



**PERANCANGAN *BOT* UNTUK *MONITORING* SERVER DARI
SERANGAN *DISTRIBUTED DENIAL OF SERVICE*
MENGUNAKAN *JSON WEB TOKEN***

SKRIPSI

ARIF MAULANA RAHMAN

1610511034

UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI INFORMATIKA

2020



**PERANCANGAN *BOT* UNTUK *MONITORING* SERVER DARI
SERANGAN *DISTRIBUTED DENIAL OF SERVICE*
MENGUNAKAN *JSON WEB TOKEN***

SKRIPSI

**Diajukan Sebagai Salah Satu Syarat Untuk Kelulusan Mata
Kuliah Skripsi**

ARIF MAULANA RAHMAN

1610511034

**UNIVERSITAS PEMBANGUNAN NASIONAL VETERAN JAKARTA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA
2020**

PERNYATAAN ORISINALITAS

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Arif Maulana Rahman
NIM : 1610511034
Tanggal : 27 Mei 2020

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 29 Mei 2020

Yang Menyatakan,



(Arif Maulana Rahman)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional Veteran Jakarta,
saya yang bertanda tangan di bawah ini :

Nama : Arif Maulana Rahman
NIM : 1610511034
Fakultas : Ilmu Komputer
Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional Veteran Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul:

Perancangan Bot Untuk Monitoring Server Dari Serangan *Distributed Denial Of Service* Menggunakan *JSON Web Token*

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional Veteran Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 29 Mei 2020

Yang menyatakan,



(Arif Maulana Rahman)

LEMBAR PENGESAHAN

Skripsi diajukan oleh:

Nama : Arif Maulana Rahman
NIM : 1610511034
Program Studi : Informatika
Judul Skripsi : Perancangan *Bot* Untuk *Monitoring* Server Dari Serangan *Distributed Denial of Service* Menggunakan *JSON Web Token*

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional Veteran Jakarta.

Jayanta, S.Kom., M.Si
Dosen Penguji I

Nurul Chamidah, S.Kom., M.Kom.
Dosen Penguji II

Henki Bayu Seta, S.Kom., M.TI.
Dosen Pembimbing I

Ria Astriratma, S.Komp., M.Cs
Dosen Pembimbing II



Dr. Ermatita, M.Kom
Dekan

Anita Muliawati, S.Kom., MTI.
Ketua Program Studi

Ditetapkan di : Jakarta
Tanggal Ujian : 19 Juni 2020



**PERANCANGAN *BOT* UNTUK *MONITORING* SERVER DARI
SERANGAN *DISTRIBUTED DENIAL OF SERVICE*
MENGUNAKAN *JSON WEB TOKEN***

ARIF MAULANA RAHMAN

ABSTRAK

Dalam menjalankan sebuah server diperlukan sistem *monitoring* untuk mengamankan jaringan agar meminimalisir resiko jika terjadi percobaan intrusi. Salah satu serangan yang sering terjadi kepada server merupakan serangan *DDOS* (*Distributed Denial of Service*) yang mengakibatkan sistem yang diserang mengalami gangguan berupa *error request*, *halt*, kegagalan sistem dan sebagainya. Berdasarkan permasalahan yang dijelaskan, maka diperlukan sebuah *bot* untuk melakukan *monitoring* serta melindungi server dari serangan *DDOS*, dalam penelitian ini difokuskan serangan *DDOS* yang berjenis *UDP Flooding* dan *SYN Flooding*. *Bot* ini akan mampu mendeteksi serangan *UDP Flooding* dan *SYN Flooding* dengan membatasi jumlah paket yang ditujukan kepada *port* yang dibuka oleh server, apabila *bot* mendeteksi serangan maka *bot* akan memblokir serta mengirimkan notifikasi kepada admin server dengan menerapkan *set push notification* serta menggunakan *JSON Web Token* untuk memastikan notifikasi yang dikirimkan oleh *bot* kepada *smartphone* admin server terjaga integritas dan kerahasiaannya. *Monitoring* server memanfaatkan *bot* untuk mendeteksi serangan *DDOS* berjenis *UDP Flooding* dan *SYN Flooding* dengan membatasi jumlah paket yang dikirimkan kepada *port* yang dibuka oleh server, apabila jumlah paket yang dikirimkan lebih dari 100 paket per detik maka *bot* akan mengidentifikasi pengiriman tersebut sebagai serangan. Penerapan metode *JSON Web Token* agar bisa dioperasikan oleh *bot* admin server yakni dengan mengimplementasikan *package JSON Web Token* pada *bot* lalu memanggil fungsi *encode* agar *JSON Web Token* dapat melakukan enkripsi pada klaim yang berisikan data penyerang oleh *bot*, sehingga *bot* admin server dapat mengamankan klaim yang akan dikirimkan ke admin server.

Kata Kunci: Keamanan, Jaringan, Server, Administrator, *Monitoring*, *Distributed Denial of Service*, *Bot*, *UDP Flooding*, *SYN Flooding*, *JSON Web Token*.

