TUGAS AKHIR

MENDETEKSI *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA *ROUTER* MENGGUNAKAN *IP FIREWALL*

Achmad Khairul Anam
2110651075

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2025

TUGAS AKHIR

MENDETEKSI *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA *ROUTER* MENGGUNAKAN *IP FIREWALL*

Disusun untuk Memenuhi Persyaratan Guna Meraih Gelar Sarjana Komputer
Teknik Informatika Universitas Muhammadiyah Jember

Achmad Khairul Anam
2110651075

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2025

HALAMAN PERSETUJUAN SIDANG TUGAS AKHIR

MENDETEKSI *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA *ROUTER* MENGGUNAKAN IP *FIREWALL*

Oleh:
Achmad Khairul Anam
2110651075

Telah disetujui Laporan Tugas Akhir ini untuk dianjurkan pada Sidang Tugas Akhir sebagai salah satu syarat kelulusan dan mendapatkan gelar Sarjana Komputer
(S.Kom)
di
Universitas Muhammadiyah Jember

Disetujui oleh,

Pembimbing I	Pembimbing II
Taufiq Timur W., S.Kom., M.Kom	**Miftahur Rahman, S.Kom., M.Kom**
NIDN. 0705078006	**NIDN. 0724039201**

HALAMAN PENGESAHAN

MENDETEKSI *DISTRIBUTED DENIAL OF SERVICE* (DDoS) PADA *ROUTER* MENGGUNAKAN IP *FIREWALL*

Oleh:
Achmad Khairul Anam
2110651075

Telah mempertanggungjawabkan Laporan Tugas Akhir pada sidang Tugas Akhir
Tanggal 04 Bulan Oktober Tahun 2025 sebagai salah satu syarat kelulusan dan
Mendapatkan gelar Sarjana Komputer (S.Kom)
di
Universitas Muhammadiyah Jember

Disetujui Oleh,

Dosen Penguji Penguji I	Dosen Pembimbing Pembimbing I
Daryanto, S.Kom., M.Kom **NIDN. 0707077203**	**Taufiq Timur W., S.Kom., M.Kom** **NIDN. 0705078006**
Penguji II	**Pembimbing II**
Hardian Oktavianto, S.Si., M.Kom **NIDN. 0722108105**	**Miftahur Rahman S.Kom., M.Kom** **NIDN. 0724039201**

Mengesahkan,
Dekan Fakultas Teknik

Dr. Ir. Muhtar, S.T., M.T., IPM
NIDN. 0010067301

Mengetahui,
Ketua
Program Studi Teknik Informatika

Rosita Yanuarti, S.Kom., M.Cs
NIDN. 0629018601

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama	:	ACHMAD KHAIRUL ANAM
NIM	:	2110651075
Program Studi	:	Teknik Informatika
Judul Tugas Akhir	:	Mendeteksi Distributed Denial of Service pada Router Menggunakan IP Firewall

Dengan ini menyatakan bahwa karya ilmiah yang saya susun adalah murni hasil pemikiran, penelitian, dan penyusunan saya sendiri. Segala sumber informasi yang berasal atau dikutip dari karya orang lain, baik berupa publikasi, artikel, buku, maupun sumber lainnya, telah disebutkan dengan jelas di dalam daftar pustaka sesuai dengan kaidah penulisan ilmiah.

Saya menyadari bahwa dalam proses penyusunan Tugas Akhir ini, saya memanfaatkan bantuan teknologi kecerdasan buatan (AI) seperti *ChatGPT/Grammarly/Alat AI lain* hanya sebatas untuk:

1. Membantu dalam penyusunan tata bahasa, parafrasa, atau perbaikan redaksi.
2. Memberikan inspirasi ide awal atau kerangka berpikir, yang selanjutnya saya kembangkan secara mandiri.
3. Membantu dalam pengecekan konsistensi format, ejaan, dan tata tulis.

Saya menegaskan bahwa tidak ada bagian dari karya ilmiah ini yang seluruhnya dibuat oleh AI tanpa keterlibatan pemikiran kritis saya sendiri. Tanggung jawab penuh atas isi, keaslian, dan kebenaran karya ilmiah ini ada pada diri saya.

