

**ANALISIS PERBANDINGAN METODE FAIL2BAN DAN
MODSECURITY DALAM EFEKTIVITAS MITIGASI
SERANGAN DDOS PADA WEB SERVER PERSONAL**

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh
ILHAMKA HALIM KUSUMA
22.11.4788

Kepada
**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2026**

**ANALISIS PERBANDINGAN METODE FAIL2BAN DAN
MODSECURITY DALAM EFEKTIVITAS MITIGASI
SERANGAN DDOS PADA WEB SERVER PERSONAL**

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Informatika



disusun oleh

ILHAMKA HALIM KUSUMA

22.11.4788

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

HALAMAN PERSETUJUAN

SKRIPSI

**ANALISIS PERBANDINGAN METODE FAIL2BAN DAN
MODSECURITY DALAM EFEKTIVITAS MITIGASI SERANGAN DDOS
PADA *WEB SERVER* PERSONAL**

yang disusun dan diajukan oleh

Ilhamka Halim Kusuma

22.11.4788

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 20 Mei 2026

Dosen Pembimbing,



Subektiningsih, S.Kom., M.Kom.
NIK. 190302413

HALAMAN PENGESAHAN

SKRIPSI

**ANALISIS PERBANDINGAN METODE FAIL2BAN DAN
MODSECURITY DALAM EFEKTIVITAS MITIGASI SERANGAN DDOS
PADA WEB SERVER PERSONAL**

yang disusun dan diajukan oleh

Ilhamka Halim Kusuma

22.11.4788

Telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Mei 2026

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ike Verawati, S.Kom., M.Kom.
NIK. 190302237

Uyock Anggoro Saputro, S.Kom., M.Kom.
NIK. 190302419

Subektiningsih, S.Kom., M.Kom.
NIK. 190302413

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Mei 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ilhamka Halim Kusuma
NIM : 22.11.4788

Menyatakan bahwa Skripsi dengan judul berikut:

Analisis Perbandingan Metode Fail2ban dan ModSecurity dalam Efektivitas Mitigasi Serangan DDoS pada Web server Personal

Dosen Pembimbing : Subektiningsih, S.Kom., M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 20 Mei 2026

Yang Menyatakan,



Ilhamka Halim Kusuma

HALAMAN PERSEMBAHAN

Sembah sujud serta syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi ini dengan baik. Skripsi ini penulis persembahkan kepada:

1. Kedua orang tua tercinta, yang senantiasa memberikan doa, kasih sayang, dukungan moral, serta pengorbanan yang tak terhingga dalam setiap langkah perjalanan hidup dan pendidikan penulis.
2. Keluarga besar, yang selalu memberikan semangat, motivasi, dan dukungan kepada penulis selama menempuh pendidikan,
3. Ibu Subektiningsih, M.Kom., selaku dosen pembimbing, yang telah memberikan arahan, ilmu, serta bimbingan dengan penuh kesabaran sehingga penelitian ini dapat terselesaikan dengan baik.
4. Teman-teman seperjuangan, yang telah memberikan dukungan, kebersamaan, dan semangat selama proses perkuliahan hingga penyusunan skripsi ini.
5. Almamater tercinta, Universitas AMIKOM Yogyakarta, yang telah menjadi tempat penulis menimba ilmu dan mengembangkan diri untuk menjadi lebih baik.
6. Semua pihak yang tidak dapat disebutkan satu per satu yang telah memberikan bantuan secara langsung maupun tidak langsung selama proses penyusunan skripsi.

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga skripsi ini dapat diselesaikan dengan baik sebagai salah satu syarat untuk memperoleh gelar Sarjana pada Program Studi Informatika, Universitas AMIKOM Yogyakarta. Dalam proses penyusunan skripsi ini, penulis memperoleh bantuan, dukungan, dan bimbingan dari berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM., selaku Rektor Universitas Amikom Yogyakarta,
2. Prof. Dr. Kusriani, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Amikom Yogyakarta,
3. Ibu Eli Pujastuti, M.Kom, selaku Ketua Program Studi Informatika Universitas Amikom Yogyakarta,
4. Ibu Subektiningsih, M.Kom., selaku dosen pembimbing yang telah memberikan arahan dan bimbingan selama penyusunan skripsi,
5. Ibu Ike Verawati, M.Kom, selaku dosen wali yang telah membimbing penulis selama masa perkuliahan,
6. Seluruh dosen dan civitas akademika Universitas Amikom Yogyakarta, yang telah memberikan ilmu, pengalaman, dan wawasan selama kuliah.

