



**ANALISIS MITIGASI SERANGAN DDOS MENGGUNAKAN
ENTROPY DAN PUZZLE BERBASIS PROOF OF WORK PADA
SERVER UBUNTU**

SKRIPSI

BERLIANNA UPIK NURNIATI 2107421022

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

2025



**ANALISIS MITIGASI SERANGAN DDOS MENGGUNAKAN
ENTROPY DAN PUZZLE BERBASIS PROOF OF WORK PADA
SERVER UBUNTU**

SKRIPSI

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

BERLIANNA UPIK NURNIATI

2107421022

PROGRAM STUDI TEKNIK MULTIMEDIA DAN JARINGAN

JURUSAN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK NEGERI JAKARTA

2025



© Hak Cipta milik Politeknik Negeri Jakarta

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini:

Nama : Berliana Upik Nurniati
NIM : 2107421022
Jurusan / Program Studi : Teknik Informatika dan Komputer /
Teknik Multimedia dan Jaringan
Judul Skripsi : Analisis Mitigasi Serangan DDoS Menggunakan
Entropy dan Puzzle Berbasis *Proof of Work* pada
Server Ubuntu

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, 23 Juli 2025

Yang membuat pernyataan,



(Berlianna Upik Nurniati)

NIM. 2107421022

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

LEMBAR PENGESAHAN

Skripsi diajukan oleh :

Nama : Berlianna Upik Nurniati

NIM : 2107421022

Program Studi : Teknik Multimedia dan Jaringan

Judul Skripsi : Analisis Mitigasi Serangan DDoS Menggunakan
Entropy dan Puzzle Berbasis Proof Of Work pada
Server Ubuntu

Telah diuji oleh tim penguji dalam Sidang Skripsi pada hari Rabu, tanggal 9, bulan Juli, tahun 2025 dan dinyatakan **LULUS**.

Disahkan oleh

Pembimbing I : Maria Agustin, S.Kom., M.Kom

Penguji I : Defiana Arnaldy, S.Tp., M.Si

Penguji II : Dr. Indra Hermawan., M.Kom

Penguji III : Chandra Wirawan, M.Kom

Mengetahui:

Jurusan Teknik Informatika dan Komputer

Ketua



(Dr. Anita Hidayati, S.Kom., M.Kom.)

NIP. 197908032003122003



KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul "Analisis Mitigasi Serangan DDoS Menggunakan *Entropy* dan Puzzle Berbasis *Proof of Work* pada Server Ubuntu". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Diploma IV pada Program Studi Teknik Multimedia dan Jaringan, Jurusan Teknik Informatika dan Komputer, Politeknik Negeri Jakarta.

Dalam proses penyusunan skripsi ini, penulis menyadari bahwa tidak akan dapat menyelesaikannya tanpa bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih dan penghargaan yang setinggi-tingginya kepada:

1. Orang tua dan seluruh keluarga tercinta, atas kasih sayang, doa, dan dukungannya moril agar proses penyusunan skripsi penulis berjalan lancar, serta memberikan dukungan dalam menyelesaikan skripsi
2. Ibu Maria Agustin, S.Kom., M.Kom. sebagai dosen pembimbing yang telah meluangkan waktu, membantu, mendukung dan memberikan masukan serta saran kepada penulis selama pengerjaan skripsi hingga selesai
3. Bapak dan Ibu Dosen Jurusan Teknik Informatika dan Komputer, khususnya program studi Teknik Multimedia dan Jaringan, atas ilmu, motivasi, dan inspirasi yang telah diberikan.
4. Teman - teman penulis, Chiara Adristi, Nurul Aulia Dewi, Yazmin Nur'Aini, Layla Rosyidah, Niken Maharani, Ainur Rafika, Qathrah Nadiyah Salsabila, Muhammad Daffa Rasyid, Shoffan Darul, Sandika Arga, Robby Akbar, dan teman teman lain yang tidak dapat disebutkan satu persatu, yang selalu mendukung, memberikan semangat, dan kebersamaan dalam suka maupun duka selama masa perkuliahan dan penyusunan skripsi ini.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat penulis harapkan demi perbaikan di masa mendatang. Semoga laporan ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang berkepentingan.

Depok, 7 Juli 2025

Berlianna Upik Nurniati





© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

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

Nama : Berlianna Upik Nurniati
NIM : 2107421022
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 Mitigasi Serangan DDoS Menggunakan *Entropy* dan Puzzle Berbasis *Proof Of Work* pada Server Ubuntu

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, 25 JULI 2025

Yang menyatakan,



(Berlianna Upik Nurniati)

