

**PERANCANGAN SISTEM MONITORING DAN  
PENCEGAHAN SERANGAN *BRUTE FORCE*  
PADA MIKROTIK BERBASIS  
*BOT* TELEGRAM**

**SKRIPSI**



Disusun Oleh

**RADITYO AJI ARIESTYA**

**16.11.0132**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
2020**

**PERANCANGAN SISTEM MONITORING DAN  
PENCEGAHAN SERANGAN *BRUTE FORCE*  
PADA MIKROTIK BERBASIS  
*BOT* TELEGRAM**

**SKRIPSI**

untuk memenuhi persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



Disusun Oleh

**RADITYO AJI ARIESTYA**

**16.11.0132**

**PROGRAM SARJANA  
PROGRAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
2020**

**PERSETUJUAN**

**SKRIPSI**

**PERANCANGAN SISTEM MONITORING DAN  
PENCEGAHAN SERANGAN *BRUTE FORCE* PADA  
MIKROTIK BERBASIS *BOT* TELEGRAM**

yang dipersiapkan dan disusun oleh

**Radityo Aji Ariestya**

**16.11.0132**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal 20 Februari 2020

**Dosen Pembimbing,**

**Sudarmawan, S.T., M.T.**

**NIK. 190302035**

# PENGESAHAN

## SKRIPSI

### PERANCANGAN SISTEM MONITORING DAN PENCEGAHAN SERANGAN *BRUTE FORCE* PADA MIKROTIK BERBASIS *BOT* TELEGRAM

yang disusun oleh

**Radityo Aji Ariestya**

**16.11.0132**

telah dipertahankan di depan Dewan Penguji  
pada tanggal 19 Maret 2020

#### Susunan Dewan Penguji

**Nama Penguji**

**Tanda Tangan**

**Andika Agus Slameto, M.Kom**

**NIK. 190302109**

**Ferry Wahyu Wibowo, S.Si, M.Cs**

**NIK. 190302235**

**Sudarmawan, S.T., M.T.**

**NIK. 190302035**

Skripsi ini telah diterima sebagai salah satu persyaratan  
untuk memperoleh gelar Sarjana Komputer  
Tanggal 19 September 2020

**Dekan Fakultas Ilmu Komputer**

**Krisnawati, S.Si, M.T.**

**NIK. 190302038**

## PERNYATAAN

### PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 19 Agustus 2020



RADITYO AJI ARIESTYA  
NIM. 16.11.0132

## MOTO

*“Berjalan tak seperti rencana adalah hal yang biasa , dan jalan terbaik adalah jalani sebaik yang kita bisa”*

(GAS! - FSTVLST)

*“Hidup tanpa permasalahan seperti halnya kita tidak hidup , jalani semua satu persatu , santai ”*

(RADITYO AJI ARIESTYA)



## PERSEMBAHAN

Dengan mengucapkan Alhamdulillah sebagai rasa syukur kepada Allah Subhanahu wa Ta'ala atas segala nikmat dan karuniaNya sehingga skripsi ini bisa terselesaikan.

Pada kesempatan ini tak lupa penulis ucapkan terimakasih kepada:

1. Allah SWT, karena berkat izin-Nya dan karunia-Nya skripsi ini dapat terselesaikan.
2. Bapak Aries dan Ibu Lisa yang telah memberikan doa, motivasi, semangat, kasih, sayang dan pengorbanan yang telah diberikan.
3. Vidya Talisa Ariestya dan Natasya Sekar Ariestya saudara perempuan penulis yang telah memberikan dukungan semangat.
4. Bapak Sudarmawan, M.T sebagai dosen pembimbing yang telah mencurahkan waktu untuk membimbing perjalanan penyusunan skripsi ini dari awal hingga akhir.
5. Putri Rachma Novianti partner yang selama ini selalu memberikan dukungan, mendengarkan setiap keluh kesah yang dialami dalam menyusun skripsi ini sampai selesai.
6. Dede Feryando teman seperjuangan penulis dalam menyelesaikan skripsi yang selalu memberikan dukungan.
7. Teman-teman kelas S1-IF-02 dan Geng Liyud yang telah menemani masa perkuliahan di Universitas Amikom Yogyakarta.
8. Dan teman-teman saya yang tidak bisa saya tulis satu persatu, saya ucapkan banyak terimakasih.