Penulis menyadari bahwa skripsi ini masih memiliki keterbatasan, sehingga kritik dan saran sangat diharapkan demi penyempurnaan karya ini. Semoga skripsi ini dapat memberikan manfaat, khususnya dalam bidang keamanan jaringan dan keamanan *web server* personal.

Yogyakarta, 17 Mei 2026

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	lii
HALAMAN PERNYATAAN KEASLIAN SKRIPSI	iv
HALAMAN PERSEMBAHAN	v
KATA PENGANTAR	vi
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xi
DAFTAR LAMBANG DAN SINGKATAN	xii
DAFTAR ISTILAH	xiii
INTISARI	xvi
<i>ABSTRACT</i>	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	4
1.5 Manfaat Penelitian	4
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	7
2.1 Studi Literatur	7
2.2 Dasar Teori	13
BAB III METODE PENELITIAN	21
3.1 Objek Penelitian	21
3.2 Alur Penelitian	22
3.3 Alat dan Bahan	26
BAB IV HASIL DAN PEMBAHASAN	29
4.1 Perancangan dan Instalasi Lingkungan Server	29

4.2	Implementasi Konfigurasi Sistem Keamanan	30
4.3	Skenario Pengujian	32
4.4	Implementasi Skenario Pengujian	34
4.5	Pelaksanaan Simulasi Serangan	35
4.6	Monitoring dan Akuisisi Data	40
4.6.1.	Perbandingan Respons Server dan Ukuran Paket (<i>Payload</i>)	43
4.6.2.	Perbandingan Beban Komputasi (<i>Resource Usage</i>)	43
4.6.3.	Perbandingan Kecepatan Deteksi dan Hasil Mitigasi	44
4.7	Analisis dan Interpretasi Hasil	45
BAB V PENUTUP		47
5.1	Kesimpulan	47
5.2	Saran	47
REFERENSI		49