Apabila di kemudian hari terbukti bahwa pernyataan ini tidak benar, maka saya bersedia menerima segala konsekuensi sesuai dengan peraturan yang berlaku di Universitas Muhammadiyah Jember.

Jember, 04 Oktober 2025

Menyatakan,

Achmad Khairul Anam

2110651075

HALAMAN PERSEMBAHAN

Puji syukur penulis panjatkan ke hadirat Allah SWT karena atas berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan Tugas Akhir ini dengan baik. Shalawat serta salam semoga senantiasa tercurahkan kepada junjungan kita, Nabi Muhammad SAW, beserta keluarga, sahabat, dan umatnya hingga akhir zaman. Dalam kesempatan ini, penulis mendapatkan banyak bimbingan, dorongan, serta bantuan dari berbagai pihak, sehingga penyusunan Tugas Akhir ini dapat terselesaikan dengan baik. Terselesainya Laporan Tugas Akhir ini, penulis mempersembahkan dan banyak terima kasih kepada:

1. Allah SWT, atas segala limpahan rahmat dan pertolongan-Nya. Tugas akhir ini dapat terselesaikan berkat izin dan kehendak-Nya.
2. Kedua orang tua tercinta, atas kasih sayang, kerja keras, doa, dan pengorbanan yang tiada henti.
3. Dr. Ir. Muhtar, S.T., M.T., IPM., selaku Dekan Fakultas Teknik, Universitas Muhammadiyah Jember.
4. Ibu Rosita Yanuarti, M.Cs., selaku Ketua Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember.
5. Bapak Taufiq Timur W., S.Kom., M.Kom., selaku Dosen Pembimbing I yang dengan penuh kesabaran dan ketelitian telah memberikan arahan, bimbingan, serta motivasi kepada penulis.
6. Bapak Miftahur Rahman, S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah banyak memberikan masukan, saran, dan bimbingan yang sangat berarti bagi penulis.
7. Teman-teman seperjuangan rizal, ageng, hesti, yokhe, yang senantiasa memberikan semangat, bantuan, serta kebersamaan dalam proses penyusunan skripsi ini.

MOTTO

"Sesungguhnya bersama kesulitan ada kemudahan." (QS. Al-Insyirah: 6)

DAFTAR ISI

HALAMAN PERSETUJUAN SIDANG TUGAS AKHIR ii
HALAMAN PENGESAHAN iii
LEMBAR PERNYATAAN iv
ABSTRAK v
ABSTRACT vi
HALAMAN PERSEMBAHAN vii
MOTTO viii
KATA PENGANTAR ix
DAFTAR ISI x
DAFTAR GAMBAR xii
DAFTAR TABEL xiii
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumus Masalah 3
1.3 Tujuan Penelitian 3
1.4 Manfaat Penelitian 3
1.5 Batasan Penelitian 4
BAB II TINJAUAN PUSTAKA 5
2.1 Studi Literatur 5
2.2 Trafik Normal 7
2.3 *Distributed Denial of Service* (DDoS) 8
2.2.1 TCP SYN-*Flooding* 9
2.2.2 UDP-*Flooding* 9
2.2.3 ICMP-*Flooding* 10
2.2.4 DNS-*Flooding* 10
2.4 *Hping3* 11
2.5 Topologi Jaringan 12
2.6 *Router* 12
2.7 *IP Firewall* 13
2.8 Deteksi Serangan *Distributed Denial of Service* (*DDoS*) 13
BAB III METODE PENELITIAN 14
3.1 Tahapan Penelitian 14
3.2 Pemodelan Topologi 15
3.3 Konfigurasi *Router* 16
3.4 Simulasi Serangan *Distributed Denial of Service* (DDoS) 21
3.5 *Monitoring* dan Deteksi 24
3.6 Analisis Data 24
3.7 Evaluasi Serangan 26
3.8 Implementasi IP *Firewall* 28
BAB IV HASIL DAN PEMBAHASAN 31
4.1 Analisis Trafik Normal Jaringan 31
4.1.1 Hasil Pemantauan Trafik Fitur *Tools Torch* 31
4.1.2 Hasil Trafik *Interface* Statistik Ether3 32
4.1.3 Hasil Pemantauan Beban Penggunaan CPU 34
4.1.4 Monitoring dari Fitur System Resources 35
4.2 Hasil Simulasi Serangan 35

