jawab dan kerja keras. Mama, sosok visioner penuh semangat dan harapan. Dengan kasih dan doa yang tak pernah putus, engkau menjadi sumber kekuatanku. Meski sering banyak harapan dan keinginan, aku tahu semuanya lahir dari cinta dan cita agar anak-anakmu melangkah lebih jauh. Dari kalian, aku belajar bahwa kasih sayang tak selalu hadir dalam kelembutan, tapi juga dalam dorongan untuk terus menjadi lebih baik, karena sejatinya tidak ada orang tua yang ingin anaknya tidak sukses di kemudian hari.
2. Kakak tercintaku, Arifa Anggraini Habidah S.T dan Adik-adikku tersayang Nabila Sahrani Isrofaatin dan Raden Kaisar Dhiaul Haq., yang menjadi sumber motivasiku dalam menempuh pendidikan setinggi-tingginya. Langkah dan pencapaian kalian menjadi inspirasi yang senyap tapi kuat, menuntunku untuk terus berjuang dan tidak mudah menyerah dan berpikir untuk mundur satu Langkah pun.
3. Keluarga besar saya yang tidak bisa saya sebutkan satu persatu, saya sangat berterima kasih atas dukungan, doa, dan pertanyaan-pertanyaan kapan lulus yang sangat memotivasi saya. Semoga Allah SWT membalas doa-doa baik dan kebaikan kalian.

LEMBAR PEDOMAN PENGGUNAAN TUGAS AKHIR

Tugas Akhir ini tidak dipublikasikan, tetapi tersedia di perpustakaan dalam lingkungan UIN Sunan Kalijaga, yang diperkenankan dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penyusun, dan harus menyebutkan sumbernya sesuai dengan kebiasaan ilmiah. Dokumen Tugas Akhir ini merupakan hak milik UIN Sunan Kalijaga Yogyakarta

INTISARI

Meningkatnya jumlah serangan siber pada infrastruktur jaringan dan aplikasi web telah menjadi ancaman serius bagi keamanan data dan layanan digital. Dua serangan yang paling umum dan berbahaya adalah Distributed Denial of Service (DDoS) dan Cross-Site Scripting (XSS). Serangan DDoS, khususnya jenis SYN Flood, dapat melumpuhkan layanan jaringan dengan membanjiri server dengan permintaan koneksi palsu, sementara XSS memungkinkan penyerang untuk menyuntikkan skrip berbahaya ke dalam aplikasi web untuk mencuri informasi atau membajak sesi pengguna. Dalam konteks ini, penelitian diperlukan untuk mengeksplorasi langkah-langkah mitigasi yang efektif terhadap kedua serangan tersebut, terutama pada perangkat jaringan MikroTik dan aplikasi web yang rentan.

Metode penelitian dilakukan menggunakan pendekatan eksperimental dengan simulasi skenario serangan dalam lingkungan yang terkendali. Untuk memitigasi serangan DDoS tipe SYN Flood pada router MikroTik, konfigurasi Firewall RAW diterapkan untuk memblokir lalu lintas berbahaya sebelum mencapai tahap pemrosesan utama. Sementara itu, pengujian serangan XSS dilakukan pada aplikasi web untuk mengidentifikasi kerentanan keamanan dan mengevaluasi efektivitas teknik pencegahan seperti validasi input dan sanitasi output. Pengujian menggunakan alat uji penetrasi serta pemantauan kinerja perangkat dan aplikasi untuk mengukur dampak dan keberhasilan strategi mitigasi.

