# IMPLEMENTASI MITIGASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE (DDOS)* PADA ROUTER MIKROTIK MENGGUNAKAN METODE *FIREWALL RAW, RATE LIMIT, DAN PORT HARDENING*

**SKRIPSI**

**Alvito Revansyah Gunawan 2207421015**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

**2026**

# IMPLEMENTASI MITIGASI SERANGAN *DISTRIBUTED DENIAL OF SERVICE (DDOS)* PADA ROUTER MIKROTIK MENGGUNAKAN METODE *FIREWALL RAW, RATE LIMIT, DAN PORT HARDENING*

**SKRIPSI**

**Dibuat untuk Melengkapi Syarat – Syarat yang Diperlukan untuk Memperoleh Diploma Empat Politeknik**

**Alvito Revansyah Gunawan**

**2207421015**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

**2026**

## SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

| | |
|---|---|
| Nama | : Alvito Revansyah Gunawan |
| NIM | : 2207421015 |
| Jurusan/Program Studi | : Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan |
| Judul Skripsi | : Implementasi Mitigasi Serangan Distributed Denial of Service (Ddos) Pada Router Mikrotik Menggunakan Metode Firewall Raw, Rate Limit, Dan Port Hardening. |

Menyatakan dengan sebenarnya bahwa skripsi ini benar – benar merupakan hasil karya saya sendiri, bebas dari peniruan terhadap karya dari orang lain. Kutipan pendapat dan tulisan orang lain ditunjuk sesuai dengan cara-cara penulisan karya ilmiah yang berlaku.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam skripsi ini terkandung ciri – ciri plagiat dan bentuk – bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Depok, 15 Juni 2026

Yang membuat pernyataan


Alvito Revansyah Gunawan

NIM. 2207421015

## LEMBAR PENGESAHAN

Skripsi diajukan oleh:

| | |
|---|---|
| Nama | : Alvito Revansyah Gunawan |
| NIM | : 2207421015 |
| Program Studi | : Teknik Multimedia dan Jaringan |
| Judul Skripsi | : Implementasi Mitigasi Serangan Distributed Denial of Service (Ddos) Pada Router Mikrotik Menggunakan Metode Firewall Raw, Rate Limit, Dan Port Hardening |

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, Tanggal 14, Bulan Juli Tahun 2026 dan dinyatakan **LULUS.**

**Disahkan oleh:**

| | | |
|---|---|---|
| Pembimbing I | Ariawan Andi Suhandana, S. Kom., M.T.I. | ( ) |
| Penguji I | Defiana Arnaldy, S.Tp., M.Si. | ( ) |
| Penguji II | Fachroni Arbi Murad, S. Kom., M. Kom. | ( ) |
| Penguji III | Andika Riyadi Jasril, M.Pd.T. | ( ) |

Mengetahui:
Jurusan Teknik Informatika dan Komputer
Ketua

Dr. Anita Hidayati, S. Kom., M. Kom.
NIP. 197908032003122003

## KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Implementasi Mitigasi Serangan Distributed Denial of Service (DDoS) pada Router MikroTik Menggunakan Metode Port Hardening, Firewall RAW, dan Rate Limit".

Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Diploma Empat pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta. Penelitian ini membahas penerapan *Firewall RAW*, *Rate Limiting*, *Port Hardening*, serta simulasi RTBH dalam mitigasi serangan DDoS pada router MikroTik.

Dalam penyusunan skripsi ini, penulis memperoleh bantuan, arahan, dan dukungan dari berbagai pihak. Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Bapak Ariawan Andi Suhandana, S. Kom., M.T.I., selaku dosen pembimbing yang telah memberikan bimbingan, arahan, dan masukan selama proses penyusunan skripsi.
2. Seluruh dosen Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta, yang telah memberikan ilmu dan pengalaman selama masa perkuliahan.
3. Pihak PT XYZ yang telah memberikan informasi dan dukungan dalam proses pengumpulan data serta kebutuhan penelitian.
4. Bapak M. Ichwan Hardiansyah, selaku IP Network Engineer di PT XYZ, yang telah membantu memberikan informasi teknis, arahan, serta dukungan dalam proses implementasi dan pengujian pada penelitian ini.

5. Orang tua dan keluarga yang selalu memberikan doa, dukungan, dan motivasi kepada penulis.
6. Teman-teman kelas TMJ 22 serta pihak yang telah memberikan dukungan, bantuan, dan semangat kepada penulis selama proses penyusunan skripsi ini.
7. Syifa Chandra Tiffani Sumardi, Muhammad Abdan Syakuron, Sahrul Apriandi, Jibran Khairy Akram, Raden Muhammad Fadil Azhar, Stephanie Meissya P dan Harsdyka Wibisono yang senantiasa memberikan dukungan, motivasi, serta menjadi tempat berbagi cerita dan pengalaman selama proses perkuliahan hingga penyelesaian skripsi ini.

Penulis menyadari bahwa skripsi ini masih memiliki kekurangan. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun agar penelitian ini dapat menjadi lebih baik. Semoga skripsi ini dapat memberikan manfaat bagi pembaca, khususnya dalam bidang keamanan jaringan dan mitigasi serangan DDoS pada router MikroTik.

Depok, 2026

Penulis,

Alvito Revansyah Gunawan

## SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Politeknik Negeri Jakarta, saya bertanda tangan dibawah ini:

| | |
|---|---|
| Nama | : Alvito Revansyah Gunawan |
| NIM | : 2207421015 |
| Jurusan/Program Studi | : Teknik Informatika dan Komputer/Teknik Multimedia dan Jaringan |

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Politeknik Negeri Jakarta Hak Bebas Royalti Non-Eksklusif atas karya ilmiah saya yang berjudul:

**Implementasi Mitigasi Serangan *Distributed Denial Of Service (Ddos)* Pada Router Mikrotik Menggunakan Metode *Firewall Raw, Rate Limit, Dan Port Hardening***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalihmediakan/formatkan, mengelola dalam bentuk pangkalan data (database), merawat, dan mempublikasikan skripsi saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Depok, 15 Juni 2026

Yang menyatakan


Alvito Revansyah Gunawan

NIM.2207421015

**Implementasi Mitigasi Serangan *Distributed Denial of Service (Ddos)* Pada Router Mikrotik Menggunakan Metode *Firewall Raw, Rate Limit*, Dan *Port Hardening***