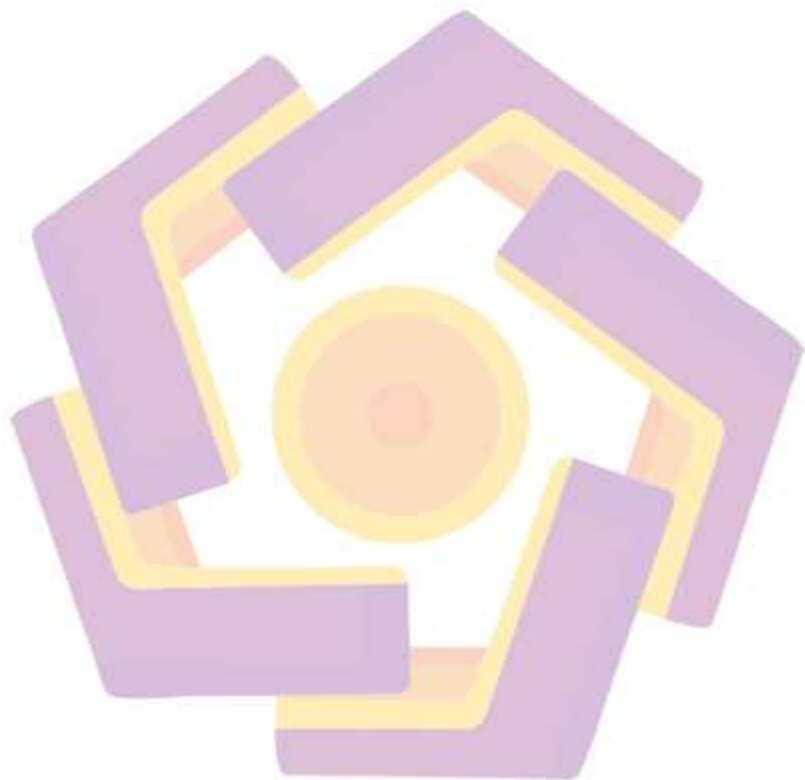
DAFTAR TABEL

Tabel 2.1 Keaslian Penelitian	10
Tabel 3.1 Spesifikasi <i>Server</i>	24
Tabel 3.2 Spesifikasi Penyerang	24
Tabel 3.3 Perangkat Keras	27
Tabel 3.4 Perangkat Lunak	28
Tabel 4.1 Perbandingan Reaksi <i>Server</i>	39
Tabel 4.2 Perbandingan Respons <i>Server</i>	43
Tabel 4.3 Perbandingan Beban Komputasi	43
Tabel 4.4 Perbandingan Beban Komputasi	44

DAFTAR GAMBAR

Gambar 2.1 Serangan DDoS dan Distribusi Tipe Serangan	15
Gambar 2.2 Alur Kerja Deteksi Serangan pada WAF	16
Gambar 3.1 Simulasi Sistem Keamanan	22
Gambar 3.2 Alur Penelitian	23
Gambar 4.1 Instalasi Lingkungan <i>Server</i>	29
Gambar 4.2 Konfigurasi <i>Fail2Ban</i>	30
Gambar 4.3 Konfigurasi OWASP	31
Gambar 4.4 Skenario Penyerang	32
Gambar 4.5 Topologi Serangan	33
Gambar 4.6 Skenario Pengujian	34
Gambar 4.7 Serangan Terhadap <i>Server</i>	35
Gambar 4.8 <i>Log</i> Tanpa Perlindungan	36
Gambar 4.9 Skenario Pertahanan <i>ModSecurity</i>	37
Gambar 4.10 Skenario Pertahanan <i>Fail2Ban</i>	38
Gambar 4.11 <i>Htop</i> Tanpa Perlindungan	40
Gambar 4.12 <i>Htop</i> Dengan <i>ModSecurity</i>	41
Gambar 4.13 <i>Htop</i> Dengan <i>Fail2Ban</i>	42

DAFTAR LAMPIRAN



DAFTAR LAMBANG DAN SINGKATAN



CPU	<i>Central Processing Unit</i>
DDoS	<i>Distributed Denial of Service</i>
HTTP	<i>Hypertext Transfer Protocol</i>
HULK	<i>HTTP Unbearable Load King</i>
IP	<i>Internet Protocol</i>
IPS	<i>Intrusion Prevention System</i>
LAN	<i>Local Area Network</i>
RAM	<i>Random Access Memory</i>
VPS	<i>Virtual Private Server</i>
WAF	<i>Web Application Firewall</i>
CRS	<i>Core Rule Set</i>
GB	<i>Gigabyte</i>
NVMe	<i>Non-Volatile Memory Express</i>
SQLi	<i>Structured Query Language Injection</i>
XSS	<i>Cross-Site Scripting</i>

DAFTAR ISTILAH



<i>Application Layer (Layer 7)</i>	Lapisan ketujuh dalam model referensi jaringan OSI yang berinteraksi langsung dengan aplikasi web.
<i>Backend</i>	Bagian dari sistem <i>server</i> (seperti PHP-FPM) yang bertugas memproses logika aplikasi dan kode web secara dinamis di belakang layar.
<i>Baseline</i>	Kondisi pengujian dasar pada server tanpa mengaktifkan sistem keamanan apa pun, digunakan sebagai standar perbandingan kinerja.
<i>Botnet</i>	Sekumpulan perangkat atau komputer yang telah disusupi dan dikendalikan dari jarak jauh untuk meluncurkan serangan siber secara serentak.
<i>Computational Overhead</i>	Beban komputasi tambahan (penggunaan CPU/RAM) yang harus ditanggung oleh sistem akibat pemrosesan perangkat lunak keamanan seperti <i>ModSecurity</i> .
<i>Downtime</i>	Kondisi kelumpuhan layanan di mana sistem atau web server berhenti beroperasi dan tidak dapat diakses oleh pengguna yang sah.
<i>Embedded Firewall</i>	Sistem keamanan yang ditanamkan atau dikonfigurasi secara langsung ke dalam arsitektur mesin <i>server</i> .
<i>Fail2Ban</i>	Perangkat lunak Intrusion Prevention System (IPS) yang bekerja dengan memblokir alamat IP penyerang pada tingkat <i>firewall</i> berdasarkan deteksi dari riwayat <i>log</i> .