NIM. 2107421022



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

ANALISIS MITIGASI SERANGAN DDOS MENGUNAKAN ENTROPY DAN PUZZLE BERBASIS PROOF OF WORK PADA SERVER UBUNTU

ABSTRAK

Server yang terhubung ke jaringan publik rentan terhadap berbagai jenis serangan siber, salah satunya adalah serangan *Distributed Denial of Service* (DDoS) yang bertujuan melumpuhkan layanan dengan membanjiri server menggunakan permintaan palsu secara terus-menerus. Penelitian ini mengusulkan metode mitigasi serangan DDoS menggunakan pendekatan dua tahap, yaitu deteksi berbasis *entropy* dan verifikasi berbasis *puzzle Proof of Work* (PoW). Deteksi dilakukan dengan menghitung nilai *entropy* dari distribusi alamat IP yang mengakses *endpoint* login server Ubuntu secara *real time*. Jika nilai *entropy* turun di bawah ambang batas tertentu atau pola trafik menunjukkan anomali, sistem akan mengaktifkan mitigasi. Selanjutnya, hanya klien yang dapat menyelesaikan tantangan puzzle kriptografi (berbasis SHA-256) yang diizinkan melanjutkan proses login. Mekanisme ini mencegah penyerang mengakses sistem tanpa autentikasi dan meminimalkan false positive pada pengguna sah. Pengujian dilakukan dalam lingkungan lokal dengan berbagai skenario jumlah *attacker* dan volume serangan menggunakan tools HTTP Flood. Hasil evaluasi menunjukkan bahwa kombinasi metode *entropy* dan puzzle PoW mampu mengklasifikasikan trafik dengan akurasi mencapai 100%, serta menjaga performa server tetap stabil saat terjadi serangan.

Kata Kunci: Ubuntu Server, DDoS, Entropy, Proof of Work (PoW)



DAFTAR ISI

SURAT PERNYATAAN BEBAS PLAGIARISME	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
SURAT PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS	v
ANALISIS MITIGASI SERANGAN DDOS MENGGUNAKAN ENTROPY DAN PUZZLE BERBASIS PROOF OF WORK PADA SERVER UBUNTU	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	ix
DAFTAR TABEL	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan dan Manfaat	4
1.4.1 Tujuan.....	4
1.4.2 Manfaat	5
1.5 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA	7
2.1 Penelitian Terdahulu.....	7
2.2 Distributed Denial of Service (DDoS)	9
2.3 Ubuntu Server	11
2.4 Metode Deteksi Serangan DDoS	12
2.5 Metode Mitigasi Serangan DDoS	15
2.6 SHA-256	15
2.7 OpenSSH.....	16
2.8 GoldenEye.....	16
BAB III METODOLOGI PENELITIAN	17
3.1 Rancangan Penelitian	17
3.2 Tahapan Penelitian	18
3.3 Objek Penelitian	19
BAB IV HASIL DAN PEMBAHASAN	20

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian , penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengemukakan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

4.1	Analisis Kebutuhan	20
4.2	Perancangan Sistem	21
4.2.1	Arsitektur Sistem.....	21
4.2.2	Flowchart Sistem	22
4.2.3	Topologi Jaringan.....	23
4.2.4	Pengalamatan IP Address.....	26
4.2.5	Spesifikasi Virtual Machine.....	27
4.3	Implementasi Sistem	28
4.3.1	Instalasi Virtual Machine dan Konfigurasi Ubuntu Server.....	28
4.3.2	Instalasi dan Konfigurasi Web Server Apache2.....	29
4.3.3	Instalasi MySQL dan Konfigurasi Database.....	34
4.3.4	Pembuatan Sistem Login Berbasis PHP	43
4.3.5	Implementasi Perhitungan Entropy.....	46
4.3.6	Implementasi Puzzle <i>Proof of Work</i> (PoW)	48
4.3.7	Logging dan Monitoring Sistem Mitigasi.....	49
4.3.8	Instalasi GoldenEye	50
4.4	Pengujian.....	51
4.4.1	Deskripsi Pengujian	51
4.4.2	Prosedur Pengujian	52
4.4.3	Data Hasil Pengujian.....	70
4.4.4	Analisis Data Pengujian.....	95
BAB V PENUTUP		102
5.1	Kesimpulan	102
5.1	Saran.....	104
DAFTAR PUSTAKA.....		105
DAFTAR RIWAYAT HIDUP		108



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR GAMBAR

Gambar 2. 1 Ilustrasi Serangan Berbasis Volume	10
Gambar 2. 2 Ilustrasi Serangan Berbasis Protokol	10
Gambar 2. 3 Ilustrasi Serangan Berbasis Layer Aplikasi.....	11
Gambar 3. 1 Tahapan Penelitian	18
Gambar 4. 1 Arsitektur Sistem.....	21
Gambar 4. 2 Flowchart Sistem.....	22
Gambar 4. 3 Topologi Jaringan 3 Virtual Machines	23
Gambar 4. 4 Topologi Jaringan 5 Virtual Machines	24
Gambar 4. 5 Topologi Jaringan 9 Virtual Machines	25
Gambar 4. 6 Logo Virtual Box.....	28
Gambar 4. 7 Memperbarui Daftar Paket	29
Gambar 4. 8 Instalasi Web Server Apache.....	29
Gambar 4. 9 Konfigurasi UFW Status	30
Gambar 4. 10 Pembaruan Konfigurasi Apache.....	30
Gambar 4. 11 Pengecekan Status Apache	31
Gambar 4. 12 Tampilan Web Server Apache	31
Gambar 4. 13 Pembuatan Direktori Baru untuk Menjalankan Sistem Mitigasi ..	32
Gambar 4. 14 Instalasi OpenSSL.....	32
Gambar 4. 15 Konfigurasi Modul SSL pada Apache.....	32
Gambar 4. 16 Instalasi OpenSSH.....	33
Gambar 4. 17 Pengecekan Status OpenSSH.....	33
Gambar 4. 18 Percobaan SSH ke Ubuntu Server dari Windows	34
Gambar 4. 19 Instalasi MySQL Server	34
Gambar 4. 20 Pengecekan Status MySQL.....	35
Gambar 4. 21 Percobaan Akses MySQL dari Terminal	35
Gambar 4. 22 Create Database.....	36
Gambar 4. 23 Create Tabel entropy_log	36
Gambar 4. 24 Struktur Tabel entropy_log.....	37
Gambar 4. 25 Create Tabel entropy_monitor.....	37
Gambar 4. 26 Struktur Tabel entropy_monitor	38
Gambar 4. 27 Create Tabel log_request.....	39