***BOT DESIGN FOR SERVER MONITORING FROM
DISTRIBUTED DENIAL OF SERVICE ATTACKS USING JSON
WEB TOKEN***

ARIF MAULANA RAHMAN

ABSTRACT

In running a server, a monitoring system is needed to secure the network in order to minimize the risk if an intrusion attempt occurs. One of the attacks that often occurs to servers is a DDOS (Distributed Denial of Service) attack which results in the system being attacked experiencing interference in the form of error requests, halt, system failure and so on. Based on the problems described, a bot is needed to monitor and protect the server from DDOS attacks, in this study the focus is on DDOS attacks of the UDP Flooding and SYN Flooding types. This bot will be able to detect UDP Flooding and SYN Flooding attacks by limiting the number of packets addressed to the port opened by the server, if the bot detects an attack the bot will block and send notifications to the server admin by implementing push notification sets and using JSON Web Tokens to ensure The integrity and confidentiality of notifications sent by the bot to the server admin smartphone are maintained. Server monitoring makes use of bot to detect DDOS attacks of the UDP Flooding and SYN Flooding types by limiting the number of packets sent to the port opened by the server, if the number of packets sent is more than 100 packets per second, the bot will identify the sending as an attack. The application of the JSON Web Token method so that it can be operated by the server admin bot, namely by implementing the JSON Web Token package on the bot and then calling the encode function so that the JSON Web Token can encrypt claims containing attacker data by bot, so that the admin server bot can secure claims that will sent to the server admin.

Keywords: *Security, Network, Server, Administrator, Monitoring, Distributed Denial of Service, Bot, UDP Flooding, SYN Flooding, JSON Web Token.*

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini yang berjudul “Perancangan Bot Untuk *Monitoring* Server Dari Serangan *Distributed Denial of Service* Menggunakan *JSON Web Token*”. Penulis juga ingin mengucapkan terima kasih kepada:

1. Kedua orang tua dari penulis yakni Asman dan Sri Endang Lestari, yang kerap memberikan dukungan serta doa yang tiada hentinya kepada penulis dalam menyelesaikan skripsi ini.
2. Bapak Henki Bayu Seta, S.Kom., M.TI. dan Ibu Ria Astriratma, S. Komp., M.Cs., selaku dosen pembimbing yang telah memberikan saran serta mendorong penulis dalam menyelesaikan skripsi ini.
3. Ibu Dr. Ermatita, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.
4. Ibu Anita Muliawati, S.Kom, MTL., selaku Ketua Jurusan Informatika Universitas Pembangunan Nasional Veteran Jakarta.
5. Teman-teman angkatan 2016 Fakultas Ilmu Komputer Universitas Pembangunan Nasional Veteran Jakarta.

Jakarta, 29 Mei 2020

Penulis,



(Arif Maulana Rahman)

DAFTAR ISI

HALAMAN JUDUL	i
PERNYATAAN ORISINALITAS.....	ii
PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS.....	iii
LEMBAR PENGESAHAN.....	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
DAFTAR SIMBOL	xiv
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.5 Ruang Lingkup	3
1.6 Luaran Yang Diharapkan	4
1.7 Sistematika Penelitian.....	4
BAB 2 LANDASAN TEORI	6
2.1. Definisi Robot (<i>Bot</i>).....	6
2.2. Web.....	6
2.3. <i>Web Service</i>	8
2.3.1. <i>Komponen Web Service</i>	9
2.3.2. <i>JSON Web Token (JWT)</i>	10
2.4. Struktur <i>JSON</i>	11
2.4.1. <i>Parser</i>	12
2.5. Algoritma <i>HMAC</i>	12
2.6. Algoritma <i>SHA256</i>	14
2.7. Sistem <i>Monitoring</i>	15
2.7.1 Tujuan Sistem <i>Monitoring</i>	16

2.8.	<i>DOS (Denial of Service) dan DDOS (Distributed Denial of Service)</i>	16
2.7.1.	<i>DOS (Denial of Service)</i>	17
2.7.2.	<i>DDOS (Distributed Denial of Service)</i>	17
2.9.	<i>PHP</i>	18
2.10.	<i>Framework</i>	18
2.11.	<i>Codeigniter</i>	20
2.12.	<i>Basis Data (Database)</i>	21
2.13.	<i>MySQL</i>	22
2.14.	<i>Black Box Testing</i>	23
2.15.	<i>Flowchart</i>	23
2.16.	<i>IPTables</i>	25
2.17.	<i>Python</i>	29
2.18.	<i>Netstat</i>	29
2.19.	<i>Penelitian Terkait</i>	29
BAB 3 METODOLOGI PENELITIAN		34
3.1.	<i>Tahapan Penelitian</i>	34
3.1.1.	<i>Identifikasi Masalah</i>	35
3.1.2.	<i>Studi Literatur</i>	35
3.1.3.	<i>Analisa Kebutuhan Sistem</i>	35
3.1.4.	<i>Perancangan Sistem</i>	35
3.1.5.	<i>Pengujian Sistem</i>	39
3.1.6.	<i>Pembuatan Laporan</i>	39
3.2.	<i>Jadwal Penelitian</i>	40
BAB 4 HASIL DAN PEMBAHASAN		41
4.1.	<i>Analisa Sistem</i>	41
4.1.1.	<i>Analisa Sistem Monitoring</i>	41
4.1.2.	<i>Analisa Penerapan JSON Web Token pada bot</i>	43
4.1.3.	<i>Analisa Rules pada IPTables</i>	45
4.2.	<i>Pengujian Sistem</i>	45
4.2.1.	<i>Pengujian Bot Sistem Monitoring Sebelum Adanya Serangan</i>	46
4.2.2.	<i>Pengujian Serangan DDOS Menggunakan Slowloris</i>	46

