# ANALISIS INTRUTION DETECTION SYSTEM MENGGUNAKAN SNORT TERHADAP SERANGAN MHDDOS BERBASIS SDN

## SKRIPSI

**MUHAMMAD NAUFAL FAUZI**

**2007422021**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**

**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**

**POLITEKNIK NEGERI JAKARTA**

**2024**

# ANALISIS INTRUTION DETECTION SYSTEM MENGGUNAKAN SNORT TERHADAP SERANGAN MHDDOS BERBASIS SDN

## SKRIPSI

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

**MUHAMMAD NAUFAL FAUZI**
**2007422021**

**PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN**
**JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER**
**POLITEKNIK NEGERI JAKARTA2024**

# SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan dibawah ini:

| | | |
|---|---|---|
| Nama | : | Muhammad Naufal Fauzi |
| NIM | : | 2007422021 |
| Jurusan/Program Studi | : | Teknik Informatika dan Komputer / Teknik Multimedia dan Jaringan |
| Judul Skripsi | : | ANALISIS INTRUSION DETECTION SYSEM MENGGUNAKAN SNORT TERHADAP SERANGAN MHDDOS BERBASIS SDN |

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, 30 Juli 2025


Muhammad Naufal Fauzi

NIM 2007422021

# LEMBAR PENGESAHAN

Skripsi diajukan oleh:

| | | |
|---|---|---|
| Nama | : | Muhammad Naufal Fauzi |
| NIM | : | 20074220021 |
| Program Studi | : | Teknik Multimedia dan Jaringan |
| Judul Skripsi | : | ANALISIS INTRUCTION DETECTION SYSTEM MENGGUNAKAN SNORT TERHADAP SERANGAN MHDDOS BERBASIS SDN |

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Jumat

Tanggal 17 , Bulan Januari, Tahun 2025 dan dinyatakan **LULUS.**

| Disahkan Oleh | | Tanda Tangan |
|---|---|---|
| Pembimbing I | : Ayu Rosyida Zain, S.ST, M.T | ( ) |
| Penguji I | : Dr. Prihatin Oktivasari, S.Si., M.Si | ( ) |
| Penguji II | : Defiana Arnaldy, S.Tp., M.Si.. | ( ) |
| Penguji III | : Fachroni Arbi Murad, S.Kom., M.Kom | ( ) |

Mengetahui :

Ketua Jurusan Teknik Informatika dan Komputer

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

# KATA PENGANTAR

Puji syukur saya ucapkan kepada Allah SWT yang telah memberikan berkah dan Rahmat-Nya kepada saya sehingga saya dapat menyelesaikan skripsi ini yang ditulis sebagai syarat kelulusan di Politeknik Negeri Jakarta. Penulisan skripsi ini tentunya melibatkan banyak pihak yang membantu dalam proses penulisannya. Oleh karena itu, penulis ingin mengucapkan terimakasih yang sebesar-besarnya kepada:

1. Ketua jurusan dan seluruh Dosen serta staf jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta yang telah memberikan ilmu yang sangat bermanfaat kepada penulis;
2. Ibu Ayu Rosyida Zain, M.T. yang telah menyediakan waktu, tenaga dan pikiran selama membimbing penulis sehingga penulis berhasil menyusun skripsi ini dengan baik dan benar;
3. Orang tua dan keluarga yang senantiasa mendoakan kelancaran proses skripsi penulis dan memberikan dukungan yang sangat berarti kepada penulis sehingga penulis memiliki semangat yang besar dalam mengerjakan skripsi;
4. Teman-teman perkopian dan perpokeran ada Anum, Aris, Apis, ,Atip dan Rean yang sudah memberikan canda tawa dan semangat untuk penulis dan juga walid karena sudah banyak mengajar dan memberitahu materi-materi yang tidak saya mengerti.
5. Penulis sendiri, karena tidak menyerah dalam menempuh pendidikan ini dan berhasil menyusun skripsi dengan baik.