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4. 28 Struktur Tabel log_request	39
Gambar 4. 29 Create Tabel puzzle_log	40
Gambar 4. 30 Struktur Tabel puzzle_log	41
Gambar 4. 31 Create Tabel users	42
Gambar 4. 32 Struktur Tabel users	42
Gambar 4. 33 Tampilan Halaman Login	43
Gambar 4. 34 Tampilan Landing Page	43
Gambar 4. 35 Form Login dengan Input Hidden Token untuk Mitigasi Puzzle ..	44
Gambar 4. 36 Script Pencatatan IP, User Agent, dan Endpoint ke dalam Tabel log_request	44
Gambar 4. 37 Pemanggilan Fungsi Perhitungan Entropy dari functions.php	45
Gambar 4. 38 Pengaturan Session Mitigasi dan Token Puzzle Berdasarkan Nilai Entropy	45
Gambar 4. 39 Penentuan Tingkat Kesulitan Puzzle Berdasarkan Nilai Entropy .	45
Gambar 4. 40 Pengiriman Kesulitan Puzzle saat Mitigasi Aktif ke puzzle.js	46
Gambar 4. 41 Query Pengambilan IP berdasarkan Sliding Window	46
Gambar 4. 42 Perhitungan Real Time Entropy dengan Rumus Shannon	47
Gambar 4. 43 Pengambilan data IP Unik, Interval, dan Request per Menit	47
Gambar 4. 44 Threshold Entropy untuk Mengaktifkan Mitigasi	47
Gambar 4. 45 Penyimpanan Hasil Monitor ke Tabel entropy_monitor	48
Gambar 4. 46 Implementasi Puzzle <i>Proof of Work</i>	48
Gambar 4. 47 Memperbarui Daftar Paket	50
Gambar 4. 48 Instalasi python3	50
Gambar 4. 49 Cloning Repository GoldenEye dari GitHub	50
Gambar 4. 50 Perintah untuk Menjalankan Serangan	51
Gambar 4. 51 Login User Sah saat Mitigasi tidak Aktif	60
Gambar 4. 52 Tampilan Berhasil masuk Landing Page saat Mitigasi tidak Aktif	60
Gambar 4. 53 Login User Sah saat Mitigasi Aktif	61
Gambar 4. 54 Tampilan User Sah Berhasil Masuk saat Mitigasi Aktif	62
Gambar 4. 55 Tampilan Login Attacker saat Mitigasi Aktif	62
Gambar 4. 56 Percobaan Login dengan Puzzle	63
Gambar 4. 57 Tampilan Attacker yang Gagal Masuk	63



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumunkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Gambar 4. 58 Perhitungan CPU dan Memory saat Mode Idle	66
Gambar 4. 59 Perhitungan PPS saat Mode Idl	66
Gambar 4. 60 Perhitungan CPU dan Memory saat Mode Normal	67
Gambar 4. 61 Perhitungan PPS saat Mode Normal	68
Gambar 4. 62 Perhitungan CPU dan Memory saat Mode Mitigation.....	69
Gambar 4. 63 Perhitungan PPS saat Mode Mitigation	69
Gambar 4. 64 Grafik Perubahan Entropy Serangan Pertama pada 3 VM.....	71
Gambar 4. 65 Grafik Perubahan Entropy Serangan Kedua pada 3 VM	72
Gambar 4. 66 Grafik Perubahan Entropy Serangan Ketiga pada 3 VM	72
Gambar 4. 67 Grafik Perubahan Entropy Serangan Pertama pada 5 VM.....	75
Gambar 4. 68 Grafik Perubahan Entropy Serangan Kedua pada 5 VM	75
Gambar 4. 69 Grafik Perubahan Entropy Serangan Ketiga pada 5 VM	76
Gambar 4. 70 Grafik Perubahan Entropy Serangan Pertama pada 9 VM.....	78
Gambar 4. 71 Grafik Perubahan Entropy Serangan Kedua pada 9 VM	79
Gambar 4. 72 Grafik Perubahan Entropy Serangan Ketiga pada 9 VM	79
Gambar 4. 73 Perbandingan Penggunaan CPU	98
Gambar 4. 74 Perbandingan Penggunaan Memory	99
Gambar 4. 75 Perbandingan Traffic PPS	99
Gambar 4. 76 Perbandingan Response Time	100