Hasilnya menunjukkan bahwa penerapan Firewall RAW pada MikroTik efektif mengurangi beban CPU hingga 35% dan mengurangi jumlah paket berbahaya yang masuk ke jaringan, sehingga menjaga stabilitas koneksi. Untuk pengujian XSS, penerapan validasi input dan sanitasi output yang konsisten berhasil mencegah eksekusi skrip berbahaya di sisi klien, sehingga melindungi data pengguna yang sensitif. Temuan ini menunjukkan bahwa menggabungkan strategi keamanan di lapisan jaringan dan aplikasi dapat secara signifikan memperkuat pertahanan sistem terhadap serangan DDoS dan XSS, sekaligus menjadi referensi untuk mengembangkan kebijakan keamanan yang lebih komprehensif.

Kata Kunci: Keamanan Jaringan, DDoS, Banjir SYN, MikroTik, XSS, Firewall RAW, Validasi Input, Sanitasi Output

ABSTRACT

The increasing number of cyber attacks on network infrastructure and web applications has become a serious threat to data security and digital services. The two most common and dangerous attacks are Distributed Denial of Service (DDoS) and Cross-Site Scripting (XSS). DDoS attacks, particularly the SYN Flood type, can paralyze network services by flooding servers with fake connection requests, while XSS allows attackers to inject malicious scripts into web applications to steal information or hijack user sessions. In this context, research is needed to explore effective mitigation measures against both attacks, particularly on MikroTik network devices and vulnerable web applications.

The research method employed an experimental approach with simulated attack scenarios in a controlled environment. To mitigate SYN Flood-type DDoS attacks on MikroTik routers, RAW Firewall configuration was applied to block harmful traffic before it reaches the main processing stage. Meanwhile, XSS attack testing was conducted on web applications to identify security vulnerabilities and evaluate the effectiveness of prevention techniques such as input validation and output sanitization. Testing used penetration testing tools and device and application performance monitoring to measure the impact and success of mitigation strategies.

The results show that the implementation of Firewall RAW on MikroTik effectively reduces CPU load by up to 35% and reduces the number of malicious packets entering the network, thereby maintaining connection stability. For XSS testing, the implementation of consistent input validation and output sanitization successfully prevented the execution of malicious scripts on the client side, thereby protecting sensitive user data. These findings indicate that combining security strategies at the network and application layers can significantly strengthen system defenses against DDoS and XSS attacks, while also serving as a reference for developing more comprehensive security policies.

Keywords: Network Security, DDoS, SYN Flood, MikroTik, XSS, RAW Firewall, Input Validation, Output Sanitization

KATA PENGANTAR

Alhamdulillahirabbil'alamin, penulis panjatkan puja dan puji syukur ke hadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul "*Implementasi Dan Analisis Mitigasi Serangan Ddos Pada Aplikasi Web Menggunakan Router Mikrotik*". Shalawat serta salam tak lupa penulis curahkan kepada junjungan kita, Nabi Muhammad SAW, yang telah menjadi teladan terbaik bagi umat manusia. Skripsi ini dibuat untuk memenuhi tugas akhir perkuliahan sebagai salah satu syarat memperoleh gelar Sarjana Strata 1 di Program Studi Informatika UIN Sunan Kalijaga Yogyakarta. Pada kesempatan ini, penulis ingin menyampaikan banyak terima kasih kepada berbagai pihak yang telah memberikan bantuan, bimbingan, dukungan, serta motivasi sehingga penulis dapat menyelesaikan tugas akhir ini, di antaranya:

Pada kesempatan ini, penulis ingin menyampaikan banyak terima kasih pada berbagai pihak yang telah meberikan bantuan, bimbingan, dukungan, serta motivasi sehingga penulis dapat menyelesaikan tugas akhir ini, sebagai berikut:

1. Papa, Mama saya tercinta, atas doa dan kasih sayang, serta motivasi yang tak pernah putus. Terima kasih telah mengajarkan apa aitu cinta yang tulus, apa itu arti perjuangan di tanah rantau dan segala bentuk perkataan berupa motivasi dan di iringi doa di dalamnya untuk selalu melihat hikmah dan sisi positif dari setiap ujian kehidupan.
2. Kakak tercintaku, Arifa Anggraini Habidah S.T dan Adik-adikku tersayang Nabila Sahrani Isrofaatin dan Raden Kaisar Dhiaul Haq., yang menjadi sumber motivasiku dalam menempuh pendidikan setinggi-tingginya.
3. Bapak Prof. Noorhaidi, M.A, M.Phil., Ph.D., selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
4. Bapak Dr. Muhammad Mustakim, S.T. M.T., selaku Ketua Program Informatika Universitas Islam Negeri Sunan Kalijaga.
5. Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng. selaku dosen pembimbing skripsi, yang telah memberikan arahan, motivasi, serta waktu yang

berharga dalam membimbing penulis hingga tugas akhir ini terselesaikan dengan baik.

6. DR. IR. Shofwatul 'Uyun, S.T., M.KOM., IPM.selaku Dosen Pembimbing Akademik yang telah membantu selama perkuliahan.
7. Bapak Eko Hadi Gunawan, M.Eng., atas kesediaannya berdiskusi secara informal yang memberikan banyak inspirasi dan wawasan tambahan selama proses penulisan ini.
8. Penulis juga ingin menyampaikan rasa terima kasih kepada keluarga besar KKS yang telah memberi dukungan, semangat, maupun gangguan kecil yang penuh makna selama proses ini
9. Penulis juga ingin menyampaikan rasa terima kasih kepada teman-teman seperjuangan yang telah memberi dukungan, semangat, maupun gangguan kecil yang penuh makna selama proses ini.Terkhusus sahabat saya Rafi M. Farham dan Fansuri Fadel Fitrah keberadaan kalian tetap menjadi bagian yang menyenangkan dalam perjalanan ini. Dan semua pihak yang telah membantu dan berkontribusi dalam penyusunan skripsi yang tidak dapat disebutkan satu persatu.
10. Akhir kata, penulis mengharapkan skripsi ini dapat bermanfaat bagi penulis dan bagi pembaca pada umumnya.

Yogyakarta, 12 Agustus 2025

Penulis,

Alfathul Abror

20106050072

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi digital yang berkembang pesat telah menyebabkan masyarakat modern bergantung pada aplikasi web untuk berbagai keperluan, seperti transaksi keuangan, layanan e-commerce, pendidikan, hingga komunikasi daring. Di Indonesia, tren ini diperkuat oleh pertumbuhan jumlah pengguna internet yang signifikan dari tahun ke tahun. Survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) mencatat bahwa penetrasi pengguna internet meningkat dari 78,19% pada tahun 2023 (215,63 juta orang) menjadi 79,5% pada awal tahun 2024 (sekitar 221,56 juta orang), dengan peningkatan sekitar 1,4% dibandingkan tahun sebelumnya[1].

Tren pertumbuhan ini terus berlanjut, dengan estimasi penetrasi internet diperkirakan menembus angka 80% dari total populasi pada tahun 2025 (APJII, 2025) kontan.co.id. Kenaikan jumlah pengguna ini mencerminkan semakin meluasnya akses internet, termasuk di daerah rural yang kontribusinya mencapai sekitar 30–31% populasi pengguna[2].

Peningkatan digitalisasi masyarakat turut meningkatkan risiko serangan siber, terutama serangan yang menyasar availability layanan seperti Distributed Denial of Service (DDoS). Serangan DDoS dapat melumpuhkan sistem dengan membanjiri server menggunakan lalu lintas jaringan berlebih, sehingga kegunaan layanan bagi pengguna sah menjadi tidak tersedia[3].

Untuk menghadapi ancaman tersebut, berbagai teknologi mitigasi seperti firewall, load balancer, dan sistem deteksi intrusi (IDS) telah dikembangkan. Router MikroTik menjadi salah satu solusi populer di kalangan organisasi berskala menengah hingga kecil karena fitur-fitur configurable-nya, seperti *firewall*, *Quality of Service (QoS)*, *connection tracking*, dan *rate limiting*. Meskipun bukan solusi enterprise, MikroTik memungkinkan penyaringan trafik berbahaya seperti serangan SYN Flood sebelum mencapai *backend server*[4].