## KATA PENGANTAR

Puji syukur peneliti panjatkan kehadiran Allah SWT yang selalu melimpahkan rahmat dan karunia-nya kepada setiap hamba-nya dan tak lupa shalawat serta salam kepada junjungan Nabi besar kita, Nabi Muhammad SAW.

Skripsi ini dibuat sebagai salah satu syarat kelulusan Program Strata-1 Jurusan Informatika Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi yang telah dibuat, peneliti mengucapkan terimakasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Rektor UNIVERSITAS AMIKOM YOGYAKARTA.
2. Ibu Krisnawati, S.Si., M.T, selaku Dekan Fakultas Ilmu Komputer UNIVERSITAS AMIKOM YOGYAKARTA.
3. Bapak Sudarmawan, S.T., M.T. selaku Ketua Program Studi Informatika fakultas Ilmu Komputer Universitas Amikom Yogyakarta dan sekaligus dosen pembimbing yang telah memberikan bimbingan dan ilmu yang bermanfaat kepada penulis selama melakukan bimbingan skripsi.
4. Segenap dosen Universitas Amikom Yogyakarta yang telah memberikan pengajaran ilmu-ilmu baru selama masa perkuliahan.
5. Bapak Aries Budiyanto, S.E., Ibu Erlisa Rafiyanti, A.Md., Vidya Talisa Ariesty, S.Tr. Natasya Sekar Ariesty dan semua keluarga tercinta yang telah begitu tulus memberikan semangat, dorongan dan doa yang bermanfaat bagi penulis.



6. Putri Rachma Novianti, S.Ikom. yang selama ini selalu menemani dan selalu memberikan semangat untuk menyusun dan menyelesaikan skripsi ini.
7. Teman – teman kelas 16-S1IF-02 dan Geng Liyud yang telah berjuang bersama selama masa perkuliahan hingga sampai saat ini.
8. Keluarga , teman-teman dimanapun berada dan semua pihak yang telah membantu dan senantiasa mendukung dalam penyelesaian skripsi ini yang tidak dapat disebutkan satu persatu.

Dalam penulisan skripsi ini penulis menyadari sepenuhnya akan kekurangan karena keterbatasan pengetahuan dan kemampuan penulis. Oleh karena itu saran dan kritik yang membangun senantiasa diharapkan demi menyempurnakan hasil penelitian ini.

Akhir kata semoga skripsi ini dapat memberikan manfaat bagi pembaca umumnya dan khususnya untuk penulis serta untuk pengembangan sistem monitoring dan pencegahan serangan jaringan berikutnya.