## *ABSTRAK*

*Serangan Distributed Denial of Service (DDoS) merupakan ancaman jaringan yang dapat menyebabkan layanan tidak tersedia akibat lonjakan trafik yang membebani router. Penelitian ini bertujuan menerapkan mitigasi serangan DDoS pada router MikroTik menggunakan metode Firewall RAW, Rate Limiting, dan Port Hardening, serta simulasi Remotely Triggered Black Hole (RTBH) sebagai langkah terakhir ketika trafik serangan perlu dibuang pada sisi upstream. Pengujian dilakukan pada jaringan uji terpisah dengan Kali Linux sebagai sumber serangan, MikroTik CHR sebagai router upstream, dan router MikroTik fisik sebagai objek pengujian akhir. Serangan yang diuji adalah UDP Flood dan TCP SYN Flood menggunakan hping3. Parameter pengamatan meliputi CPU Load, Free Memory, traffic WAN, dan jumlah paket yang diblokir. Hasil pengujian menunjukkan bahwa Firewall RAW mampu membuang trafik dari IP attacker pada tahap awal, sedangkan Rate Limiting membantu membatasi trafik berlebih yang masih diproses router. Port Hardening memperkuat akses manajemen melalui pembatasan layanan, penggantian Telnet dengan SSH, dan port knocking. Simulasi RTBH mampu menurunkan trafik ke router utama, tetapi seluruh trafik menuju IP target ikut terbuang.*

**Kata kunci:** DDoS, *Firewall RAW*, MikroTik, *Port Hardening*, *Rate Limiting*, RTBH.

# DAFTAR ISI

# DAFTAR TABEL

## DAFTAR GAMBAR

# BAB I
# PENDAHULUAN

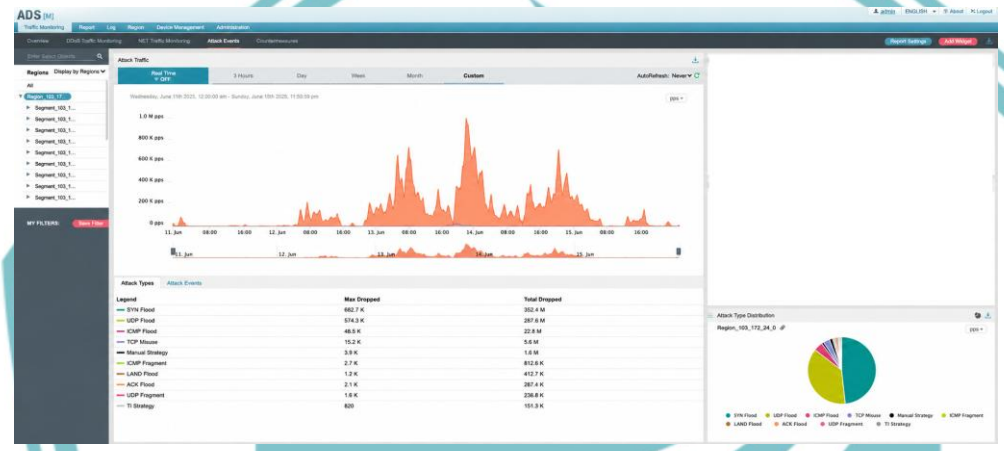
## 1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat menjadikan jaringan komputer sebagai komponen utama dalam mendukung operasional perusahaan, khususnya pada layanan berbasis internet. Tingginya ketergantungan terhadap jaringan menyebabkan aspek keamanan menjadi sangat penting, karena gangguan pada jaringan dapat berdampak langsung pada kualitas layanan dan aktivitas operasional. Salah satu ancaman yang sering terjadi pada infrastruktur jaringan adalah serangan siber yang menargetkan ketersediaan layanan, seperti serangan *Distributed Denial of Service* (DDoS), yang mampu melumpuhkan jaringan dalam waktu singkat dengan membanjiri lalu lintas data secara berlebihan (Mamuriyah et al., 2024; Susanto et al., 2023).

Router MikroTik berperan sebagai gerbang utama yang menghubungkan jaringan lokal dengan internet publik, sehingga menjadi salah satu target utama serangan DDoS. Ketika router tidak dilengkapi dengan konfigurasi keamanan yang memadai, serangan DDoS dapat menyebabkan lonjakan penggunaan sumber daya perangkat, seperti peningkatan beban CPU dan kepadatan lalu lintas jaringan. Kondisi ini berpotensi menyebabkan layanan jaringan menjadi tidak stabil atau bahkan tidak dapat diakses oleh pengguna yang sah (Riduan et al., 2025).

Berdasarkan informasi yang diperoleh melalui wawancara daring dengan pihak teknis PT XYZ, diketahui bahwa perusahaan mengalami permasalahan serius pada infrastruktur jaringan akibat serangan siber. Serangan tersebut menyebabkan gangguan layanan internet yang berdampak langsung pada operasional perusahaan. Pihak manajemen

menyampaikan bahwa gangguan jaringan yang terjadi menimbulkan kerugian materi yang diperkirakan mencapai kisaran 1 hingga 3 miliar rupiah, yang berasal dari hilangnya pendapatan layanan, biaya pemulihan sistem, serta penanganan gangguan jaringan. Selain itu, kondisi tersebut juga berdampak pada penurunan nilai perusahaan dan berkurangnya jumlah pelanggan akibat ketidakpuasan terhadap kualitas layanan yang diberikan.



Gambar 1. 1 Data Monitoring Serangan pada Jaringan PT XYZ

Sumber: IP Network Engineer PT XYZ

Berdasarkan data monitoring serangan dari PT XYZ, terlihat adanya lonjakan *attack traffic* dalam satuan *packet per second* (pps) pada periode 11 Juni 2025 sampai 15 Juni 2025. Pada grafik monitoring, trafik serangan mengalami beberapa lonjakan besar, dengan puncak tertinggi mendekati 1,0 juta pps sekitar tanggal 14 Juni 2025. Data *Attack Types* menunjukkan bahwa serangan yang dominan adalah *SYN Flood* dan *UDP Flood*, di mana *SYN Flood* memiliki nilai *Max Dropped* sebesar 682,7 K pps dengan *Total Dropped* 352,4 juta paket, sedangkan *UDP Flood* memiliki nilai *Max Dropped* sebesar 574,3 K pps dengan *Total Dropped* 287,6 juta paket. Besarnya jumlah paket yang diblokir menunjukkan bahwa jaringan menerima trafik *flooding* dalam volume tinggi dan berpotensi membebani perangkat router. Kondisi tersebut dapat menyebabkan peningkatan penggunaan

sumber daya perangkat, seperti *CPU Load* dan memori, serta mengganggu kestabilan layanan jaringan. Oleh karena itu, data monitoring ini digunakan sebagai dasar pemilihan skenario pengujian pada penelitian, yaitu *UDP Flood* dan *TCP SYN Flood* pada router MikroTik.