Penulis berharap skripsi ini dapat dengan mudah dipahami oleh pembaca agar menjadi ilmu yang bermanfaat. Sebagai manusia tentu tidak ada yang sempurna, begitu pula dengan skripsi yang ditulis ini. Dengan begitu, penulis akan menerima kritik dan saran dengan senang hati agar kedepannya dapat menulis dengan lebih baik lagi

# SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

Nama : Muhammad Naufal Fauzi

NIM : 2007422021

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: ANALISIS INTRUSION DETECTION SYSEM MENGGUNAKAN SNORT TERHADAP SERANGAN MHDDOS BERBASIS SDN

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Politeknik Negeri Jakarta Berhak menyimpan, mengalih mediakan/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, 30 Juli 2025


Muhammad Naufal Fauzi

NIM 2007422021

**ANALISIS INTRUSION DETECTION SYSEM MENGGUNAKAN SNORT TERHADAP SERANGAN MHDDOS BERBASIS SDN**

***Abstrak***

Perkembangan pesat teknologi informasi telah meningkatkan ketergantungan pada jaringan komputer, yang secara langsung memperbesar risiko serangan siber, khususnya Distributed Denial of Service (DDoS). Serangan ini dapat menyebabkan layanan tidak tersedia dengan membanjiri jaringan atau server dengan lalu lintas yang berlebihan. Penelitian ini mengusulkan implementasi sistem keamanan berbasis Software Defined Networking (SDN) untuk mendeteksi dan merespons serangan DDoS yang diluncurkan menggunakan alat MHDDOS. Simulasi dilakukan dalam lingkungan Mininet dengan Ryu sebagai kontroler SDN, Snort sebagai sistem deteksi intrusi (IDS), dan Wireshark untuk analisis lalu lintas. Hasil penelitian menunjukkan bahwa sistem yang diimplementasikan berhasil mendeteksi ancaman DoS, terutama jenis serangan SYN Flood, dengan tingkat keberhasilan yang baik. Sistem dapat mendeteksi anomali lalu lintas secara efektif dan merespons ancaman secara real-time. Keberhasilan ini menunjukkan bahwa pendekatan SDN menawarkan solusi yang lebih fleksibel dan efisien dalam menghadapi ancaman keamanan jaringan yang dinamis dan berkembang, khususnya serangan DDoS. Sistem ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan jaringan berbasis SDN.

Kata kunci: DDoS, Intrusion Detection System, Mininet, SDN, Snort

***DAFTAR ISI***

DAFTAR GAMBAR

DAFTAR TABEL

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah cara hidup, bekerja, dan berinteraksi. Di tengah transformasi digital yang masif, jaringan komputer menjadi tulang punggung bagi banyak aktivitas sehari-hari, dari transaksi bisnis hingga komunikasi pribadi. Namun, seiring dengan peningkatan ketergantungan pada jaringan ini, ancaman terhadap keamanan jaringan juga meningkat, menciptakan kebutuhan mendesak untuk solusi keamanan yang lebih canggih dan adaptif.

Salah satu ancaman terbesar yang dihadapi oleh jaringan adalah serangan Distributed Denial of Service (DDoS). Serangan DDoS adalah upaya untuk membuat layanan jaringan tidak tersedia dengan membanjiri jaringan atau server dengan lalu lintas internet yang luar biasa besar, sehingga mengganggu fungsinya. Alat seperti MHDDOS memungkinkan penyerang untuk meluncurkan serangan DDoS dengan berbagai metode yang efektif dalam melumpuhkan infrastruktur jaringan hanya dalam hitungan menit. (Badotra & Panda, 2020)

Tradisionalnya, pendekatan keamanan jaringan cenderung bersifat statis dan reaktif, yang seringkali tidak memadai untuk mengatasi ancaman yang berkembang secara dinamis seperti DDoS. Untuk itu, Software Defined Networking (SDN) muncul sebagai paradigma baru yang menawarkan solusi lebih fleksibel dan terpusat dalam pengelolaan jaringan. SDN memisahkan kontrol jaringan dari perangkat kerasnya, memungkinkan pengelola jaringan untuk merespons ancaman keamanan dengan cara yang lebih dinamis dan efisien. Ini memberi pengelola kemampuan untuk mendeteksi dan memitigasi serangan DDoS secara real-time, yang merupakan langkah maju dari pendekatan tradisional. (Karan et al., 2018)