Yogyakarta, 20 Agustus 2020

Penulis,

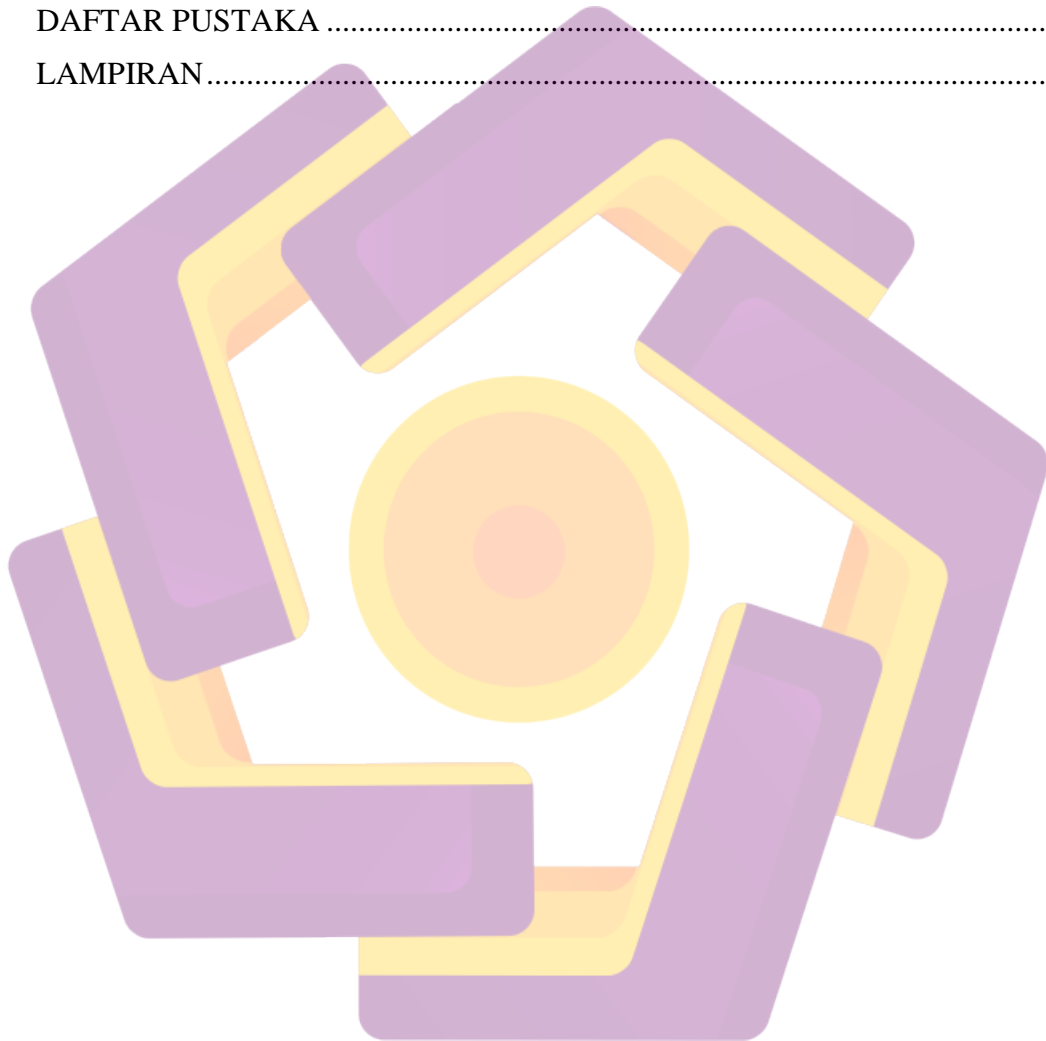
Radityo Aji Ariestya

## DAFTAR ISI

JUDUL.....	i
PERSETUJUAN .....	ii
PENGESAHAN .....	iii
PERNYATAAN.....	iv
MOTO.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR .....	xiii
INTISARI.....	xvi
ABSTRACT.....	xvii
BAB I.....	1
PENDAHULUAN .....	1
1.1 Latar Belakang .....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
1.6 Alur Penelitian.....	4
1.6.1 Pengumpulan Data .....	4
1.6.2 Analisis dan Perencanaan.....	5
1.6.3 Implementasi dan Pengujian .....	5
1.6.4 Penulisan Laporan.....	5
1.7 Sistematika Penulisan.....	6
BAB II.....	8
TINJAUAN PUSTAKA DAN LANDASAN TEORI.....	8
2.1 Tinjauan Pustaka .....	8
2.2 Landasan Teori .....	11
2.2.1 Jaringan Komputer .....	11