4.2.3.	Pengujian <i>Bot</i> Sistem <i>Monitoring</i> Saat Adanya Serangan.....	47
4.2.4.	Pengujian Kecepatan Sistem Dari Deteksi Hingga Notifikasi	49
4.3	Analisa Hasil Pengujian.....	50
BAB 5 PENUTUP		51
5.1.	Kesimpulan.....	51
5.2.	Saran	51
DAFTAR PUSTAKA		52
RIWAYAT HIDUP		54
LAMPIRAN		55
	Lampiran 1 Kode Program	56
	Lampiran 2 Konfigurasi Ubuntu.....	58
	Lampiran 3 Konfigurasi <i>Python</i>	59
	Lampiran 4 Konfigurasi <i>IPTables</i> dan <i>Rules</i>	60
	Lampiran 5 Konfigurasi <i>Pip Python3</i>	64
	Lampiran 6 Konfigurasi <i>Setup autorun Python Script</i>	65
	Lampiran 7 Tabel Hasil Pengukuran.....	69
	Lampiran 8 Hasil Turnitin	70

DAFTAR GAMBAR


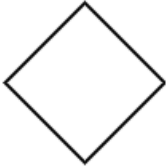
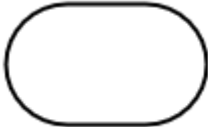


Gambar 1. Cara Kerja Web Yang Diakses.....	7
Gambar 2. <i>JSON Web Token</i> Proses.....	10
Gambar 3. <i>JWT Header</i>	10
Gambar 4. <i>JWT Payload</i>	11
Gambar 5. <i>JWT Signature</i>	11
Gambar 6. Diagram Algoritma <i>HMAC</i>	13
Gambar 7. Blok diagram perintah <i>IPTables</i>	26
Gambar 8. <i>Flowchart</i> Tahapan Penelitian	34
Gambar 9. Rancangan <i>Monitoring</i> Server	36
Gambar 10. <i>Flowchart</i> Set <i>Push Notification Bot Token</i>	37
Gambar 11. <i>Flowchart</i> Program <i>Bot</i>	38
Gambar 12. Penerapan <i>JWT</i> Pada Sistem	39
Gambar 13. Rancangan Sistem <i>Monitoring</i>	41
Gambar 14. <i>Flowchart</i> Cara Kerja <i>Bot</i>	42
Gambar 15. <i>Package JWT</i>	43
Gambar 16. <i>Secret Key</i> dan <i>Push Notification</i> Server	43
Gambar 17. Memanggil fungsi <i>encode JWT</i> pada <i>bot</i>	44
Gambar 18. Token Pada <i>JSON Web Token</i>	44
Gambar 19. <i>Rules</i> pada <i>IPTables</i>	45
Gambar 20. <i>Bot Monitoring</i> Server	46
Gambar 21. Serangan <i>DDOS</i> Menggunakan <i>Slowloris</i>	46
Gambar 22. <i>Bot</i> Mendeteksi dan Memblokir Serangan.....	47
Gambar 23. <i>IP</i> Penyerang Terdaftar Dalam <i>Blacklist IPTables Chain Input</i>	47
Gambar 24. Notifikasi Terdeksinya Serangan	48

Gambar 25. Hasil Pengukuran Kecepatan Sistem	49
Gambar 26. Instalasi Ubuntu.....	57

DAFTAR TABEL

Tabel 1. Tabel Keterangan Diagram Algoritma <i>HMAC</i>	13
Tabel 2. Simbol <i>Flowchart</i>	24
Tabel 3. Perintah <i>IPTables</i>	27
Tabel 4. Tabel Jadwal Penelitian.....	40
Tabel 5. Hasil Serangan	49
Tabel 6. Tabel Hasil Pengukuran.....	68

DAFTAR SIMBOL

Simbol	Nama Simbol	Keterangan
	Simbol Proses	Menggambarkan Proses
	Simbol Keputusan	Menggambarkan keputusan berdasarkan kondisi yang diberikan
	Simbol Terminator	Simbol untuk permulaan atau akhir sebuah kegiatan
	Simbol Fungsi	Simbol yang menandakan implementasi fungsi
	Simbol Arus Program	Sebagai petunjuk arus proses pada program