Dampak serangan tidak hanya dirasakan dari sisi finansial, tetapi juga memengaruhi kepercayaan publik terhadap PT XYZ. Banyaknya keluhan pelanggan serta sentimen negatif yang muncul di media sosial menunjukkan adanya penurunan reputasi layanan perusahaan. Dari sisi teknis, gangguan jaringan ditandai dengan lonjakan penggunaan *Central Processing Unit* (CPU) router hingga mencapai 100%, disertai dengan terkurasnya kapasitas *Random Access Memory* (RAM) dalam waktu singkat. Kondisi ini mengindikasikan bahwa serangan yang terjadi bersifat masif dan bertujuan untuk menghabiskan sumber daya perangkat jaringan, sehingga *router* tidak mampu memproses lalu lintas data secara normal dan layanan menjadi tidak tersedia bagi pengguna yang sah (Kushaeiri et al., 2024).

Serangan DDoS yang terjadi umumnya dilakukan dengan mengirimkan trafik dalam jumlah besar secara terus-menerus, sehingga memenuhi kapasitas bandwidth dan membebani proses pengolahan paket pada *router*. Akibatnya, lalu lintas data yang sah tidak dapat diproses dengan baik dan layanan jaringan menjadi tidak tersedia. Kondisi ini menunjukkan bahwa diperlukan mekanisme mitigasi yang mampu menyaring trafik berbahaya sejak tahap awal sebelum membebani sumber daya router (Siregar et al., 2025).

Pendekatan mitigasi serangan Denial of Service berbasis firewall telah dibahas dalam penelitian sebelumnya melalui analisis efektivitas penggunaan firewall iptables dalam menghadapi serangan Slowloris pada web server. Penelitian tersebut menunjukkan bahwa penerapan

firewall mampu membatasi serta memblokir lalu lintas serangan secara langsung, sehingga ketersediaan layanan tetap dapat dipertahankan meskipun sistem menerima trafik serangan. Hasil penelitian tersebut menegaskan bahwa mekanisme penyaringan trafik menggunakan firewall memiliki peran penting dalam menjaga stabilitas layanan jaringan dari serangan yang bertujuan mengganggu ketersediaan layanan (Oktivasari et al., 2022).

Untuk mengatasi permasalahan tersebut, penelitian ini menerapkan pendekatan keamanan berlapis dengan menggunakan metode *Firewall RAW*, *Rate Limiting*, dan *Port Hardening* pada router MikroTik. *Firewall RAW* digunakan untuk memblokir paket mencurigakan pada tahap awal pemrosesan, sehingga dapat mengurangi beban *CPU router*. *Rate Limiting* diterapkan untuk membatasi jumlah trafik atau koneksi dari satu sumber agar tidak melebihi batas yang ditentukan. Selain itu, *Port Hardening* digunakan untuk mengamankan akses manajemen *router* dengan membatasi *port* yang dapat diakses dari jaringan publik (Riduan et al., 2025; Hendry, 2024; Siregar et al., 2025).

Sebagai tambahan, penelitian ini juga mempertimbangkan penggunaan metode *Remotely Triggered Black Hole (RTBH)* sebagai salah satu cara untuk mengurangi dampak serangan DDoS pada jaringan. Metode ini bekerja dengan cara mengarahkan seluruh trafik yang menuju alamat IP target ke jalur khusus sehingga paket data tersebut dibuang sebelum mencapai jaringan utama. Dengan demikian, serangan dapat dihentikan dari sisi upstream dan tidak membebani router internal. Namun, penerapan RTBH secara langsung membutuhkan dukungan dari penyedia layanan internet (ISP) serta konfigurasi protokol routing seperti BGP, sehingga sulit diterapkan pada lingkungan penelitian atau jaringan internal yang memiliki keterbatasan akses. Oleh karena itu, pada penelitian ini RTBH hanya

disimulasikan secara sederhana menggunakan fitur blackhole route pada MikroTik untuk menggambarkan prinsip kerjanya, dan hasilnya digunakan sebagai skenario tambahan untuk menunjukkan kondisi ketika trafik harus dibuang pada sisi *upstream* (Khant Htal Myo, 2025).

Melalui penerapan ketiga metode tersebut, penelitian ini bertujuan untuk meningkatkan keamanan dan kestabilan jaringan PT XYZ dalam menghadapi serangan DDoS. Pendekatan ini difokuskan pada mitigasi di sisi gateway agar layanan tetap dapat berjalan tanpa harus memutus akses secara keseluruhan, seperti pada metode RTBH. Diharapkan sistem mitigasi yang diterapkan mampu mengurangi dampak serangan terhadap penggunaan CPU dan lalu lintas jaringan, sehingga layanan internet kepada pelanggan dapat tetap berjalan dengan baik dan gangguan operasional dapat diminimalkan.

## 1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan, fokus penelitian ini adalah peningkatan keamanan infrastruktur jaringan melalui pendekatan preventif dan mitigasi teknis. Maka, rumusan masalah yang diajukan adalah:

1. Bagaimana kondisi kerentanan router MikroTik terhadap serangan *packet flooding* berupa UDP *Flood* dan TCP SYN *Flood* serta pengaruhnya terhadap CPU Load, Free Memory, dan trafik jaringan?
2. Bagaimana penerapan *Port Hardening* dapat mengurangi celah keamanan pada akses manajemen router MikroTik?
3. Bagaimana merancang dan mengimplementasikan *Firewall RAW* serta *Rate Limiting* untuk memitigasi serangan UDP *Flood* dan TCP SYN *Flood* pada router MikroTik?

4. Sejauh mana efektivitas *Firewall RAW* dan *Rate Limiting* dalam mengurangi dampak serangan DDoS terhadap penggunaan sumber daya router?
5. Bagaimana penerapan simulasi metode Remotely Triggered Black Hole (RTBH) dalam menangani serangan DDoS pada router MikroTik?