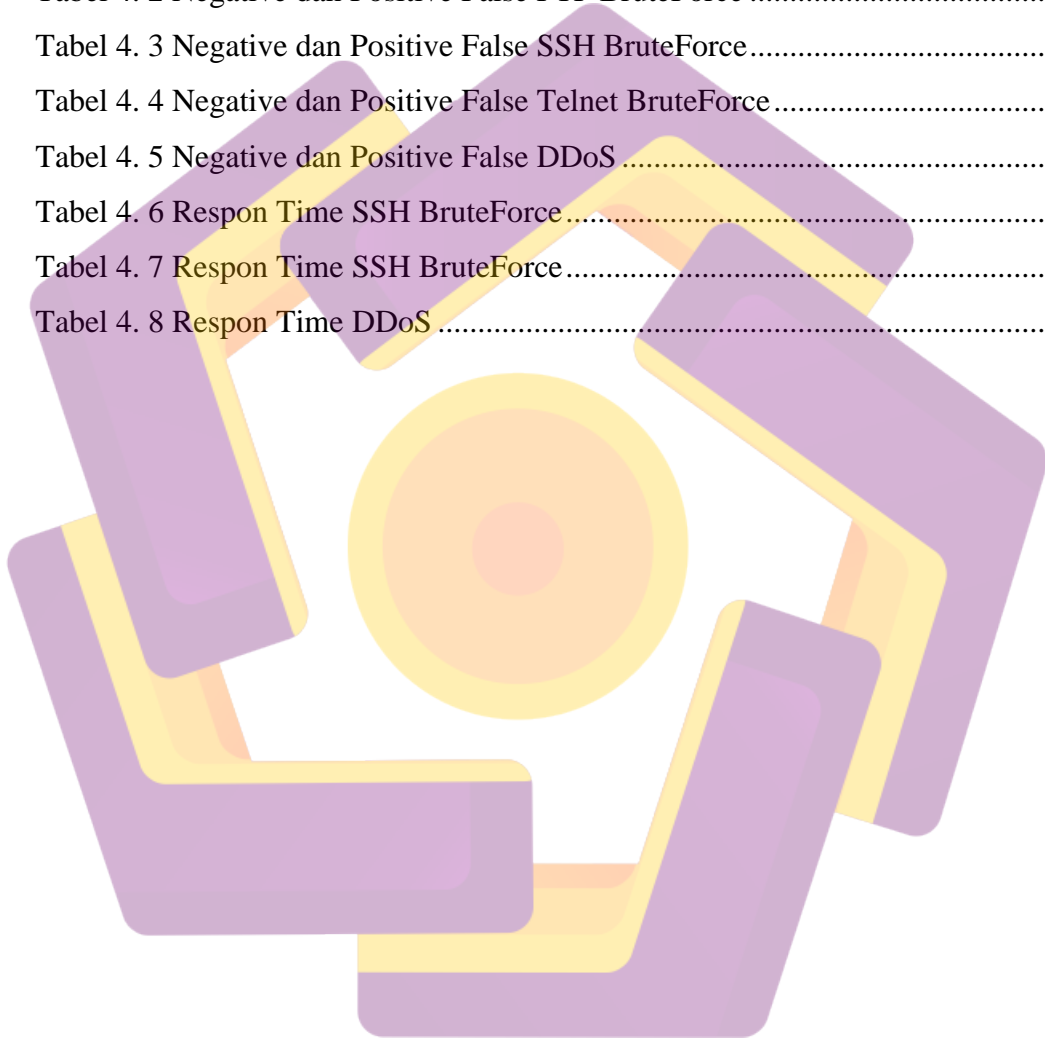
2.2.2	Jenis Jaringan Komputer .....	11
2.2.3	Media Transmisi Jaringan .....	12
2.2.4	MikroTik .....	13
2.2.5	Keamanan Jaringan .....	15
2.2.6	Konsep Keamanan Jaringan .....	16
2.2.7	Tujuan Keamanan Jaringan .....	17
2.2.8	Serangan Pada Jaringan Komputer .....	18
2.2.9	<i>Brute Forces</i> .....	21
2.2.10	<i>Intrusion Detection System</i> dan <i>Intrusion Prevention System</i> .....	21
2.2.11	Sistem Monitoring Jaringan Komputer .....	23
2.2.12	<i>Bot ( Robot )</i> .....	25
2.2.13	Telegram .....	25
2.3	Metode Pengujian .....	26
2.3.1	Black Box Testing .....	26
2.3.2	Negative dan Positive False .....	26
BAB III .....		27
PERANCANGAN PENELITIAN .....		27
3.1	Gambaran Umum .....	27
3.1.1	Desain Topologi Jaringan .....	28
3.2	Perangkat Penelitian .....	30
3.2.1	Perangkat Keras ( <i>Hardware</i> ) .....	30
3.2.2	Perangkat Lunak ( <i>Software</i> ) .....	32
3.3	Langkah Penelitian .....	33
3.3.1	Instalasi <i>Hardware</i> dan <i>Software</i> .....	34
3.3.2	Konfigurasi .....	36
3.3.3	Skenario Pengujian .....	62
3.4	Parameter Pengukuran .....	65
BAB IV .....		66
HASIL DAN PEMBAHASAN .....		66
4.1	Hasil Pengujian Serangan dan Notifikasi Telegram .....	66
4.1.1	FTP Brute Forces .....	66
4.1.2	SSH/Telnet Brute Forces .....	72
4.1.3	DDoS Attack .....	79
4.2	Hasil Pengujian .....	82