Walaupun beberapa studi awal menunjukkan potensi penggunaan MikroTik untuk mitigasi DDoS, efektivitas secara empiris pada lingkungan aplikasi web belum banyak dianalisis secara sistematis. Penelitian oleh Syaiful & Purba (2022) melaporkan bahwa penggunaan *firewall-raw* pada RouterOS efektif mengurangi beban kerja CPU perangkat

router, meskipun memperingatkan adanya keterbatasan performa perangkat keras saat menangani traffic sangat tinggi. Sementara itu, studi oleh Anung & Niti (2024) mencatat penurunan signifikan penggunaan CPU dan RAM server ketika firewall MikroTik diaktifkan di lingkungan LAN.

Dengan demikian, penelitian ini bertujuan untuk mengimplementasikan dan menganalisis mitigasi serangan DDoS pada aplikasi web menggunakan Router MikroTik, dengan fokus pada evaluasi beban sistem sebelum dan setelah penerapan firewall melalui pengujian empiris. Metode pengujian akan mencakup konfigurasi *connection tracking*, *rate limiting*, NAT, dan filter pola serangan seperti SYN Flood. Selain itu, penelitian ini juga akan memasukkan aspek keamanan aplikasi seperti potensi kerentanan Cross-Site Scripting (XSS), untuk memberikan pendekatan menyeluruh dari sudut pandang lapisan jaringan dan aplikasi[5].

Melalui pendekatan eksperimen dan analisis data, penelitian diharapkan dapat memberikan rekomendasi konfigurasi MikroTik yang optimal untuk mengurangi dampak serangan DDoS, sehingga menjaga ketersediaan layanan web dan memberikan strategi mitigasi yang tepat bagi organisasi dengan sumber daya terbatas[6].

Untuk mengatasi serangan DDoS, berbagai metode seperti firewall, load balancer, dan sistem deteksi intrusi telah dikembangkan. Router MikroTik sering digunakan karena fitur firewall dan QoS-nya yang dapat dikonfigurasi untuk mencegah dan memitigasi serangan DDoS. MikroTik juga menyediakan mekanisme perlindungan seperti filtering traffic, connection tracking, dan rate limiting, yang membantu mengidentifikasi dan menghalangi lalu lintas berbahaya sebelum mencapai server aplikasi web.

Meskipun MikroTik menawarkan berbagai fitur keamanan, efektivitas penerapannya dalam mitigasi serangan DDoS masih perlu dianalisis lebih lanjut. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan dan menganalisis mitigasi serangan DDoS pada aplikasi web menggunakan Router MikroTik. Melalui eksperimen dan pengujian, penelitian ini diharapkan dapat memberikan wawasan tentang sejauh mana konfigurasi MikroTik dapat mengurangi dampak serangan DDoS serta rekomendasi konfigurasi terbaik untuk meningkatkan ketahanan sistem terhadap ancaman tersebut[7].

Selain ancaman Distributed Denial of Service (DDoS), keamanan aplikasi web juga sering terancam oleh serangan pada lapisan aplikasi seperti Cross-Site Scripting (XSS). XSS

adalah kerentanan yang memungkinkan penyerang menyisipkan skrip berbahaya ke dalam halaman web yang dilihat oleh pengguna lain. Serangan ini terjadi ketika aplikasi web tidak melakukan validasi atau sanitasi input dengan benar, sehingga kode HTML atau JavaScript yang dimasukkan pengguna dapat dieksekusi di browser korban[7].