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu.....	7
Tabel 2. 2 Data Nilai entropy	13
Tabel 4. 1 Analisis Kebutuhan Perangkat Lunak dan Perangkat Keras	20
Tabel 4. 2 Pengalamatan IP Address	26
Tabel 4. 3 Spesifikasi Virtual Machine	27
Tabel 4. 4 Fungsi Tabel Database.....	49
Tabel 4. 5 Mode Uji	53
Tabel 4. 6 IP Address Attacker 3 Virtual Machines	54
Tabel 4. 7 IP Address Attacker 5 Virtual Machines	56
Tabel 4. 8 IP Address Attacker 9 Virtual Machines	58
Tabel 4. 9 Ketentuan Confusion Matrix	65
Tabel 4. 10 Pengamatan Entropy dari 3 Virtual Machines.....	71
Tabel 4. 11 Total Request dari 3 Virtual Machines	73
Tabel 4. 12 Pengamatan Entropy dari 5 Virtual Machines.....	74
Tabel 4. 13 Total Request dari 5 Virtual Machines	76
Tabel 4. 14 Pengamatan Entropy dari 9 Virtual Machines.....	77
Tabel 4. 15 Total Request dari 9 Virtual Machines	80
Tabel 4. 16 Perbandingan Hasil Deteksi DDoS	81
Tabel 4. 17 Perbandingan Metode Mitigasi DDoS	84
Tabel 4. 18 Hasil Confusion Matrix 3 VM.....	86
Tabel 4. 19 Hasil Confusion Matrix 5 VM.....	87
Tabel 4. 20 Hasil Confusion Matrix 9 VM.....	89
Tabel 4. 21 Hasil Pemantauan Resource Usage Mode Idle.....	91
Tabel 4. 22 Hasil Pemantauan Resource Usage Mode Normal.....	92
Tabel 4. 23 Hasil Pemantauan Resource Usage Mode Mitigation	92
Tabel 4. 24 Data Response Time Mode Normal	93
Tabel 4. 25 Data Response Time Mode Mitigation.....	94
Tabel 4. 26 Data Login Delay User Sah.....	95



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB I PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital telah mendorong peningkatan ketergantungan masyarakat terhadap layanan daring dan infrastruktur jaringan. Dalam kondisi ini, keamanan siber menjadi isu yang sangat krusial, karena sistem informasi terbuka terhadap berbagai jenis ancaman, salah satunya adalah serangan Distributed Denial of Service (DDoS). Serangan DDoS merupakan upaya untuk mengganggu ketersediaan layanan dengan membanjiri server target menggunakan lalu lintas jaringan secara berlebihan, sehingga menyebabkan layanan menjadi lambat atau bahkan tidak dapat diakses sama sekali (Wu et al., 2022).

Ancaman DDoS menjadi semakin berbahaya karena teknik yang digunakan oleh penyerang semakin canggih dan bersifat terdistribusi. Serangan ini tidak hanya berdampak pada gangguan layanan, tetapi juga dapat menyebabkan kerugian finansial, turunnya kepercayaan pengguna, serta terhambatnya operasional bisnis. Menurut laporan ID-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure), lebih dari satu juta insiden serangan siber terjadi di Indonesia dalam kurun waktu satu tahun, dan tren ini terus meningkat akibat kelemahan sistem dan aplikasi yang dieksploitasi secara masif (Chotimah, 2019).

Salah satu platform yang banyak digunakan dalam pengembangan sistem layanan berbasis web adalah Ubuntu Server, karena sifatnya yang open source, ringan, serta kompatibel dengan berbagai tools keamanan dan web server seperti Apache2 (Gorave, 2019). Namun demikian, server berbasis open-source seperti Ubuntu juga menjadi target potensial serangan DDoS, terutama karena banyaknya layanan publik yang di-host di dalamnya tanpa perlindungan adaptif yang memadai (Aydin et al., 2022; Xiong et al., 2020).

Pendekatan mitigasi tradisional seperti penggunaan firewall, intrusion detection system (IDS), dan blacklist IP sering kali tidak cukup efektif dalam menghadapi serangan DDoS berskala besar, terutama ketika serangan bersifat terdistribusi dan menyamar sebagai lalu lintas normal. Misalnya, dalam penelitian oleh (Patil & G,



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2023), ditemukan bahwa serangan DDoS terhadap infrastruktur cloud berbasis OpenStack mampu melumpuhkan firewall dan IDS karena perangkat tersebut tidak dirancang untuk memfilter lalu lintas dalam jumlah besar yang tampak seperti trafik normal. Dalam skenario simulasi menggunakan tools seperti LOIC dan Slowloris, firewall gagal membedakan antara trafik sah dan trafik berbahaya, sementara IDS mengalami beban berlebih hingga menurunkan performa sistem secara keseluruhan. Oleh karena itu, dibutuhkan pendekatan yang lebih adaptif dan dinamis dalam mendeteksi serta merespons anomali lalu lintas yang mengindikasikan adanya serangan (Aydın et al., 2022).