4.2.1	Pengujian <i>Black Box</i> ( <i>Firewall Rule</i> ).....	82
4.2.2	Pengujian <i>Negative</i> dan <i>Positive False</i> .....	83
4.2.3	Pengujian Respon Time Firewall Rule ( <i>IDS/IPS</i> ).....	85
BAB V.....		88
PENUTUP.....		88
5.1	Kesimpulan.....	88
5.3	Penutup.....	89
DAFTAR PUSTAKA .....		90
LAMPIRAN.....		91



## DAFTAR TABEL

Tabel 2. 1 Perbandingan Penelitian.....	9
Tabel 3. 1 Tabel IP .....	29
Tabel 3. 2 Kebutuhan Perangkat Keras (Hardware) .....	31
Tabel 4. 1 BlackBox Testing.....	82
Tabel 4. 2 Negative dan Positive False FTP BruteForce .....	83
Tabel 4. 3 Negative dan Positive False SSH BruteForce.....	83
Tabel 4. 4 Negative dan Positive False Telnet BruteForce.....	84
Tabel 4. 5 Negative dan Positive False DDoS .....	84
Tabel 4. 6 Respon Time SSH BruteForce.....	85
Tabel 4. 7 Respon Time SSH BruteForce.....	85
Tabel 4. 8 Respon Time DDoS .....	86