Dampak XSS dapat mencakup pencurian cookie sesi, pengambilalihan akun, pengalihan ke situs berbahaya, hingga manipulasi antarmuka pengguna. Relevansi XSS dalam penelitian ini adalah untuk menunjukkan bahwa meskipun mitigasi DDoS menggunakan MikroTik efektif pada lapisan jaringan, celah keamanan di lapisan aplikasi tetap dapat dimanfaatkan oleh penyerang. Oleh karena itu, keamanan menyeluruh memerlukan kombinasi antara perlindungan jaringan dan pengamanan kode aplikasi[8].

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, permasalahan yang akan dijadikan objek dalam penelitian ini adalah sebagai berikut:

1. Bagaimana karakteristik dan jenis serangan DdoS dan XSS yang dapat mengancam aplikasi web?
2. Bagaimana cara mengimplementasikan konfigurasi mitigasi serangan DDoS menggunakan Router MikroTik dan Bagaimana cara menangani serangan XSS pada Aplikasi Web?
3. Apa parameter kinerja jaringan yang dapat digunakan untuk mengukur efektivitas mitigasi serangan DDoS menggunakan MikroTik?

1.3 Tujuan Penelitian

Tujuan dari proyek Analisis Keamanan Website ejournal.uin-suka.ac.id terhadap Serangan Password Reset Poisoning Menggunakan Host Header Injection adalah sebagai berikut:

1. Menganalisis karakteristik dan jenis serangan DdoS dan XSS yang dapat mengancam aplikasi web.
2. Mengimplementasikan konfigurasi mitigasi serangan DDoS menggunakan Router MikroTik.
3. Mengimplementasikan konfigurasi mitigasi serangan XSS menggunakan teknik Secure Input Handling.

4. Mengukur kinerja jaringan berdasarkan parameter seperti bandwidth usage, latency, packet loss, dan CPU load sebelum dan sesudah penerapan mitigasi.
5. Menentukan konfigurasi optimal pada Router MikroTik untuk meningkatkan ketahanan aplikasi web terhadap serangan DDoS.
6. Mengubah konfigurasi dan mengontrol sumber konten (seperti JavaScript, CSS, gambar, atau iframe) yang dapat dimuat dan dijalankan oleh sebuah halaman web.

1.4 Manfaat Penelitian

Adanya beberapa manfaat yang dapat diambil dari proyek yang dibuat sebagai berikut:

1. . strategi mitigasi serangan XSS pada Web dan DDoS yang efektif menggunakan perangkat MikroTik.
2. Menambah referensi dan kajian akademik mengenai keamanan jaringan dan aplikasi .
3. Memberikan rekomendasi praktis bagi organisasi yang menggunakan MikroTik untuk perlindungan aplikasi web mereka.

1.5 Batasan Penelitian

Batasan masalah dalam penelitian ini dibatasi dengan ruang lingkup sebagai berikut:

1. Lokasi Penelitian: dilakukan di laboratorium SJK.
2. Waktu Penelitian: berlangsung selama kurang lebih 3 bulan.
3. Metode mitigasi yang digunakan: firewall dan rate-limiting pada DdoS dan Secure Input Handling pada XSS.
4. Perangkat yang digunakan: MikroTik CHR.
5. Web aplikasi yang digunakan sederhana dan mudah diserang
6. Metode pengumpulan data: Simulasi serangan DDoS yang dilakukan pada Web Server Ubuntu dan pada XSS hanya diuji terbatas pada serangan Stored XSS pada kolom komentar Aplikasi Web saja.

1.6 Sistematika Penulisan

Bab I: Pendahuluan — berisi latar belakang, rumusan masalah, tujuan, manfaat, batasan, dan sistematika penulisan.

Bab II: Tinjauan Pustaka — membahas literatur yang relevan dengan serangan DDoS, MikroTik, serta penelitian sebelumnya.

Bab III: Metodologi Penelitian — menjelaskan metode penelitian, lokasi dan waktu, objek penelitian, alat dan bahan, serta langkah-langkah implementasi.

Bab IV: Hasil dan Pembahasan — menyajikan hasil eksperimen dan analisis terhadap efektivitas mitigasi.