Untuk menyelesaikan masalah tersebut, diperlukan pendekatan mitigasi yang lebih adaptif dan cerdas, yang mampu melakukan deteksi dini dan respons otomatis terhadap anomali lalu lintas jaringan. Salah satu pendekatan yang dilakukan adalah analisis *entropy*, yaitu pengukuran tingkat ketidakpastian dalam distribusi trafik. Ketika trafik normal terjadi, distribusi alamat IP yang mengakses server cenderung merata, menghasilkan nilai *entropy* yang tinggi. Namun, ketika serangan DDoS terjadi, terutama pada jenis serangan berbasis botnet atau HTTP Flood, permintaan banyak dikirimkan dari IP yang sama atau jumlah IP yang sangat sedikit, menyebabkan penurunan drastis pada nilai *entropy*, menjadi indikator bahwa sedang terjadi trafik mencurigakan karena data *real time* dalam membaca pola trafik jaringan. (Hassan et al., 2024; Jawahar et al., 2024). Metode ini memiliki keunggulan karena tidak membutuhkan pelatihan data dan mampu berjalan secara *real time* dengan penggunaan sumber daya minimal (M, 2024).

Di sisi lain, deteksi trafik mencurigakan saja tidak cukup sistem juga memerlukan respon aktif dalam bentuk mekanisme mitigasi, untuk mencegah bot atau pelaku serangan melanjutkan permintaan ke server. Salah satu pendekatan yang terbukti efektif adalah penerapan puzzle berbasis *Proof of Work* (PoW). PoW memaksa klien menyelesaikan teka-teki komputasi, misalnya dengan mencari *nonce* yang menghasilkan hash SHA-256 berawalan nol sebanyak n digit. Puzzle ini ringan bagi pengguna manusia yang hanya melakukan satu permintaan login, tetapi menjadi sangat berat bagi bot yang melakukan ratusan permintaan per detik. Strategi ini menjadikan PoW sebagai semacam *rate limiter* kriptografis yang tidak



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

mengganggu pengguna sah, tetapi sangat memperlambat pelaku serangan (Chakraborty et al., 2022).

Penelitian oleh (Bazzanella & Gangemi, 2023) memperkenalkan sistem PoW adaptif yang mengatur tingkat kesulitan berdasarkan beban jaringan, dengan bukti bahwa pendekatan ini dapat secara signifikan mengurangi efektivitas botnet dan memaksa penyerang mengalokasikan sumber daya komputasi yang besar untuk setiap permintaan. Lebih lanjut, studi oleh (Bostanov, 2021) menekankan bahwa implementasi server side dari SHA-256 PoW dapat divalidasi dalam waktu kurang dari 20 milidetik, sehingga tidak membebani performa server secara signifikan jika proses komputasi klien menghasilkan *nonce*, *hash*, dan *base* yang valid secara efisien, yakni dalam satu atau dua iterasi hash pada tingkat kesulitan rendah. Dengan solusi penggabungan metode *entropy* untuk deteksi dan PoW sebagai mitigasi, sistem akan mampu mengidentifikasi serta memperlambat atau bahkan menghentikan serangan DDoS secara efisien, tanpa mengganggu akses pengguna sah (Alviano, 2023; Chakraborty et al., 2022).

1.2 Rumusan Masalah

Berdasarkan hal hal yang sudah disampaikan di atas, maka rumusan masalah yang dijadikan fokus pada penelitian ini adalah:

1. Bagaimana metode *entropy* dapat digunakan untuk mendeteksi potensi serangan DDoS berdasarkan distribusi lalu lintas IP pada server Ubuntu?
2. Bagaimana merancang dan mengimplementasikan sistem mitigasi serangan DDoS dengan menggunakan puzzle berbasis *Proof of Work* (PoW) secara dinamis saat terdeteksi trafik mencurigakan?
3. Bagaimana performa kombinasi metode *entropy* dan puzzle PoW dalam membedakan pengguna sah dan penyerang selama simulasi serangan DDoS?
4. Bagaimana dampak penerapan sistem mitigasi *entropy* dan puzzle PoW terhadap performa dan stabilitas server Ubuntu saat menghadapi trafik tinggi atau serangan DDoS?



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1.3 Batasan Masalah

Penelitian yang dilakukan untuk analisis mitigasi serangan ddos menggunakan *entropy* dan puzzle berbasis *Proof of Work* pada server ubuntu, memiliki sejumlah batasan masalah. Batasan-batasan tersebut adalah:

1. Jenis serangan DDoS yang dianalisis terbatas pada HTTP Flood (layer 7), dengan target utama endpoint login.php pada server web.
2. Deteksi dini serangan dilakukan menggunakan metode perhitungan *entropy* berbasis distribusi IP dan jumlah request.
3. Mekanisme mitigasi dirancang menggunakan puzzle berbasis *Proof of Work* (PoW) dengan algoritma SHA-256, yang dikerjakan oleh klien menggunakan JavaScript (client-side) dan diverifikasi oleh server menggunakan PHP.
4. Lingkungan pengujian dilakukan dalam jaringan lokal (private LAN) menggunakan platform VirtualBox, dengan skenario simulasi serangan dilakukan dari VM attacker ke VM target (Ubuntu Server).
5. Perangkat lunak (tools) yang digunakan untuk simulasi serangan adalah HTTP Flood tools GoldenEye.
6. Sistem yang diuji dan diimplementasikan berbasis Ubuntu Server dan tidak mencakup sistem operasi lain seperti Windows Server atau distribusi Linux lainnya.
7. Analisis efektivitas sistem dibatasi pada parameter-parameter seperti nilai *entropy*, status mitigasi, validitas puzzle, dan performa sistem (login success, CPU usage, dan logging), tanpa membandingkan dengan pendekatan machine learning atau IDS konvensional.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun Tujuan penelitian ini adalah sebagai berikut:

1. Untuk merancang dan mengimplementasikan metode deteksi serangan DDoS berbasis *entropy* dengan memanfaatkan distribusi IP dan jumlah permintaan dalam jangka waktu tertentu pada server Ubuntu.



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

2. Untuk mengembangkan sistem mitigasi dinamis terhadap serangan DDoS menggunakan puzzle berbasis *Proof of Work* (PoW) yang aktif hanya ketika trafik mencurigakan terdeteksi.
3. Untuk menganalisis dampak penerapan sistem mitigasi terhadap stabilitas dan performa server, khususnya dalam aspek validitas puzzle, tingkat keberhasilan login, serta penggunaan sumber daya selama kondisi serangan.

1.4.2 Manfaat

Adapun manfaat penelitian ini adalah sebagai berikut

1. Memberikan kontribusi terhadap pengembangan studi di bidang keamanan jaringan dan sistem informasi, khususnya dalam pendekatan mitigasi serangan DDoS berbasis statistik dan kriptografi.
2. Menawarkan solusi ringan dan efisien untuk mengamankan endpoint web login dari serangan HTTP Flood tanpa membebani server.
3. Memungkinkan administrator sistem untuk menerapkan mitigasi DDoS tanpa memerlukan perangkat keras tambahan atau lisensi berbayar, karena sistem ini dapat dibangun sepenuhnya dengan *software open source*.
4. Menjadi referensi dalam pengembangan penelitian lanjutan, baik pada sisi deteksi anomali, algoritma mitigasi dinamis, maupun integrasi dengan model machine learning.
5. Memberikan referensi implementatif bagi praktisi keamanan jaringan maupun pengembang sistem web dalam membangun mekanisme pertahanan terhadap DDoS berbasis *web layer* (Layer 7).
6. Memberikan dasar bagi pengembang dan penyedia layanan web untuk membangun sistem anti-DDoS sederhana namun efektif, yang dapat diterapkan pada server produksi dengan biaya rendah.

1.5 Sistematika Penulisan

Berikut adalah sistematika penulisan yang digunakan dalam penyusunan proposal penelitian ini, yaitu sebagai berikut:



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

1. BAB I PENDAHULUAN

Bab pertama pendahuluan, menguraikan tentang latar belakang dari penelitian, rumusan masalah yang didapat dari latar belakang, Batasan masalah pada penelitian ini, serta manfaat dan tujuan dalam penelitian ini.

2. BAB II TINJAUAN PUSTAKA

Bab kedua menguraikan tentang landasan-landasan teori dan konsep-konsep terkait dengan sebuah permasalahan pada penelitian ini, serta beberapa penelitian yang relevan terkait dari penelitian-penelitian terdahulu untuk dikaji dalam penelitian ini.

3. BAB III METODE PENELITIAN

Bab ketiga dalam penelitian ini akan menjabarkan tentang metode penelitian yang akan digunakan, baik berhubungan dengan perancangan penelitian, tahapan-tahapan yang akan ditempuh dalam penelitian, objek dari penelitian, model penelitian, begitu juga teknik pengumpulan dan analisis data, hingga jadwal pelaksanaan.

4. BAB IV HASIL DAN PEMBAHASAN

Bab keempat pada penelitian ini berisikan analisis kebutuhan, perancangan sistem, implementasi sistem, pengujian, dan analisis hasil mitigasi serangan terhadap sistem yang telah dibuat.

5. BAB V PENUTUP

Bab kelima berisikan penjelasan mengenai hasil akhir dari penelitian berupa kesimpulan dan saran untuk penelitian berikutnya.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan hasil yang telah dicapai dalam penelitian skripsi ini, terdapat beberapa kesimpulan sebagai berikut:

1. Metode entropy terbukti efektif untuk mendeteksi potensi serangan DDoS pada server Ubuntu. Sistem berhasil mengamati penurunan nilai entropy secara real-time pada setiap skenario serangan (3 VM, 5 VM, dan 9 VM), dengan nilai entropy turun hingga <1.0 saat serangan aktif. Sistem juga mempertimbangkan status cooldown untuk mencegah false negative. Tingkat keberhasilan deteksi serangan tercatat 100% dari seluruh skenario pengujian.
2. Sistem mitigasi dengan puzzle PoW berhasil diimplementasikan secara adaptif dan selektif. Puzzle dikirim hanya kepada IP yang terdeteksi mencurigakan saat mitigasi aktif. Validasi puzzle di sisi server memastikan bahwa hanya pengguna yang menyelesaikan puzzle dan memiliki kredensial valid yang dapat login, memperkuat keamanan tanpa mengganggu user sah.
3. Performa sistem dalam membedakan pengguna sah dan penyerang sangat tinggi, dibuktikan dengan hasil confusion matrix pada tiga skenario:
 - Akurasi mencapai $>99\%$ pada semua pengujian,
 - Precision berada pada kisaran 98.52% – 98.64% ,
 - Recall sempurna 100% ,
 - F1-Score rata-rata $>99\%$.