## 1.3 Batasan Masalah

Berdasarkan latar belakang dan perumusan masalah yang telah diuraikan, ruang lingkup permasalahan pada penelitian ini perlu dibatasi agar pembahasan lebih terarah dan tidak meluas ke aspek keamanan jaringan lain yang berada di luar fokus penelitian. Oleh karena itu, batasan masalah dalam penelitian ini dirumuskan sebagai berikut:

1. Penelitian ini berfokus pada penanganan serangan Distributed Denial of Service (DDoS) pada lapisan Transport (Layer 4), khususnya UDP *Flood* dan TCP SYN *Flood*. Penelitian ini tidak membahas serangan pada lapisan aplikasi seperti HTTP *Flood*, Slowloris, maupun serangan lain seperti *phishing* dan SQL *injection*.
2. Pengukuran dampak serangan dibatasi pada kondisi sumber daya router dan lalu lintas jaringan, yaitu CPU Load, Free Memory, *traffic* WAN, serta jumlah paket yang diblokir oleh rule mitigasi. Penelitian ini tidak membahas dampak serangan terhadap server, aplikasi, atau layanan *backend* secara mendalam.
3. Objek penelitian tidak menggunakan jaringan operasional aktif PT XYZ. Implementasi awal dan validasi konfigurasi dilakukan pada lingkungan laboratorium menggunakan MikroTik CHR, sedangkan pengujian akhir dilakukan pada router MikroTik fisik

milik PT XYZ yang ditempatkan pada jaringan uji terpisah agar tidak mengganggu layanan pelanggan.

4. Metode mitigasi yang digunakan dibatasi pada fitur bawaan MikroTik, yaitu *Firewall RAW*, *Rate Limiting*, dan *Port Hardening*. Penelitian ini tidak membandingkan hasil mitigasi dengan perangkat Anti-DDoS pihak ketiga, *load balancing*, atau sistem keamanan eksternal lainnya.
5. Evaluasi efektivitas mitigasi dilakukan melalui skenario pengujian bertahap, yaitu tanpa mitigasi, *Firewall RAW*, kombinasi *Firewall RAW* dan *Rate Limiting*, serta simulasi RTBH. *Port Hardening* diuji secara terpisah melalui pengujian akses layanan manajemen router.
6. Simulasi RTBH pada penelitian ini hanya dilakukan menggunakan mekanisme *blackhole route* pada MikroTik. Penelitian ini tidak menerapkan RTBH nyata berbasis BGP dan tidak melibatkan kerja sama langsung dengan ISP atau pihak *upstream*.
7. Konfigurasi *Port Hardening* disesuaikan dengan informasi dari pihak teknis PT XYZ terkait layanan manajemen MikroTik yang digunakan. Layanan yang tidak digunakan seperti API, API-SSL, FTP, WWW, dan WWW-SSL dinonaktifkan, sedangkan layanan manajemen yang masih digunakan dibatasi sesuai kebutuhan pengujian.
8. Pengujian pada penelitian ini tidak menggunakan serangan DDoS nyata dari banyak sumber, melainkan merepresentasikan karakteristik trafik DDoS melalui simulasi *UDP Flood* dan *TCP SYN Flood* menggunakan satu perangkat Kali Linux pada jaringan uji terpisah.

## 1.4 Tujuan dan Manfaat

Berdasarkan rumusan masalah yang telah disusun, penelitian ini memiliki tujuan yang ingin dicapai serta manfaat yang diharapkan bagi pengembangan ilmu maupun praktik keamanan jaringan komputer. Oleh karena itu, pada bagian ini diuraikan tujuan dan manfaat penelitian sebagai berikut.

Tujuan penelitian ini adalah:

1. Mengidentifikasi dan menganalisis dampak serangan UDP *Flood* dan TCP SYN *Flood* terhadap stabilitas sumber daya router MikroTik, khususnya CPU Load, Free Memory, dan *traffic* jaringan.
2. Menerapkan metode *Port Hardening* melalui pengaturan layanan dan pembatasan akses manajemen router untuk mengurangi celah keamanan pada perangkat MikroTik.
3. Merancang dan mengimplementasikan *Firewall RAW* serta *Rate Limiting* untuk memitigasi trafik serangan UDP *Flood* dan TCP SYN *Flood* pada router MikroTik.
4. Mengevaluasi efektivitas *Firewall RAW* dan *Rate Limiting* dalam menjaga efisiensi penggunaan sumber daya router, serta mengevaluasi *Port Hardening* dalam memperkuat keamanan akses manajemen router.
5. Untuk mengetahui penerapan dan hasil simulasi metode Remotely Triggered Black Hole (RTBH) dalam menangani serangan DDoS pada router MikroTik.

Secara umum, penelitian ini diharapkan memberikan manfaat sebagai berikut:

1. Menambah kajian ilmiah di bidang keamanan jaringan (*Network Security*), khususnya terkait mekanisme mitigasi serangan *Distributed Denial of Service* (DDoS) pada lapisan transport

menggunakan fitur bawaan RouterOS MikroTik tanpa bergantung pada perangkat keras tambahan.

2. Memberikan gambaran mengenai karakteristik serangan UDP *Flood* dan TCP SYN *Flood* terhadap penggunaan CPU Load, Free Memory, dan *traffic* jaringan pada router MikroTik.
3. Menjadi referensi teknis bagi administrator jaringan dalam menerapkan pertahanan berlapis melalui *Firewall RAW*, *Rate Limiting*, dan *Port Hardening* untuk meningkatkan keamanan router.
4. Memberikan masukan bagi PT XYZ dalam memahami penerapan mitigasi DDoS pada router MikroTik, terutama pada lingkungan uji yang disesuaikan dengan kondisi jaringan perusahaan tanpa mengganggu layanan operasional

Bagi pihak perusahaan PT XYZ dan administrator jaringan pada umumnya, hasil penelitian ini dapat menjadi referensi teknis dan rekomendasi *best practice* dalam mengamankan infrastruktur router dari serangan DDoS, serta meningkatkan keandalan layanan jaringan melalui konfigurasi *Firewall Raw*, *Rate Limiting,* dan *Port Hardening*.

## 1.5 Sistematika Penulisan

Sistematika penulisan dalam penelitian ini terdiri dari 5 bab, yaitu:

1. BAB I PENDAHULUAN

   Bab I memuat latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan terkait pada Implementasi Mitigasi Serangan *Distributed Denial of Service* (DDoS) pada Router MikroTik Menggunakan Metode *Port Hardening*, *Firewall Raw*, dan *Rate Limit*.

2. BAB II TINJAUAN PUSTAKA

Bab II berisikan tinjauan pustaka dan landasan teori atau kajian ilmu secara garis besar mengenai topik permasalahan pada penelitian ini, serta beberapa penelitian-penelitian terdahulu berkaitan pada isu relevan.

3. BAB III METODOLOGI PENELITIAN

   Bab III menjabarkan penjelasan mengenai perencanaan dan perancangan sistem keamanan jaringan yang akan dibangun berupa Rancangan Penelitian, Tahapan Penelitian, Objek Penelitian (Simulasi Virtual), Jadwal Penelitian, dan Rincian Biaya dalam melakukan penelitian ini.