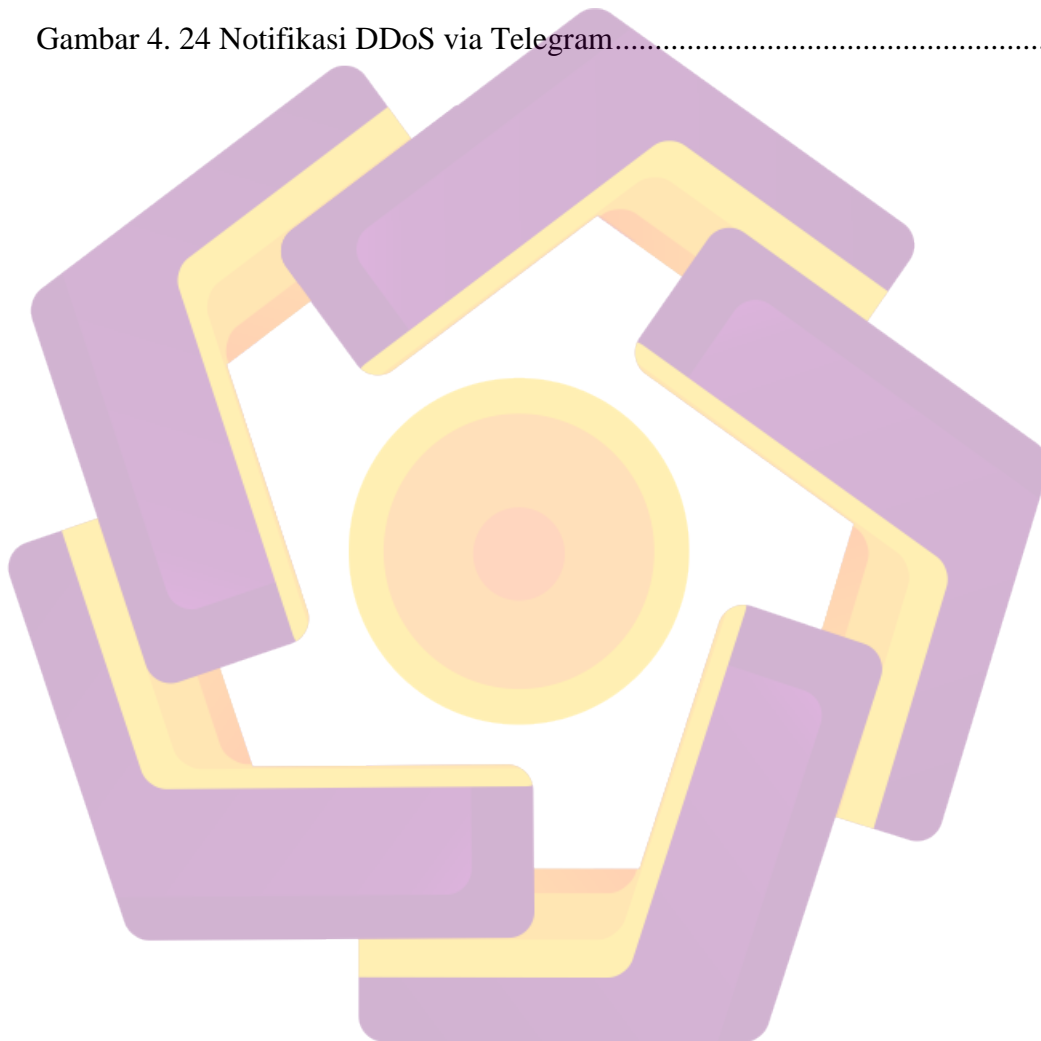


## DAFTAR GAMBAR

Gambar 2. 1 Router MikroTik .....	13
Gambar 2. 2 Penerapan IDS dan IPS .....	22
Gambar 2. 3 Logo Aplikasi Telegram.....	25
Gambar 2. 4 Black Box Testing .....	26
Gambar 3. 1 Topologi Jaringan.....	28
Gambar 3. 2 Alur Pengujian.....	33
Gambar 3. 3 Halaman awal MikroTik .....	36
Gambar 3. 4 MAC address MikroTik .....	36
Gambar 3. 5 Halaman menu winbox.....	37
Gambar 3. 6 3.6 Set username baru .....	37
Gambar 3. 7 Set password.....	38
Gambar 3. 8 Dhcp client .....	38
Gambar 3. 9 Dhcp client status .....	39
Gambar 3. 10 IP address ether1 .....	39
Gambar 3. 11 Konfigurasi ip ether2.....	40
Gambar 3. 12 Setting DNS perangkat MikroTik .....	40
Gambar 3. 13 Ip pada PC admin .....	41
Gambar 3. 14 Ping test dari winbox.....	41
Gambar 3. 15 Ping test dari PC admin.....	42
Gambar 3. 16 Enable wlan interface .....	42
Gambar 3. 17 Konfigurasi wlan1 .....	43
Gambar 3. 18 Setting ip wlan1 .....	44
Gambar 3. 19 Halaman DHCP server .....	44
Gambar 3. 20 DHCP server set interface .....	45
Gambar 3. 21 DHCP addresses space .....	45
Gambar 3. 22 DHCP gateway wlan1 .....	45
Gambar 3. 23 DHCP lease time .....	46
Gambar 3. 24 DHCP server sukses .....	46
Gambar 3. 25 Terminal Rule SSH dan Telnet .....	48
Gambar 3. 26 Filter Rules SSH dan Telnet.....	48