Bab V: Kesimpulan dan Saran — menyimpulkan temuan penelitian dan memberikan rekomendasi.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, pengujian, dan pembahasan yang telah dilakukan dalam implementasi dan analisis mitigasi serangan DDoS menggunakan Router MikroTik terhadap aplikasi web, maka kesimpulan yang dapat diambil disusun berdasarkan rumusan masalah sebagai berikut:

1. Karakteristik dan jenis serangan DDoS yang mengancam aplikasi web umumnya bersifat membanjiri lalu lintas jaringan dengan permintaan palsu secara terus-menerus, sehingga menyebabkan server menjadi overload dan tidak mampu merespons permintaan yang sah. Salah satu jenis serangan yang diuji dalam penelitian ini adalah SYN Flood, yaitu serangan berbasis protokol TCP yang menargetkan kelemahan dalam proses handshake. Serangan ini menyebabkan terbentuknya banyak koneksi setengah terbuka (half-open) yang menguras sumber daya server, sehingga berpotensi menyebabkan layanan web menjadi tidak responsif atau bahkan berhenti beroperasi.
2. Konfigurasi mitigasi serangan DDoS pada Router MikroTik dapat diimplementasikan dengan memanfaatkan fitur-fitur seperti firewall filter, connection tracking, NAT, rate limiting, dan address-list dinamis. Dalam penelitian ini, MikroTik CHR ditempatkan di antara attacker dan web server sebagai firewall yang menyaring trafik masuk. Beberapa rule penting yang diterapkan meliputi pembatasan koneksi TCP berdasarkan IP (menggunakan connection-limit), pembuatan address-list otomatis untuk memblokir IP mencurigakan, dan penggunaan firewall raw untuk menangani paket sebelum masuk ke connection tracking. Implementasi ini dilakukan secara virtual menggunakan VirtualBox dan terbukti dapat menahan lalu lintas berbahaya secara efektif.
3. Parameter kinerja jaringan yang digunakan untuk mengukur efektivitas mitigasi serangan DDoS dalam penelitian ini adalah penggunaan CPU server target. Penggunaan CPU dijadikan sebagai indikator utama karena serangan SYN Flood secara langsung mempengaruhi tingkat pemrosesan koneksi oleh server. Hasil pengujian menunjukkan bahwa tanpa mitigasi, beban CPU mencapai 100%, sedangkan setelah konfigurasi MikroTik diterapkan, beban CPU turun drastis menjadi 9–15%. Parameter ini

menunjukkan bahwa filtering di tingkat router dapat secara langsung mengurangi beban pemrosesan pada server aplikasi web.

4. Konfigurasi terbaik pada MikroTik untuk meningkatkan ketahanan aplikasi web terhadap serangan DDoS adalah kombinasi antara firewall filter rule, connection-limit, address-list dinamis, dan penggunaan firewall raw. Rule seperti pembatasan jumlah koneksi per IP, pemblokiran paket SYN berlebih, serta pemrosesan awal paket mencurigakan melalui raw prerouting terbukti efektif dalam menyaring trafik sebelum mencapai server. Dengan konfigurasi ini, Router MikroTik tidak hanya mampu meredam serangan, tetapi juga menjaga performa dan ketersediaan layanan web tetap optimal selama serangan berlangsung.
5. Penelitian ini berhasil menunjukkan bahwa penerapan firewall RAW pada Router MikroTik efektif dalam menurunkan beban CPU dan memblokir trafik berbahaya pada serangan DDoS SYN Flood. Sementara itu, serangan Stored XSS tidak dapat ditangani di level jaringan, tetapi dapat dimitigasi secara efektif di level aplikasi dengan kombinasi teknik validasi input, sanitasi output, output encoding, dan penerapan Content Security Policy (CSP), sehingga skrip berbahaya tidak dapat dieksekusi di browser korban.
6. Penelitian ini tidak bermaksud mengklaim tingkat keberhasilan secara kuantitatif, namun menunjukkan bahwa kombinasi mitigasi pada lapisan jaringan dan aplikasi mampu memberikan perlindungan yang lebih komprehensif sehingga sistem dapat beroperasi dengan lebih aman.