4. BAB IV HASIL DAN PEMBAHASAN

   Bab IV membahas hasil dari proses analisis kebutuhan, perancangan sistem, implementasi konfigurasi, serta pengujian sistem mitigasi serangan *DDoS* pada router MikroTik. Pada bab ini dijelaskan penerapan metode *Firewall RAW, Rate Limiting, Port Hardening*, serta simulasi *RTBH*, kemudian dilakukan pengujian terhadap serangan *UDP Flood* dan *TCP SYN Flood*. Hasil pengujian dianalisis berdasarkan parameter *CPU Load*, *Free Memory*, *traffic jaringan*, dan jumlah paket yang berhasil diblokir oleh rule mitigasi.

5. BAB V PENUTUP

   Bab V berisi kesimpulan dari hasil penelitian yang telah dilakukan serta saran untuk pengembangan penelitian selanjutnya. Kesimpulan disusun berdasarkan hasil implementasi dan pengujian sistem mitigasi yang telah diterapkan, sedangkan saran diberikan sebagai masukan untuk penyempurnaan sistem keamanan jaringan pada penelitian berikutnya.

# BAB V
# PENUTUP

Bab ini berisi simpulan dan saran berdasarkan hasil implementasi dan pengujian sistem mitigasi serangan DDoS pada router MikroTik. Simpulan disusun berdasarkan hasil pengujian terhadap serangan UDP *Flood* dan TCP SYN *Flood*, sedangkan saran diberikan sebagai masukan untuk pengembangan penelitian dan penerapan sistem keamanan jaringan selanjutnya.

## 5.1 Simpulan

Berdasarkan hasil pengujian, serangan *UDP Flood* dan *TCP SYN Flood* terbukti memberikan dampak terhadap stabilitas sumber daya router MikroTik. Pada kondisi tanpa mitigasi, serangan *UDP Flood* menyebabkan peningkatan *CPU Load*, penurunan *Free Memory*, serta kenaikan *traffic* pada *interface* WAN. Sementara itu, serangan *TCP SYN Flood* memberikan dampak yang lebih besar terhadap beban CPU karena router harus memproses banyak permintaan koneksi TCP secara terus-menerus. Hal ini menunjukkan bahwa router MikroTik tetap memiliki kerentanan terhadap serangan *packet flooding* apabila belum dilengkapi dengan konfigurasi mitigasi yang sesuai.

Penerapan *Port Hardening* berhasil dilakukan dengan menonaktifkan layanan manajemen yang tidak digunakan, seperti API, API-SSL, FTP, WWW, WWW-SSL, dan Telnet. Akses manajemen kemudian diperkuat dengan penggunaan SSH, pembatasan akses dari jaringan luar, serta penerapan *port knocking*. Hasil pengujian menunjukkan bahwa akses Telnet dari sisi luar tidak dapat dilakukan, akses SSH dari jaringan luar ditolak sebelum proses *port knocking*, dan akses hanya dapat dilakukan setelah alamat IP sumber berhasil masuk ke daftar *secured-admin*. Dengan demikian, *Port Hardening* dapat mengurangi celah keamanan pada akses manajemen router MikroTik.

Perancangan dan implementasi *Firewall RAW* serta *Rate Limiting* berhasil diterapkan untuk memitigasi trafik serangan *UDP Flood* dan *TCP SYN Flood*. *Firewall RAW* digunakan untuk membuang trafik dari IP *attacker* yang telah terdeteksi pada tahap awal melalui *chain prerouting*, sehingga paket serangan tidak diproses lebih jauh oleh router. Sementara itu, *Rate Limiting* digunakan untuk membatasi paket *UDP* dan *TCP SYN* berlebih yang masih sempat diproses oleh router. Implementasi ini menunjukkan bahwa kedua metode dapat bekerja sebagai mekanisme mitigasi berlapis pada router MikroTik.

Hasil evaluasi menunjukkan bahwa *Firewall RAW* dan *Rate Limiting* mampu membantu menjaga efisiensi penggunaan sumber daya router saat terjadi serangan. Pada skenario *TCP SYN Flood*, kondisi tanpa mitigasi menyebabkan *CPU Load* sangat tinggi, sedangkan setelah *Firewall RAW* diterapkan, beban CPU menjadi lebih terkendali dan jumlah paket yang diblokir terus meningkat. Pada skenario kombinasi *Firewall RAW* dan *Rate Limiting*, *Firewall RAW* terlihat lebih dominan karena trafik dari IP *attacker* langsung dibuang setelah terdeteksi, sedangkan *Rate Limiting* berperan sebagai lapisan tambahan untuk membatasi trafik berlebih. Selain itu, *Port Hardening* terbukti memperkuat keamanan akses manajemen router, meskipun pengujiannya dilakukan secara fungsional dan bukan berdasarkan parameter CPU atau memori.

Simulasi *Remotely Triggered Black Hole* atau RTBH berhasil diterapkan menggunakan mekanisme *blackhole route* pada router *upstream*. Hasil pengujian menunjukkan bahwa ketika RTBH diaktifkan, trafik serangan tidak lagi diteruskan ke MikroTik utama sehingga *traffic* pada *interface* WAN menurun secara signifikan dan beban CPU router utama menjadi rendah. Namun, RTBH juga membuang seluruh trafik menuju IP target, termasuk trafik normal. Oleh karena itu, RTBH tidak digunakan sebagai metode utama,

melainkan sebagai langkah terakhir ketika mitigasi utama seperti *Firewall RAW*, *Rate Limiting*, dan *Port Hardening* tidak mampu menahan dampak serangan yang lebih besar.

## 5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, terdapat beberapa saran yang dapat digunakan untuk pengembangan penelitian selanjutnya maupun penerapan pada lingkungan jaringan yang lebih luas.

Pertama, nilai ambang batas pada *Firewall RAW* dan *Rate Limiting* perlu disesuaikan kembali apabila diterapkan pada jaringan operasional. Nilai batas yang digunakan pada penelitian ini disusun berdasarkan kebutuhan pengujian dan kondisi perangkat yang digunakan, sehingga pada penerapan nyata perlu dilakukan penyesuaian terhadap pola trafik normal pelanggan agar tidak menyebabkan *false positive*.

Kedua, penelitian selanjutnya dapat menambahkan parameter pengujian lain seperti latency, packet loss, atau throughput. Parameter tersebut dapat digunakan untuk melihat dampak mitigasi tidak hanya dari sisi CPU Load, Free Memory, dan *traffic* jaringan, tetapi juga dari sisi kualitas layanan yang dirasakan oleh pengguna.