Penelitian ini berfokus pada implementasi sistem keamanan jaringan berbasis SDN yang dirancang untuk mendeteksi dan merespons serangan DDoS yang dilakukan dengan alat seperti MHDDOS. Dalam pengaturan ini, Mininet digunakan untuk mensimulasikan topologi jaringan, yang memungkinkan uji coba dalam lingkungan

yang terkendali dan realistis. Ryu, sebagai kontroler SDN, memainkan peran sentral dalam mengatur dan mengelola lalu lintas jaringan, sementara Snort digunakan sebagai sistem deteksi intrusi (Intrusion Detection System, IDS) untuk mengidentifikasi ancaman potensial. Dengan adanya Snort, sistem ini dapat mengenali pola serangan berdasarkan tanda tangan yang diketahui dan memberikan respons cepat untuk memitigasi dampak serangan. Penggunaan Wireshark sebagai alat pemantauan paket lebih lanjut memungkinkan analisis mendalam terhadap lalu lintas jaringan yang dicurigai, yang memperkuat kemampuan sistem dalam mendeteksi dan merespons ancaman. (Wang & Li, 2022)

Di era di mana jaringan komputer menjadi semakin kompleks dan vital, keamanan jaringan yang adaptif dan responsif menjadi kunci untuk memastikan kontinuitas layanan. Dengan mengadopsi arsitektur SDN dan alat-alat terkait seperti Ryu, Snort, dan Mininet, penelitian ini berkontribusi dalam menyediakan solusi yang lebih kuat dan efisien untuk mengatasi ancaman DDoS yang terus berkembang. Sistem keamanan berbasis SDN yang diusulkan diharapkan dapat menawarkan perlindungan yang lebih baik, meningkatkan keandalan infrastruktur jaringan, dan menjamin kontinuitas layanan di tengah lanskap ancaman yang semakin canggih. (Kareem et al., 2023)

## 1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, perumusan masalah dari penelitian adalah :

1. Bagaimana mengimplementasikan intrusion detection system pada SDN untuk mendeteksi serangan DDoS?
2. Bagaimana kinerja intrusion detection system pada SDN dalam mengidentifikasi dan menganalisis pola serangan DDoS?

## 1.3 Batasan Masalah

Adapun batasan masalah yang ditentukan dalam penelitian ini adalah :

1. Pada penelitian ini mengimplementasikan IDS menggunakan snort untuk mendeteksi serangan DDOS
2. Tools Wireshark yang digunakan dalam menganalisis serangan DDOS

menggunakan MHDDOS

## 1.4 Tujuan dan Manfaat

Adapun tujuan dan manfaat dari dilakukannya pengembangan ini adalah sebagai berikut:

### 1.4.1 Tujuan

Adapun tujuan dari dilakukannya pengembangan ini adalah sebagai berikut:

1. Menerapkan dan menguji sistem keamanan jaringan berbasis Software Defined Networking (SDN) yang efektif dalam mendeteksi dan merespons serangan Distributed Denial of Service (DDoS) yang dilancarkan menggunakan alat MHDDOS.
2. Menganalisis efektivitas sistem keamanan yang diimplementasikan dalam mendeteksi dan merespons serangan DDoS secara real-time dalam lingkungan simulasi berbasis Mininet.

### 1.4.2 Manfaat

Adapun manfaat dari dilakukannya pengembangan ini adalah sebagai berikut:

1. Hasil penelitian ini diharapkan dapat memberikan solusi yang lebih efektif untuk meningkatkan keamanan jaringan terhadap serangan DDoS, khususnya dalam konteks infrastruktur berbasis SDN.
2. Penelitian ini dapat menjadi referensi bagi pengelola jaringan dan peneliti lain dalam mengimplementasikan dan mengoptimalkan penggunaan SDN untuk keamanan jaringan, terutama dalam konteks perlindungan terhadap serangan DDoS.
3. Memberikan panduan praktis untuk melakukan simulasi dan evaluasi sistem keamanan jaringan dalam lingkungan yang dikontrol, memungkinkan pengujian berbagai skenario ancaman dan respons keamanan.