Firewall

Sistem keamanan jaringan dasar yang bertugas memantau, menyaring, dan mengontrol lalu lintas data yang masuk atau keluar.

HTTP Flood

Metode serangan DDoS pada lapisan aplikasi yang membanjiri target dengan ribuan permintaan HTTP palsu untuk menguras sumber daya *server*.

Log-parsing

Metode pemantauan keamanan yang bekerja secara reaktif dengan membaca dan menganalisis rekam jejak (log) aktivitas *server* untuk menemukan pola anomali.

Malicious Request

Permintaan akses atau paket data lalu lintas berbahaya yang dikirimkan oleh penyerang dengan tujuan merusak atau membebani *server*.

ModSecurity

Perangkat lunak *Web Application Firewall* (WAF) yang bekerja menyaring dan menolak permintaan berbahaya secara instan di lapisan aplikasi.

Rate Limiting

Mekanisme kontrol dan pembatasan laju jumlah permintaan akses ke dalam jaringan komputer dalam periode waktu tertentu.

Resource Exhaustion

Kondisi kritis di mana sumber daya komputasi utama *server* (seperti CPU dan RAM) habis terkuras akibat beban pemrosesan yang melebihi kapasitas.

Reverse Proxy

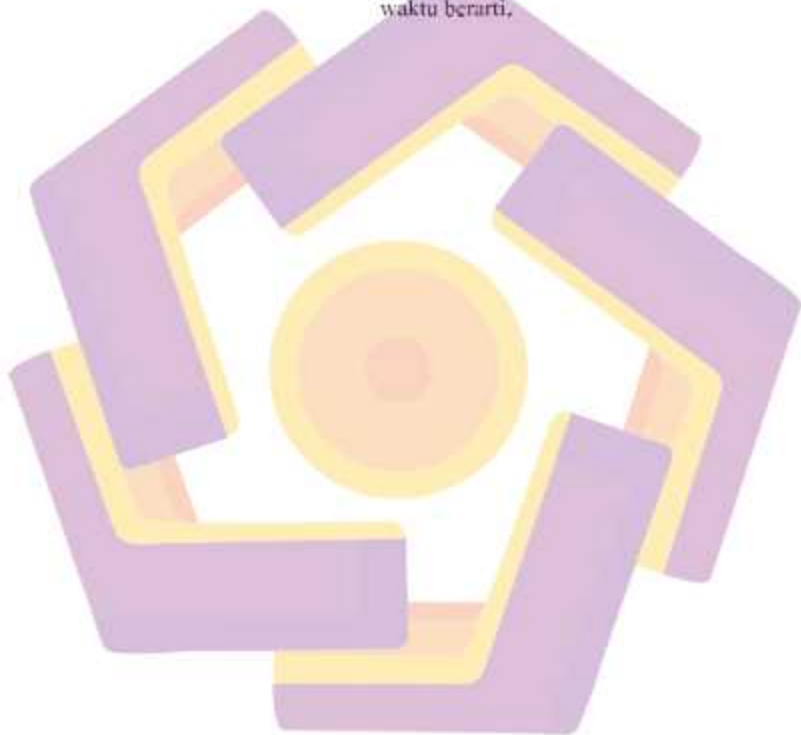
Server perantara yang menerima dan meneruskan lalu lintas klien ke *web server* utama, yang umumnya digunakan pada perancangan topologi keamanan *web*.

Throughput

Ukuran volume data aktual yang berhasil diproses dan ditransmisikan oleh server kepada klien di dalam sebuah jaringan.