Ketiga, simulasi RTBH dapat dikembangkan lebih lanjut dengan rancangan yang lebih mendekati kondisi jaringan skala besar. Pada penelitian ini, RTBH masih disimulasikan menggunakan *blackhole route* pada MikroTik, sehingga penelitian selanjutnya dapat mengkaji skenario RTBH yang melibatkan mekanisme *routing* yang lebih lengkap pada lingkungan uji yang aman dan terkontrol.

## DAFTAR PUSTAKA

Fikri, A. H., Rahmi, A. A., & Rahman, R. (2025). *Analisis keamanan protokol Telnet vs SSH menggunakan Wireshark dalam jaringan terbuka*. Journal of System & Technology, 1(1), 26–29.

Haniyah, W., Hidayat, M. C., Putra, Z. F. I., Pertama, V. A., & Setiawan, A. (2024). *Simulasi serangan Denial of Service (DoS) menggunakan Hping3 melalui Kali Linux*. Journal of Internet and Software Engineering, 1–8.

Hardono, H. (2024). *Manajemen bandwidth router MikroTik menggunakan metode Simple Queue di laboratorium komputer SMA Swasta Kemala Bhayangkari Kotabumi*. Jurnal Sienna, 5(1).

Hendry, S. (2024). *Membangun sekuritas jaringan terhadap penggunaan VPN, serangan DDoS, dan akses eksternal ke MikroTik*. Samarinda: STMIK Widya Cipta Dharma.

Khant Htal Myo. (2025). *BGP Routing Security Using Remotely Triggered Blackholing*.

Kushaeiri, F. A., Muhyidin, Y., & Singasatia, D. (2024). *Implementasi pencegahan serangan DDoS pada router MikroTik menggunakan metode ethical hacking*. Jurnal Ilmiah Sain dan Teknologi, 2(11), 229–244.

Lueis, P. dan Kanigoro, B. (2025). *Multithreaded Automation for Mass Configuration of MikroTik Routers in Campus Networks*. Proceedings of the International Conference on Cyber and IT Service Management (CITSM).

Mamuriyah, N., Prasetyo, S. E., & Sijabat, A. O. (2024). *Rancangan sistem keamanan jaringan dari serangan DDoS menggunakan*

*metode pengujian penetrasi*. Jurnal Teknologi dan Sistem Informasi Bisnis, 6(1), 162–167.

Oktivasari, P., Zain, A.R., Agustin, M., Kurniawan, A., Murad, F.A. and Anshor, M.F. (2022) *Analysis of Effectiveness of Iptables on Web Server from Slowloris Attack*. Proceedings of the 5th International Conference of Computer and Informatics Engineering (IC2IE). IEEE, pp. 215–219. doi:10.1109/IC2IE56416.2022.9970143.

Riduan, M. A. O., Riska, & Alamsyah, H. (2025). *Analisa dan implementasi keamanan jaringan berbasis firewall raw terhadap serangan DDoS pada router MikroTik*. Jurnal Media Infotama, 21(1).

Siregar, M. I., Lubis, I., & Liza, R. (2025). *Implementasi keamanan anti DDoS menggunakan router MikroTik pada layanan cloud storage berbasis lokal*. Jurnal Networking System and Security System, 2(1).

Sitorus, M. A., Nasution, D. dan Iqbal, M. (2025). *Analisis Efektivitas RAW Firewall MikroTik dalam Mitigasi Serangan DDoS pada Infrastruktur Jaringan*. Journal of Science and Social Research, 8(2), 3354–3358.

Susanto, Daru, A. F. dan Christanto, F. W. (2023). *Packet Filtering Gateway and Application Layer Gateway on MikroTik Router Based Firewalls for Server and Internet Access Restrictions*. Proceedings of the IEEE International Conference on Technology, Engineering, and Computing Applications.

Wijaya, F. I., Innuddin, M., & Latif, K. A. (2025). *Analisa penerapan fitur firewall pada MikroTik untuk mengamankan dari serangan Denial of Service (DoS)*. Panthera: Jurnal Ilmiah Pendidikan Sains dan Terapan, 5(3), 570–592.

## DAFTAR RIWAYAT HIDUP PENULIS

Penulis bernama Alvito Revansyah Gunawan, lahir di Jakarta pada tanggal 31 Januari 2003. Penulis menyelesaikan pendidikan dasar di SDN 01 Kebon Kosong pada tahun 2015, kemudian melanjutkan pendidikan di SMPN 59 Jakarta dan lulus pada tahun 2018. Selanjutnya, penulis menempuh pendidikan menengah kejuruan di SMKN 1 Jakarta dan lulus pada tahun 2022.

Setelah menyelesaikan pendidikan menengah kejuruan, penulis melanjutkan pendidikan ke jenjang perguruan tinggi di Politeknik Negeri Jakarta, Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan Jaringan. Selama menjalani perkuliahan, penulis mempelajari berbagai bidang terkait jaringan komputer, keamanan jaringan, sistem komputer, serta teknologi multimedia.

## LAMPIRAN

Lampiran 1 – Dokumentasi Wawancara

Tempat : Daring (Online)

Tanggal : 17 Januari 2026

Narasumber : Pihak PT XYZ (M. Ichwan Hardiansyah - IP Network Engineer)

Wawancara dilakukan untuk memvalidasi permasalahan terkait kerentanan infrastruktur jaringan PT XYZ pasca-insiden serangan siber tahun 2025. Data yang diperoleh meliputi detail teknis mengenai kelelahan sumber daya (resource exhaustion) dan dampak kerugian finansial perusahaan. Hasil diskusi ini selanjutnya dijadikan dasar penentuan kebutuhan sistem, khususnya dalam perancangan konfigurasi Firewall Raw dan manajemen trafik sebagai solusi mitigasi utama.

| Pertanyaan | Jawaban |
|---|---|
| Bisa diceritakan mengenai insiden keamanan yang pernah terjadi di PT XYZ? | Pada tahun 2025, kami mengalami satu insiden berupa serangan DDoS. Meskipun hanya sekali, dampaknya sangat fatal karena menyebabkan traffic full dan pelanggan normal yang lain tidak mendapatkan traffic, akhirnya jaringan menjadi lemot. |
| Secara teknis, apa yang terjadi pada perangkat Router saat insiden itu berlangsung? | Saat kejadian, Resource CPU Router melonjak hingga 100% dan RAM terkuras habis. |
| Apa dampak kerugian yang dialami perusahaan akibat insiden tersebut? | Estimasi kerugian materi saat itu mencapai 1-3 Milyar Rupiah. Selain itu, reputasi kami sempat turun drastis, kehilangan subscribers, karena banyaknya keluhan |