## 1.5 Sistematika Penulisan

Sistematika penulisan dalam penyusunan laporan dari penelitian ini adalah sebagai berikut:

a. BAB I PENDAHULUAN

Berisi latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat, serta sistematika penulisan.

b. BAB II TINJAUAN PUSTAKA

Berisi uraian pembahasan mengenai teori yang mendukung dan membantu penelitian

c. BAB III METODOLOGI PENELITIAN

Berisi metode pembahasan metode penelitian, tahapan penelitian, objek penelitian, teknik pengumpulan data, dan jadwal penelitian.

d. BAB IV PEMBAHASAN

Berisi pembahasan proses serta hasil kegiatan selama penelitian yang dilakukan sesuai dengan tahapan dan metode yang telah ditentukan sebelumnya.

e. BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran dari penelitian yang telah dilaksanakan

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Setelah melakukan serangkaian pengujian terhadap sistem keamanan jaringan berbasis SDN untuk mendeteksi dan merespons serangan Denial of Service (DoS) yang dilakukan dengan tool MHDDOS, beberapa kesimpulan dapat diambil. Pengujian dilakukan dalam lingkungan Mininet, dengan menggunakan Ryu sebagai kontroler SDN, Snort sebagai IDS, dan Wireshark untuk analisis lalu lintas. Sistem yang dikembangkan terbukti efektif dalam mendeteksi ancaman DoS, terutama serangan SYN Flood. Variasi ancaman (threat) yang digunakan, mulai dari 10 hingga 1000 paket dalam satu menit, memberikan gambaran yang jelas mengenai efektivitas sistem dalam menghadapi intensitas serangan yang berbeda-beda. Hasil pengujian menunjukkan bahwa sistem mampu mendeteksi anomali lalu lintas, khususnya pola SYN Flood yang merupakan ciri khas serangan DoS. Waktu respons sistem bervariasi tergantung pada jumlah threat yang dikirimkan, dengan hasil yang semakin cepat ketika ancaman meningkat. Secara keseluruhan, sistem mencapai tingkat keberhasilan yang baik dalam mendeteksi dan merespons ancaman, sehingga dapat dikatakan bahwa sistem ini mampu memberikan perlindungan yang memadai terhadap serangan DoS.

## 5.2 Saran

Saran yang dapat penulis berikan terkait penulisan ini adalah Untuk pengembangan lebih lanjut, beberapa saran dapat dipertimbangkan agar sistem ini dapat lebih optimal dalam menghadapi berbagai jenis serangan dan kondisi jaringan yang berbeda Berikut saran :

1. Variasi Serangan yang Lebih Luas:

Uji sistem terhadap berbagai jenis serangan selain SYN Flood, seperti UDP Flood atau DNS Amplification, untuk mengukur kemampuan sistem dalam mendeteksi dan merespons beragam ancaman di jaringan.

2. Perlindungan Terhadap Serangan yang Lebih Baik:

Tambahkan mekanisme perlindungan lebih lanjut seperti rate limiting atau blacklisting otomatis untuk memblokir IP penyerang setelah deteksi ancaman. Ini

akan meningkatkan kemampuan sistem dalam memitigasi dampak serangan secara lebih efektif.

3. Optimasi Respons Sistem:

Lakukan analisis terhadap waktu respons sistem dan optimasi agar sistem dapat memberikan respons lebih cepat, terutama dalam menangani serangan berskala besar.

# DAFTAR PUSTAKA

Badotra, S., & Panda, S., 2020. SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking. *Cluster Computing*, 24, pp. 501 – 513

V., K., G., N., & Hiremath, P., 2018. Detection of DDoS Attacks in Software Defined Networks. 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), pp. 265-270.

Wang, D., & Li, S., 2022. Automated DDoS Attack Mitigation for Software Defined Network. 2022 IEEE 16th International Conference on Anti-counterfeiting, Security, and Identification (ASID), pp. 100-104.