5.2 Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, penulis memberikan beberapa saran yang diharapkan dapat menjadi masukan bagi pengembangan sistem keamanan jaringan, khususnya dalam mitigasi serangan DDoS terhadap aplikasi web menggunakan Router MikroTik:

1. Perlu dilakukan pengujian lebih lanjut dengan variasi jenis serangan DDoS lainnya, seperti UDP Flood, ICMP Flood, dan HTTP Flood, agar diperoleh gambaran yang lebih komprehensif mengenai efektivitas konfigurasi MikroTik terhadap berbagai tipe serangan. Setiap jenis serangan memiliki pola dan karakteristik yang berbeda, sehingga dapat memengaruhi kinerja sistem dengan cara yang tidak sama.

2. Dianjurkan untuk mengintegrasikan sistem monitoring dan logging yang lebih detail seperti penggunaan IDS (Intrusion Detection System) berbasis open-source, misalnya Snort atau Suricata, guna memantau aktivitas lalu lintas jaringan secara real-time. Integrasi ini dapat membantu administrator dalam mendeteksi pola serangan lebih awal dan memberikan respons yang lebih cepat terhadap potensi ancaman.
3. Untuk implementasi di lingkungan nyata, seperti jaringan institusi pendidikan atau organisasi kecil-menengah, sebaiknya dilakukan penyesuaian konfigurasi secara periodik dan berkala, mengingat pola serangan siber selalu mengalami evolusi. Administrator jaringan perlu rutin memeriksa performa firewall MikroTik, memperbarui rule filtering, dan mengevaluasi efektivitas address-list agar tetap sesuai dengan kondisi terkini.
4. Penggunaan perangkat keras Mikrotik yang memiliki spesifikasi lebih tinggi dapat dipertimbangkan apabila mitigasi dilakukan pada lingkungan dengan lalu lintas data yang padat atau berada dalam jaringan produksi. Meskipun Mikrotik CHR dapat berjalan efektif di lingkungan virtual, penggunaan perangkat fisik dengan kemampuan CPU dan RAM yang lebih besar akan meningkatkan efisiensi dan daya tahan sistem terhadap serangan berskala besar.
5. Penelitian selanjutnya diharapkan dapat mengkaji aspek bandwidth usage dan packet loss sebagai parameter tambahan, guna memberikan analisis performa jaringan yang lebih mendalam. Selain penggunaan CPU, kedua parameter tersebut juga penting dalam menilai sejauh mana serangan berdampak pada kualitas layanan dan kestabilan jaringan secara keseluruhan.
6. Menerapkan Validasi Input yang Ketat – Pastikan semua data dari pengguna diperiksa sesuai format yang diizinkan sebelum disimpan atau diproses, serta menolak input yang mengandung tag HTML atau skrip.
7. Melakukan Sanitasi Output – Gunakan fungsi seperti htmlspecialchars() atau htmlentities() sebelum menampilkan data ke browser, agar karakter khusus tidak dieksekusi.
8. Mengaktifkan Content Security Policy (CSP) – Membatasi sumber skrip yang boleh dijalankan oleh browser untuk mencegah eksekusi skrip berbahaya.

9. Melakukan Pengujian Keamanan Berkala – Gunakan penetration testing dan vulnerability scanner untuk mendeteksi celah XSS yang mungkin muncul setelah pembaruan sistem.
10. Memberikan Edukasi kepada Tim Pengembang – Pastikan semua pihak yang terlibat memahami praktik keamanan coding untuk mencegah celah serupa di masa depan.