(lanjutan)

| | |
|---|---|
| | pelanggan di media sosial dan juga omongan tetangga. |
| Sebenarnya apa sih pemicu utama serangan DDoS ini bisa terjadi, Mas? Apakah tim IT punya gambaran siapa yang melancarkan serangan? | penyebabnya ada dua sisi. Pertama dari penyerang, kebanyakan sih motifnya uang atau pemerasan, kayak Ransom DDoS. Tapi ada juga yang cuma iseng uji coba botnet atau malah persaingan bisnis (kompetitor). Kedua sisi korban, Firewall masih settingan standar, server langsung terekspos ke internet, dan kita nggak pasang rate-limit. Jadi pas diserang, trafik langsung lolos semua bikin router hang |
| Berdasarkan kejadian tersebut, bagian apa saja yang harus saya analisis dalam penelitian ini? | Mungkin dari kita ingin melihat analisis dari CPU dan Bandwidth/Traffic. Untuk metode nya saya sarankan menggunakan Firewall Filtering atau ACL, Rate Limit, dan konfigurasi di bagian port. |

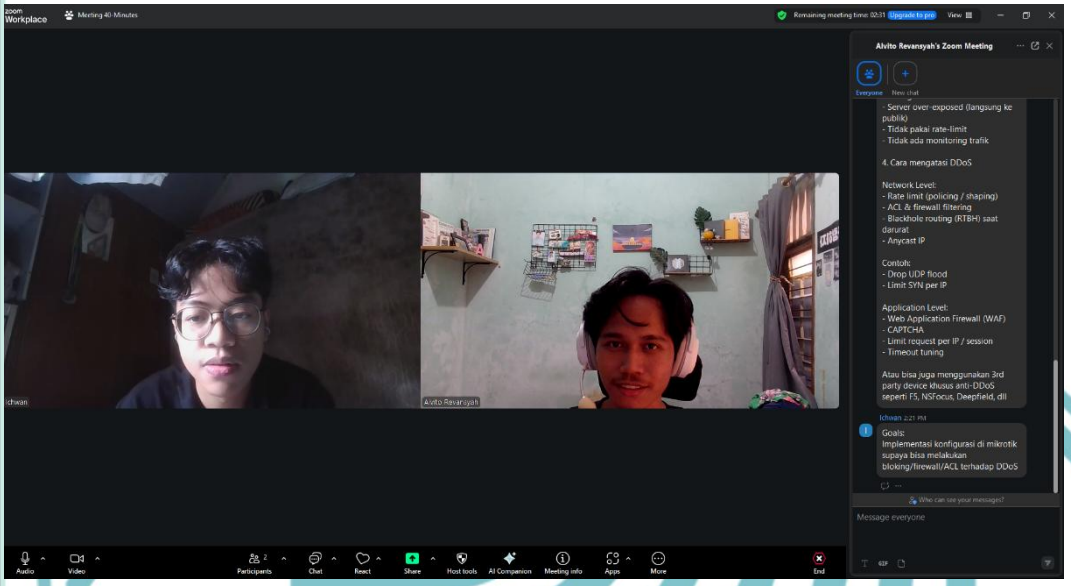
(lanjutan)

| | |
|---|---|
| Apakah penerapan sistem mitigasi serangan DDoS ini dilakukan langsung pada perangkat fisik di kantor PT XYZ, atau ada tahapan pengujian terlebih dahulu sebelum diimplementasikan? | Implementasi tidak langsung dilakukan di jaringan kantor. Pengujian dan simulasi dilakukan terlebih dahulu pada lingkungan virtual atau laboratorium. Setelah sistem dianggap sudah berjalan dengan baik dan stabil, barulah diterapkan pada jaringan operasional PT XYZ. |
| Apakah topologi asli jaringan PT XYZ dapat dijadikan dasar penyusunan topologi pengujian pada penelitian ini? | Ya. Topologi asli PT XYZ terdiri dari perangkat seperti Router IGW, Switch Core, Router PE, Router Colo, Router Dist CCR-2116, Switch Backbone, OLT, ONT, dan server pendukung. Dalam penelitian ini, alur tersebut dapat disederhanakan menjadi Kali Linux sebagai sumber trafik, MikroTik CHR upstream sebagai perantara/modem simulasi, MikroTik utama sebagai router target, dan Ubuntu Desktop sebagai perangkat admin. |
| Apakah di PT XYZ ada aturan khusus terkait penggunaan Firewall RAW pada MikroTik? | Tidak ada aturan yang terlalu kompleks. Firewall RAW dapat digunakan untuk drop awal trafik serangan seperti UDP Flood dan TCP SYN Flood dari interface publik, serta trafik dari IP attacker yang sudah diketahui. Namun, untuk akses port manajemen seperti Winbox/SSH, sebaiknya tidak langsung dibuang, tetapi divalidasi terlebih dahulu melalui port knocking. Rule RAW disarankan tetap sederhana agar tidak menambah beban |