Kareem, M., Jasim, M., Hussein, H., & Ibrahim, K., 2023. Performance evaluation of RYU controller under distributed denial of service attacks. *Indonesian Journal of Electrical Engineering and Computer Science.*

Abhishta, A. *et al.* (2020) 'Why would we get attacked? An analysis of attacker's aims behind DDoS attacks', *Journal of Wireless Mobile Networks, Ubiquitous Computing, andDependable Applications*, 11(2), pp. 3–22. Available at: https://doi.org/10.22667/JOWUA.2020.06.30.003.

Akhir, T. *et al.* (no date) *SERANGAN DDOS PADA SOFTWARE DEFINED NETWORK*.

Badotra, S. and Panda, S.N. (2019) 'A review on software-defined networking enabled iot cloud computing', *IIUM Engineering Journal*, 20(2), pp. 105–126. Available at: https://doi.org/10.31436/iiumej.v20i2.1130.

Ekawijana, A., Bakhrun, A. and Kurniawan, T. (2024) 'JURNAL MEDIA INFORMATIKA BUDIDARMA Deteksi Serangan DDOS Pada Jaringan SDN dengan Metode Random Forest'. Available at: https://doi.org/10.30865/mib.v8i1.6928.

Fortinet (2024) *What is a DDoS Attack? DDoS Meaning, Definition & Types | Fortinet.* Available at:

https://www.fortinet.com/it/resources/cyberglossary/ddos-attack (Accessed:22 February 2024).

GitHub (2023) *GitHub - MatrixTM/MHDDoS: Best DDoS Attack Script Python3, (Cyber / DDos) Attack With 56 Methods*. Available at: https://github.com/MatrixTM/MHDDoS(Accessed: 24 February 2024).

Loftus, T. (2022) *MHDDoS - A DDoS Attack Script With Over 50 Different Methods - Latest Hacking News | Cyber Security News, Hacking Tools and Penetration Testing Courses.* Available at: https://latesthackingnews.com/2022/08/05/mhddos-a-ddos-attack- script-with-over-50-different-methods/ (Accessed: 23 February 2024).

Mamuriyah, N., Prasetyo, S.E. and Sijabat, A.O. (2024) 'Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi', *Jurnal Teknologi Dan Sistem Informasi Bisnis*, 6(1), pp. 162–167. Available at: https://doi.org/10.47233/jteksis.v6i1.1124.

Rana, D.S., Dhondiyal, S.A. and Chamoli, S.K. (2019) 'Software Defined Networking (SDN) Challenges, issues and Solution', *International Journal of Computer Sciences andEngineering*, 7(1), pp. 884–889. Available at: https://doi.org/10.26438/ijcse/v7i1.884889.

Siler, E.M. (2024) *What is an OpenDaylight Controller? — SDxCentral.com.* Available at: https://www.sdxcentral.com/networking/sdn/definitions/what-the- definition-of- software-defined-networking-sdn/what-is-sdn-controller/openflow- controller/opendaylight-controller.

WHA Muraga (2020) *CHAPTER TWO LITERATURE REVIEW 2.1 Introduction*. Wright, G. (2023) *What is OpenFlow and how does it work? | Definition from TechTarget.* Available at: https://www.techtarget.com/whatis/definition/OpenFlow.

Zola, A. and Scarpati, J. (2023) *What is Cisco IOS software, and how does it work? | Definition from TechTarget.* Available at: https://www.techtarget.com/searchnetworking/definition/Cisco-IOS-Cisco-Internetwork- Operating-System

# DAFTAR RIWAYAT HIDUP PENULIS

Muhammad Naufal Fauzi, Lahir di Jakarta, 22 November 1999. Sudah menempuh Pendidikan Sekolah Dasar SDN Negeri Magersari dan SD Islam Sabilillah (2006-2012), Sekolah Menengah Pertama SMP Negeri 2 Sidoarjo (2012-2015), Sekolah Menengah Atas SMA Negeri 1 Gedangan, SMA Negeri 35 Jakarta (2015-2018), Pendidikan professi CEP-CCIT Fakultas Teknik Universitas Indoenesia (2019-2021) konsentrasi Network Administrator Professional dan Perguruan Tinggi Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer program studi Teknik Multimedia dan Jaringan konsentrasi Sistem Keamanan Informasi.