DAFTAR PUSTAKA

1. Akamai Technologies. (2019). *What is a DDoS attack?* Akamai. https://www.akamai.com/us/en/resources/ddos-attacks
2. Gupta, V., & Gupta, S. (2017). *Serangan skrip lintas situs (XSS) dan mekanisme pertahanan: Klasifikasi.Jurnal Internasional Sistem*
3. Andriani. (2021). *Mitigasi serangan DDoS menggunakan MikroTik RouterOS*. [Unpublished undergraduate thesis].
4. Anung, & Niti. (2024). *Analisis efektivitas mitigasi DDoS menggunakan firewall MikroTik pada jaringan LAN*. [Unpublished research report].
5. Nunes, E., Laranjeira, R., & Vieira, M. (2021). *Menguji aplikasi web untuk XSS yang disimpan dan dipantulkan*Jo*Jurnal Sistem dan Perangkat Lunak* ,https://doi.org/10.1016/j.jss.2021.110890
6. APJII — Asosiasi Penyelenggara Jasa Internet Indonesia. (2024). *Survei penetrasi & perilaku pengguna internet Indonesia 2023/2024* (laporan). APJII. https://apjii.or.id
7. Cloudflare. (n.d.). *What is a DDoS attack?* Cloudflare Learning. https://www.cloudflare.com/learning/ddos/
8. Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning DDoS detection for consumer Internet of Things devices. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29–35). IEEE. https://doi.org/10.1109/SPW.2018.00013
9. Fakhmi, & Gultom. (2021). *[Judul lengkap tidak tersedia]*. [Unpublished manuscript].
10. Hping3. (n.d.). *hping3 manual / tool information*. Linux Documentation. https://linux.die.net/man/8/hping3
11. Invicti. (n.d.). *Low Orbit Ion Cannon (LOIC) — description and risks*. https://www.invicti.com/learn/low-orbit-ion-cannon-loic/
12. MDN Web Docs (Mozilla). (2024). *Content Security Policy (CSP)*. Mozilla Developer Network. https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
13. MicroTik. (2024). *RouterOS documentation / tcp-syncookies and firewall raw information*. MikroTik Help. https://help.mikrotik.com
14. Nginx. (n.d.). *Nginx documentation*. https://nginx.org/en/docs/

15. OWASP Foundation. (2023). *Cross Site Scripting (XSS)*. OWASP. https://owasp.org/www-community/attacks/xss
16. Salunkhe, H. S., Jadhav, S. V., & Bhosale, P. V. (2017). Analysis and review of TCP SYN flood attack on network with its detection and performance metrics. *International Journal of Engineering Research & Technology (IJERT)*, 6(1), 250–256.
17. Sensors (MDPI). Yang, C.-H., Wu, J.-P., Lee, F.-Y., Lin, T.-Y., & Tsai, M.-H. (2023). Detection and mitigation of SYN flooding attacks through SYN/ACK packets and black/white lists. *Sensors, 23*(8), 3817. https://doi.org/10.3390/s23083817
18. Siregar, dkk. (2023). *Pengujian firewall RAW MikroTik terhadap efisiensi trafik TCP/UDP saat serangan DDoS*. [Unpublished manuscript].
19. Syaiful, & Purba. (2022). *Optimalisasi firewall RAW MikroTik dalam menangani serangan SYN flood*. [Unpublished manuscript].
20. VirtualBox (Oracle). (2025). *Oracle VM VirtualBox — documentation*. https://www.virtualbox.org/
21. Wireshark Foundation. (2025.). *Wireshark user guide / documentation*. https://www.wireshark.org/docs/
22. Yuwono. (2020). *Analisis performansi MikroTik sebagai firewall pada jaringan komputer*. [Unpublished manuscript].
23. Setiawan, A., & Nugroho, Y. (2025). *Analisis Efektivitas RAW Firewall MikroTik dalam Mitigasi Serangan DDoS pa*Jurnal Sains dan Teknologihttps://jurnal.g