Gambar 3. 27 Action Filter Rule SSH dan Telnet .....	49
Gambar 3. 28 Terminal Rule FTP .....	50
Gambar 3. 29 Filter Rules FTP .....	51
Gambar 3. 30 Action Filter Rule FTP .....	51
Gambar 3. 31 Terminal Rule DDOS .....	53
Gambar 3. 32 Filter Rules DDOS .....	53
Gambar 3. 33 Action Filter Rule DDOS .....	54
Gambar 3. 34 Atur Nama dan Interval Scheduler .....	55
Gambar 3. 35 Script On Event .....	58
Gambar 3. 36 Token API bot Telegram .....	59
Gambar 3. 37 Chat ID Bot Telegram .....	59
Gambar 3. 38 Clone Tool Hydra Dari GitHub .....	60
Gambar 3. 39 Command eksekusi Mkrutus .....	60
Gambar 3. 40 Proses Eksekusi Hydra .....	61
Gambar 3. 41 Bot berhasil .....	62
Gambar 3. 42 Skenario Pengujian .....	64
Gambar 4. 1 Nmap Hydra .....	67
Gambar 4. 2 FTP Berhasil Melalui Hydra .....	67
Gambar 4. 3 Hydra Gagal Brute Force FTP .....	68
Gambar 4. 4 Notifikasi FTP via Telegram .....	69
Gambar 4. 5 Address List Blokir FTP .....	69
Gambar 4. 6 Tampilan Filezilla .....	70
Gambar 4. 7 Filezilla Gagal Terkoneksi .....	71
Gambar 4. 8 FTP Address List Filezilla .....	71
Gambar 4. 9 Notifikasi FTP Filezilla .....	72
Gambar 4. 10 Nmap Hydra .....	73
Gambar 4. 11 Telnet Berhasil Melalui Hydra .....	73
Gambar 4. 12 Hydra Gagal Brute Force Telnet dan SSH .....	74
Gambar 4. 13 Notifikasi SSH Telnet via Telegram .....	75
Gambar 4. 14 Address List Blokir SSH Telnet .....	75
Gambar 4. 15 Halaman Konfigurasi Putty .....	76
Gambar 4. 16 Percobaan SSH Putty .....	77

Gambar 4. 17 Akses Putty Diblokir .....	77
Gambar 4. 18 Address List SSH Putty.....	78
Gambar 4. 19 Notifikasi SSH Putty ke Telegram .....	78
Gambar 4. 20 Perintah DDoS Hping3 .....	79
Gambar 4. 21 Proses DDoS .....	80
Gambar 4. 22 MikroTik Winbox Logout.....	80
Gambar 4. 23 Address List DDoS .....	81
Gambar 4. 24 Notifikasi DDoS via Telegram.....	81





## INTISARI

Perkembangan teknologi internet saat ini dapat dibuktikan dengan semakin pesat berkembangnya dan banyaknya berbagai situs di internet. Hingga saat ini perkembangan internet tidak luput dari berbagai macam serangan pada jaringan komputer. Sistem yang dapat mendeteksi serangan pada jaringan komputer umumnya hanya bisa mendeteksi berbagai jenis serangan tetapi tidak bisa mengambil tindakan yang lebih lanjut. Dengan pembuatan otomatisasi pencegahan (Intrusion Prevention System) yang bagus pencegahan dalam serangan dapat dilakukan dengan cepat.

Pembuatan sistem notifikasi jika terjadi serangan bruteforce pada jaringan komputer ini menggunakan bot telegram sebagai pendukung notifikasi dan mengaplikasikan pada jaringan nirkabel MikroTik dengan menggunakan beberapa parameter rule firewall, scheduler, dan script.

Dari hasil pengujian dapat disimpulkan jika sistem mengirim notifikasi ke telegram untuk dapat mengetahui informasi pada interval waktu yang sudah ditentukan jika terjadi serangan pada jaringan MikroTik. Dan Pengiriman notifikasi pada jaringan ini tergantung pada interval scheduler, dan di saat bersamaan IPS (Intrusion Prevention System) yang sudah terkonfigurasi dalam perangkat MikroTik akan melakukan aksi melacak dan memblokir ip address penyerang .

**Kata Kunci :** *MikroTik , monitoring , IDS/IPS , jaringan internet*

## **ABSTRACT**

*The development of internet technology today can be proven by the rapid development and number of various sites on the internet. Until now, the development of the internet has not been spared from various kinds of attacks on computer networks. Systems that can detect attacks on computer networks generally can only detect various types of attacks but cannot take further action.*

*With the creation of a good prevention automation (Intrusion Prevention System) prevention in attacks can be done quickly. Making a notification system in the event of a bruteforce attack on this computer network uses a telegram bot as notification support and applies it to a MikroTik wireless network using several parameters of firewall rule, scheduler, and script.*

*From the test results, it can be concluded that the system sends notifications to telegram to be able to find out information at predetermined time intervals in the event of an attack on the MikroTik network. And sending notifications on this network depends on the scheduler interval, and at the same time the IPS (Intrusion Prevention System) that has been configured in the MikroTik device will take action to track and block the attacker's IP address.*

**Keywords:** Mikrotik, monitoring, IDS/IPS, network