Hasil ini menunjukkan sistem sangat efektif dalam mengenali dan memblokir trafik berbahaya tanpa kesalahan deteksi attacker (FN = 0).

4. Penerapan sistem mitigasi berdampak pada peningkatan beban server, namun performa sistem tetap berada dalam tingkat yang dapat diterima dan tidak mengganggu fungsionalitas layanan secara keseluruhan.
 - Saat mode normal, rata-rata penggunaan CPU sekitar 12% , memory 40% , dan traffic sekitar 7 PPS.



© Hak Cipta milik Politeknik Negeri Jakarta

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

- Saat mode mitigasi, CPU melonjak hingga 92%, dan traffic mencapai 264 PPS, menandakan server bekerja intensif untuk memproses puzzle dan validasi serangan.
- Response time juga meningkat:
 - Mode normal: rata-rata 3,32 detik
 - Mode mitigasi: rata-rata 51,97 detik
- Login delay user sah bertambah, dari 0,68 detik (tanpa serangan) menjadi 2,77 detik (saat mitigasi aktif), namun tetap tidak menyebabkan kegagalan login.

Keseluruhan hasil menunjukkan bahwa sistem mitigasi DDoS berbasis *entropy* dan puzzle PoW yang dirancang telah berhasil mendeteksi serangan secara adaptif, memitigasi secara selektif, serta mempertahankan aksesibilitas pengguna sah dengan dampak minimal terhadap performa server. Sistem ini dinilai layak diimplementasikan dalam lingkungan nyata untuk meningkatkan keamanan server terhadap ancaman DDoS berbasis HTTP Request.

**POLITEKNIK
NEGERI
JAKARTA**



5.1 Saran

Berdasarkan penelitian yang telah dilakukan, berikut beberapa saran yang dapat dijadikan masukan untuk penelitian selanjutnya, diantaranya:

1. Penelitian ini dilakukan dalam jaringan lokal. Pengujian lebih lanjut perlu dilakukan di lingkungan nyata agar sistem dapat dievaluasi dalam kondisi trafik yang lebih kompleks.
2. Pengujian hanya melibatkan sedikit perangkat. Disarankan menambah variasi perangkat dan jaringan user sah untuk menguji ketepatan sistem dalam membedakan pengguna dan attacker.
3. Sistem perlu dikembangkan lebih lanjut dengan mengintegrasikan firewall (seperti iptables) dan IDS (seperti Snort) guna memperkuat mitigasi serangan.
4. Sistem saat ini fokus pada serangan HTTP GET. Pengembangan lanjutan diperlukan untuk mendeteksi serangan aplikasi seperti HTTP POST Flood.

Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR PUSTAKA

- Afifah Rodhiyatun Nisa, A., Ananditto Daffa Wijayanto, Arya Prabudi Jaya Priana, & Setiawan, A. (2024). Analisis Log Server untuk mendeteksi Serang DDoS pada Keamanan Jaringan di Website. *Journal of Internet and Software Engineering*, 1(3), 17. <https://doi.org/10.47134/pjise.v1i3.2612>
- Alviano, M. (2023). Hashcash Tree, a Data Structure to Mitigate Denial-of-Service Attacks. *Algorithms*, 16. <https://doi.org/10.3390/a16100462>
- Asa'ari Lubis, B., Yanuar Ar-Rafi, D., Widiyani, I., Lestari, K. I., & Zy, A. T. (2024). *Analysis and Mitigation Technique of DDoS on Server Networks Based on Modern Technology*.
- Aydın, H., Orman, Z., & Aydın, M. A. (2022). A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment. *Computers and Security*, 118. <https://doi.org/10.1016/j.cose.2022.102725>
- Bashurov, V., & Safonov, P. (2023). Anomaly detection in network traffic using entropy-based methods: application to various types of cyberattacks. *Issues in Information Systems*, 24(4), 82–94. https://doi.org/10.48009/4_iis_2023_107
- Bazzanella, D., & Gangemi, A. (2023). Bitcoin: a new proof-of-work system with reduced variance. *Financial Innovation*, 9. <https://doi.org/10.1186/s40854-023-00505-2>
- Bostanov, V. (2021). Client Puzzle Protocols as Countermeasure against Automated Threats to Web Applications. *IEEE Access*, 9, 75722–75728. <https://doi.org/10.1109/ACCESS.2021.3082037>
- Center Canadian for Cyber. (2024). *Defending against distributed denial of service (DDoS) attacks*. <https://www.cyber.gc.ca/en/guidance/defending-against-distributed-denial-service-ddos-attacks-itsm80110>
- Chakraborty, T., Mitra, S., Mittal, S., & Young, M. (2022). AI_Adaptive_POW: An AI assisted Proof Of Work (POW) framework for DDoS defense. *Software Impacts*, 13. <https://doi.org/10.1016/j.simpa.2022.100335>
- Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency].
Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 10(2), 113–128. <https://doi.org/10.22212/jp.v10i2.1447>

Cloudflare. (n.d.). *What is a DDoS attack?*

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

Documentation, U. (2025). *Ubuntu Server documentation*.