Zero-latency

Kondisi waktu respons penolakan lalu lintas yang sangat cepat (*instan*) tanpa adanya jeda waktu berarti.



INTISARI

Peningkatan penetrasi internet berbanding lurus dengan ancaman keamanan siber, salah satunya adalah serangan *Distributed Denial of Service* (DDoS) pada lapisan aplikasi (Layer 7). Serangan jenis *HTTP Flood*, seperti penggunaan modul penelitian HULK, sangat berbahaya karena meniru perilaku pengguna sah secara masif. Masalah utama dari serangan ini adalah penipisan sumber daya komputasi secara langsung (*resource exhaustion*), yang berdampak pada terkurasnya kapasitas CPU dan memori hingga menyebabkan kelumpuhan layanan secara total (*downtime*) pada *web server* personal yang berspesifikasi terbatas. Untuk menyelesaikan permasalahan tersebut, penelitian ini melakukan eksperimen pada lingkungan *Virtual Private Server* (VPS) terisolasi dengan sistem operasi Linux Ubuntu, *Nginx*, dan PHP-FPM. Peneliti menggunakan metode komparatif untuk membandingkan efektivitas dua sistem mitigasi, yaitu *Fail2Ban* (berbasis pemantauan log) dan *ModSecurity* (berbasis *Web Application Firewall*). Tahapan penyelesaian masalah meliputi implementasi sistem keamanan, simulasi serangan menggunakan modul HULK, serta akuisisi data metrik kinerja server (pemakaian CPU, memori, dan waktu deteksi) secara *real-time*. Hasil penelitian menunjukkan bahwa kedua metode sangat efektif mencegah *downtime*. *ModSecurity* mampu memblokir serangan secara instan (*zero-latency*), namun mengonsumsi CPU secara ekstrem hingga 158,1%. Sebaliknya, *Fail2Ban* terbukti jauh lebih hemat sumber daya karena mampu mengembalikan CPU ke batas normal (0,0% - 2,8%) setelah memblokir IP di tingkat *firewall*, meskipun memiliki jeda deteksi 1-2 detik. Kontribusi penelitian ini dapat dimanfaatkan oleh administrator *web server* personal untuk menentukan solusi mitigasi DDoS yang paling efisien. Untuk penelitian lebih lanjut, direkomendasikan pengembangan arsitektur keamanan hibrida yang mengintegrasikan kedua metode tersebut.

Kata kunci: DDoS, Fail2Ban, HULK, ModSecurity, Web Server.

ABSTRACT

The increase in internet penetration is directly proportional to cybersecurity threats, one of which is the Application Layer (Layer 7) Distributed Denial of Service (DDoS) attack. HTTP Flood attacks, such as those utilizing the HULK research module, are highly dangerous as they massively mimic legitimate user behavior. The primary issue with these attacks is direct resource exhaustion, which severely drains CPU and memory capacities, ultimately causing total service downtime on personal web servers with limited specifications. To address this problem, this study conducted experiments in an isolated Virtual Private Server (VPS) environment running the Linux Ubuntu operating system, Nginx, and PHP-FPM. The researcher employed a comparative method to evaluate the effectiveness of two mitigation systems: Fail2Ban (log monitoring-based) and ModSecurity (Web Application Firewall-based). The problem-solving stages included the implementation of the security systems, attack simulations using the HULK module, and real-time acquisition of server performance metrics (CPU usage, memory consumption, and detection time). The results indicate that both methods are highly effective in preventing downtime. ModSecurity was able to block attacks instantly (zero-latency) but consumed an extreme amount of CPU, reaching up to 158.1%. Conversely, Fail2Ban proved to be significantly more resource-efficient; it restored CPU usage to normal levels (0.0% - 2.8%) after blocking IPs at the firewall level, despite having a 1-2 second detection delay. The findings of this study can assist personal web server administrators in determining the most efficient DDoS mitigation solution. For future research, developing a hybrid security architecture that integrates both methods is recommended.

Keywords: DDoS, Fail2Ban, HULK, ModSecurity, Web Server.