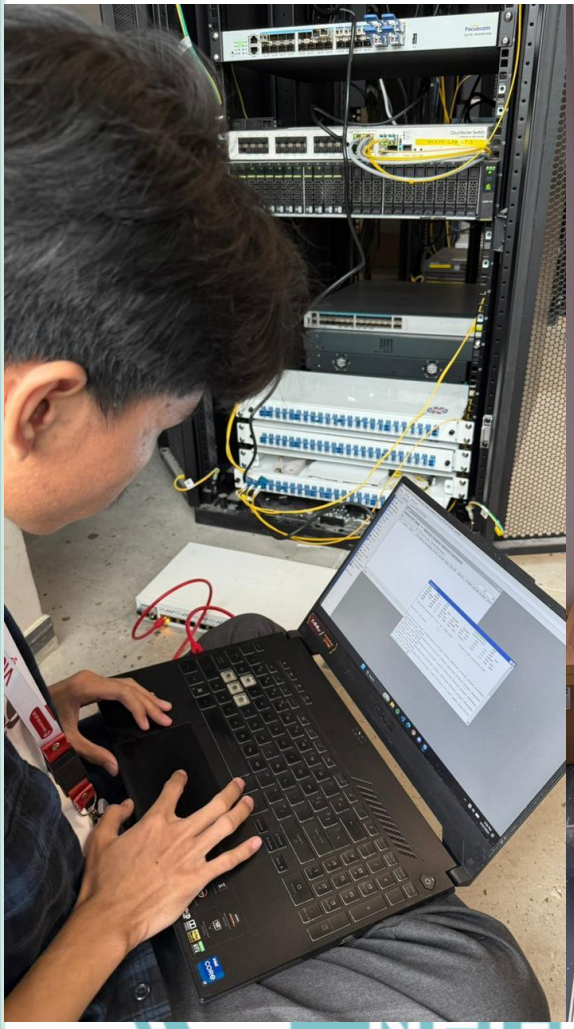
| | |
|---|---|
| | CPU dan tidak mengganggu trafik normal pelanggan. |
| Apakah ada aturan atau arahan terkait penerapan Rate Limiting pada MikroTik untuk mitigasi DDoS? | Untuk Rate Limiting, pembatasan bisa dilakukan pada trafik atau koneksi berlebih dari satu sumber IP. Fokusnya bisa pada koneksi baru TCP, trafik UDP berlebih, dan total koneksi dari satu IP. Namun, nilai batasnya tidak bisa dibuat sembarangan karena harus menyesuaikan trafik normal pelanggan agar tidak mengganggu layanan. |
| Apakah terdapat aturan khusus terkait Port Hardening pada MikroTik, seperti port/service yang dibuka, ditutup, atau dibatasi aksesnya? | Untuk MikroTik, layanan yang aktif adalah Winbox pada port 7090 dan Telnet pada port 2332. Layanan lain seperti API, API-SSL, FTP, SSH MikroTik, WWW, dan WWW-SSL tidak aktif. Untuk perangkat selain MikroTik, akses administrasi yang dibuka hanya SSH. |
| Apakah ada aturan khusus jika ingin menggunakan RTBH sebagai mitigasi DDoS di jaringan PT XYZ? | Ada. RTBH tidak bisa langsung diterapkan dari sisi internal saja karena perlu izin dan koordinasi dengan ISP/upstream, terutama jika menggunakan routing seperti BGP. Secara sederhana, RTBH bekerja dengan mengarahkan seluruh trafik yang menuju IP target ke jalur blackhole, sehingga trafik tersebut dibuang sebelum masuk ke jaringan utama. Namun, metode ini tidak membedakan trafik serangan dan trafik normal, sehingga semua trafik ke IP target |

| | |
|---|---|
| | ikut terbuang. Karena dampaknya cukup besar terhadap ketersediaan layanan, penerapan RTBH biasanya hanya dilakukan pada kondisi tertentu ketika serangan sudah sangat mengganggu jaringan. |
| Dari sisi mana trafik tidak normal dapat masuk pada topologi asli PT XYZ? | Trafik tidak normal dapat masuk melalui sisi perangkat pelanggan seperti ONT, kemudian melewati jalur jaringan sampai mencapai Router Dist CCR-2116. Oleh karena itu, Router Dist CCR-2116 menjadi perangkat yang menerima dampak utama dari peningkatan trafik. |
| Apakah pengujian akhir boleh dilakukan pada jaringan operasional aktif PT XYZ? | Tidak. Pengujian tidak dilakukan pada jaringan operasional aktif agar tidak mengganggu layanan pelanggan. Konfigurasi divalidasi terlebih dahulu di lingkungan laboratorium, kemudian pengujian akhir dilakukan pada perangkat MikroTik fisik milik PT XYZ di jaringan uji terpisah. |

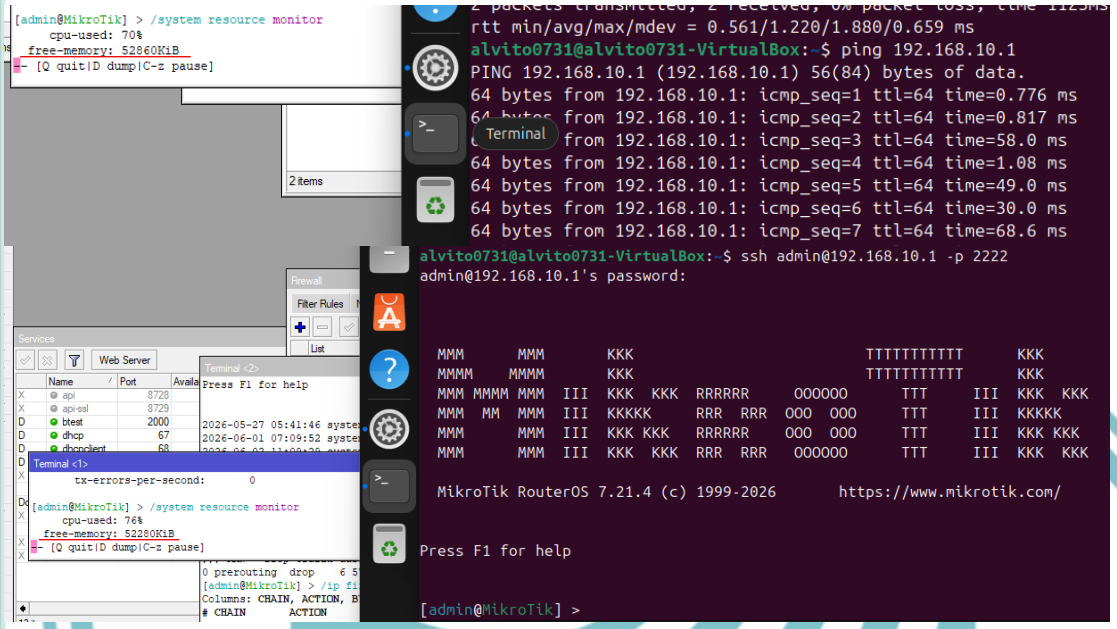
Lampiran 2 – Dokumentasi Wawancara



Lampiran 3 – Implementasi Sistem di Lingkungan Perusahaan



Lampiran 4 – Pengujian akses Admin pada saat serangan berjalan



Lampiran 5 – Counter Rate Limiting bertambah

```
;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos    return                      6 280       157
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos    drop                1 128 200    28 205
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos    return                     37 044     1 323
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos    drop                1 727 964    61 713
;;; Rate Limit - TCP SYN masih dalam batas
10 rate-limit-ddos    return                     26 280       657
;;; Rate Limit - Drop TCP SYN berlebih
11 rate-limit-ddos    drop                5 416 920   135 423
;;; Rate Limit - UDP masih dalam batas
12 rate-limit-ddos    return                     52 864     1 888
;;; Rate Limit - Drop UDP berlebih
13 rate-limit-ddos    drop                2 381 372    85 049
```