<https://Documentation.Ubuntu.Com/Server/>.

Gorave, A. (2019). Ambient Intelligence for Rehabilitation: A Survey General Terms. In *International Journal of Computer Applications* (Vol. 178, Issue 38).
www.ijcaonline.org

Hassan, A. I., El Reheem, E. A., & Guirguis, S. K. (2024). An entropy and machine learning based approach for DDoS attacks detection in software defined networks. *Scientific Reports*, 14. <https://doi.org/10.1038/s41598-024-67984-w>

Jawahar, A., Kaythry, P., Vinoth Kumar, C., Vinu, R., Amrith, R., Bavapriyan, K., & Gopinaath, V. (2024). DDoS mitigation using blockchain and machine learning techniques. *Multimedia Tools and Applications*, 83, 60265–60278.
<https://doi.org/10.1007/s11042-023-18028-4>

Kurniawan, M. T. (2023). *UNIVERSITAS INDONESIA PENGEMBANGAN METODE ENTROPY UNTUK DETEKSI SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDoS) PADA SOFTWARE DEFINED NETWORK (SDN) DAN DENGAN PENERAPAN FEATURE SELECTION*.

M, J. (2024). *Entropy: A Mathematical Approach to DDoS Protection*.

<https://Medium.Com/%40remind.Stephen.to.Do.Sth/Entropy-a-Mathematical-Approach-to-Ddos-Protection-71a2af38ab91>.

openssh. (2023). *OpenSSHManual Pages*. <https://Www.Openssh.Com/Manual.Html>.

Patil, R., & G, N. D. (2023). *Mitigation of DDoS Attacks using Entropy and Proof-of-Work Based Puzzle in OpenStack Cloud*.
<https://doi.org/10.1109/CONIT59222.2023.10205888>

Pebrianto, J., & Suryani, V. (2025). Adaptive DDoS Attack Detection: Entropy-Based Model With Dynamic Threshold and Suspicious IP Reevaluation. *IEEE Access*, 13, 55858–55876. <https://doi.org/10.1109/ACCESS.2025.3553144>



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

Seidl, J. (2020). *GitHub - jseidl/GoldenEye: GoldenEye Layer 7 (KeepAlive+NoCache) DoS Test Tool*. <https://Github.Com/Jseidl/GoldenEye>.

Sumayyah, Z. I., Permana, S. D. S., Tsabit, M., & Setiawan, A. (2024). Penerapan dan Mitigasi Teknik Slowloris dalam Serangan Distributed Denial-of-Service (DDos) terhadap Website Ilegal dengan Kali Linux. *Journal of Internet and Software Engineering*, 1(2), 14. <https://doi.org/10.47134/pjise.v1i2.2694>

Süzen, A. A. (2021). UNI-CAPTCHA: A Novel Robust and Dynamic User-Non-Interaction CAPTCHA Model Based on Hybrid biLSTM+Softmax. *Journal of Information Security and Applications*, 63. <https://doi.org/10.1016/j.jisa.2021.103036>

Tao, T. (2017, January). *The Erdos discrepancy problem*.

Wu, X., Xiao, L., Sun, Y., Zhang, J., Ma, T., & He, L. (2022). A survey of human-in-the-loop for machine learning. In *Future Generation Computer Systems* (Vol. 135, pp. 364–381). Elsevier B.V. <https://doi.org/10.1016/j.future.2022.05.014>

Xiong, J., Chen, L., Bhuiyan, M. Z. A., Cao, C., Wang, M., Luo, E., & Liu, X. (2020). A secure data deletion scheme for IoT devices through key derivation encryption and data analysis. *Future Generation Computer Systems*, 111, 741–753. <https://doi.org/10.1016/j.future.2019.10.017>

**POLITEKNIK
NEGERI
JAKARTA**



Hak Cipta :

1. Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan dan menyebutkan sumber :
 - a. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penulisan laporan, penulisan kritik atau tinjauan suatu masalah.
 - b. Pengutipan tidak merugikan kepentingan yang wajar Politeknik Negeri Jakarta
2. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Politeknik Negeri Jakarta

DAFTAR RIWAYAT HIDUP



Berlianna Upik Nurniati

Lahir di Magetan, 14 Juni 2002, anak pertama dari dua bersaudara. Lulus dari SD Negeri Kemanggisan 06 Pagi pada tahun 2015, kemudian melanjutkan pendidikan di SMP Negeri 111 Jakarta Barat dan lulus pada tahun 2018, dan selanjutnya melanjutkan pendidikan di SMA Negeri 16 Jakarta Barat dan lulus pada tahun 2021.

Setelah itu pada tahun 2021, penulis berkesempatan untuk melanjutkan pendidikan tinggi di Politeknik Negeri Jakarta Jurusan Teknik Informatika dan Komputer, Program Studi Teknik Multimedia dan jaringan.