4.2.1 Hasil Pemantauan *Torch* saat Terjadi Serangan 36
4.2.2 Pemantauan Trafik *Interface* Ether3 Saat Terjadi Serangan 37
4.2.3 Hasil dari Fitur *Profile* dan System Resources 39
4.2.4 Hasil Analisis 40
4.3 Tindakan *Mitigasi* dan Pemblokiran IP 45
4.4 Perbandingan Kondisi Sebelum dan Sesudah Mitigasi 49
4.4.1 Kondisi Sebelum Mitigasi 49
4.4.2 Kondisi Setelah Mitigasi 50
4.4.3 Evaluasi Efektivitas Mitigasi 52
BAB V KESIMPULAN DAN SARAN 54
5.1 Kesimpulan 54
5.2 Saran 54
DAFTAR PUSTAKA 56
LAMPIRAN 58
Lampiran 1 : Komponen Yang di gunakan 58
Lampiran 2 : Konfigurasi Topologi jaringan 58
Lampiran 3 : pengecekan trafik normal 60
Lampiran 4 : Simulasi serangan 61
Lampiran 5 : Konfigurasi IP *Firewall* 62
Lampiran 6 : Link Youtobe 62

DAFTAR GAMBAR

Gambar 3. 1 Tahapan Penelitian 14
Gambar 3. 2 Topologi Jaringan Mikrotik 15
Gambar3. 3 Konfigurasi WLAN 17
Gambar3. 4 Konfigurasi DHCP Client 17
Gambar3. 5 IP Address 18
Gambar3. 6 Konfigurasi DNS 18
Gambar3. 7 Konfigurasi NAT 19
Gambar3. 8 Konfigurasi DHCP Server 19
Gambar3. 9 Route list 20
Gambar 3. 10 Simulasi Serangan Pada Router 21
Gambar3. 11 Lonjakan CPU 26
Gambar 3. 12 Menganalisis IP Firewall (Filter-Rules) 29
Gambar 3. 13 Mitigasi Menggunakan IP Firewall 30
Gambar 4. 1 Hasil Tools Torch 31
Gambar 4. 2 Hasil Trafik Interface Statistik Ether3 33
Gambar 4. 3 Tools Profile 34
Gambar 4. 4 System Resources 35
Gambar 4. 5 Hasil Tools Torch saat terjadi serangan 36
Gambar 4. 6 Hasil Traffik Interface ether3 38
Gambar 4. 7 Hasil Fitur Profile 39
Gambar 4. 8 Hasil Fitur System Resources 40
Gambar 4. 9 Hasil pemantauan Torch saat terjadi serangan TCP SYN Flood. 46
Gambar 4. 10 Hasil pemantauan Torch saat terjadi serangan UDP SYN Flood. 47
Gambar 4. 11 Hasil pemantauan Torch saat terjadi serangan ICMP Flood 47
Gambar 4. 12 Hasil pemantauan Torch saat terjadi serangan DNS SYN Flood. 48
Gambar 4. 13 Konfigurasi IP Firewall 49
Gambar 4. 14 Konfigurasi Firewal yang Mengarah ke Laptop 49
Gambar 4. 15 Hasil fitur Profile Sebelum Mitigasi 50
Gambar 4. 16 Hasil Resource Sebelum Mitigasi 50
Gambar 4. 17 Hasil Resources setelah mitigasi 51
Gambar 4. 18 Hasil Trafik setelah mitigasi 51

DAFTAR TABEL

Tabel 2. 1 Studi Literatur 5
Tabel 3. 1 Teknik Serangan 27
Tabel 4. 1 Hasil Simulasi 41
Tabel 4. 2 Hasil Parameter Pengujian 44
Tabel 4. 3 Parameter Mitigasi 52

UNIVERSITAS MUHAMMADIYAH JEMBER