

SKRIPSI
IMPLEMENTASI SISTEM KEAMANAN JARINGAN
DENGAN DETEKSI SERANGAN DENIAL OF SERVICE
DAN BRUTE-FORCE PADA ROUTER MIKROTIK
DENGAN NOTIFIKASI MELALUI WHATSAPP



NANDA HERNAWATI

NIM : 195410217

PROGRAM STUDI INFORMATIKA
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
2024

SKRIPSI
IMPLEMENTASI SISTEM KEAMANAN JARINGAN
DENGAN DETEKSI SERANGAN DENIAL OF SERVICE
DAN BRUTE-FORCE PADA ROUTER MIKROTIK
DENGAN NOTIFIKASI MELALUI WHATSAPP

Diajukan sebagai salah satu syarat untuk menyelesaikan studi jenjang Sarjana
(S1)

Program Studi Informatika

Universitas Teknologi Digital Indonesia
Yogyakarta

Disusun Oleh

NANDA HERNAWATI

NIM : 195410217

PROGRAM STUDI INFORMATIKA
PROGRAM SARJANA
FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS TEKNOLOGI DIGITAL INDONESIA
2024

LEMBAR PERSETUJUAN

Judul : Implementasi Sistem Keamanan Jaringan dengan Deteksi Serangan Denial of Service dan Brute-Force pada Router MikroTik dengan Notifikasi melalui WhatsApp

Nama : Nanda Hernawati

NIM : 195410217

Jurusan : Informatika

Semester : 10 (Sepuluh)

Telah diperiksa dan disetujui

Yogyakarta, Mei 2024

Dosen Pembimbing,



(Wagito, S.T., M.T.)

LAMAN PENGESAHAN

SKRIPSI




IMPLEMENTASI SISTEM KEAMANAN JARINGAN DENGAN DETEKSI SERANGAN DENIAL OF SERVICE DAN BRUTE-FORCE PADA ROUTER MIKROTIK DENGAN NOTIFIKASI MELALUI WHATSAPP

Telah dipertahankan di depan Dewan Penguji Skripsi dan Dinyatakan diterima
untuk memenuhi sebagai syarat guna memperoleh Gelar Sarjana Komputer
Universitas Teknologi Digital Indonesia Yogyakarta

Yogyakarta, Mei 2024

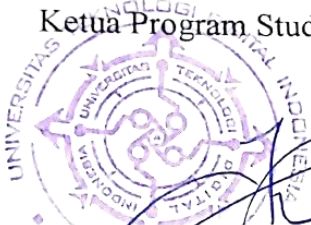

Mengesahkan

1. Wagito, S.T., M.T.
NIDN : 0522126901
2. L. N. Harnaningrum, S. Si., M.T.
NIDN : 0513057101
3. Danny Kriestanto, S.Kom., M.Eng.
NIDN : 0503068002


.....

.....

.....

Mengetahui

Ketua Program Studi Informatika



Dini Fakta Sari, S.T., M.T.
NIDN : 0507108401

PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa naskah skripsi ini belum pernah diajukan untuk memperoleh gelar Sarjana Komputer di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara sah diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, Mei 2024



Nanda Hernawati

NIM : 195410217

HALAMAN PERSEMBAHAN

Alhamdulillah hirabbil 'alamin dengan rasa syukur penulis menyampaikan kata pengantar ini sebagai bentuk pengesahan penyelesaian skripsi yang berjudul " Implementasi Sistem Keamanan Jaringan Dengan Deteksi Serangan *Denial of Service* dan *Brute-Force* Pada Router MikroTik Dengan Notifikasi Melalui Whatsapp ". Skripsi ini diajukan untuk memenuhi salah satu syarat untuk memperoleh gelar Sarjana Pendidikan Jurusan Informatika Universitas Teknologi Digital Indonesia.

Segala upaya yang telah dilakukan tidak terlepas dari dukungan, bimbingan, serta arahan dari berbagai pihak yang dengan ikhlas memberikan kontribusi dalam penulisan skripsi ini. Oleh karena itu, dengan rendah hati penulis mengucapkan terima kasih kepada:

1. Allah Subhanahu wa ta'ala atas waktu, kesempatan, kesabaran dan anugerah kepada penulis sehingga penulis dapat menyelesaikan skripsi dengan sebaik mungkin.
2. Kedua orang tua saya, Bapak Sarju dan Ibu Prihatin atas kasih sayang, perhatian, dukungan, serta doa yang terbaik untuk penulis.

3. Kedua kakak saya, Mas Hermawan dan Mbak Aulia Urrahamani atas kasih sayang, perhatian, dukungan, serta doa untuk penulis.
4. Keponakan dan adik-adik saya yang menjadi penyemangat penulis.
5. Sahabat dan teman hidup saya yang telah banyak membantu dan memberikan dukungan kepada penulis.
6. Dosen pembimbing dan seluruh dosen penguji saya yang telah memberikan masukan dan arahan kepada penulis.
7. Seluruh pihak yang terlibat dalam penulisan skripsi ini.

MOTTO

“ Kamu punya Allah ”

“ And if it's not enough, If it's not enough. Try again and again.

Over and over again “

- Avenged Sevenfold

“ Kalau tiga kali tidak bisa yang keempat pasti bisa “

- Pahlawan Bertopeng

“ Kami harus sekolah karena kami perlu belajar lebih banyak untuk menemukan pekerjaan yang memenuhi jiwa kami agar kami tidak sia-siakan hidup karena mengejar uang dan membeli barang tidak berguna untuk mengisi

lubang dari ketakutan diri kami “

- Gumball Watterson

“ hehehe hehe hehe hehe “

- Gojo Satoru

KATA PENGANTAR

Dengan nama Allah Yang Maha Pengasih dan Maha Penyayang, segala puji hanya bagi-Nya yang telah memberikan petunjuk dan kekuatan dalam perjalanan penulisan skripsi dengan judul "Implementasi Sistem Keamanan Jaringan Dengan Deteksi Serangan *DoS (Denial of Service)* dan *Brute-Force* Pada Router MikroTik Dengan Notifikasi Melalui Whatsapp" ini.

Latar belakang penelitian membahas kompleksitas keamanan jaringan, terutama rentannya router terhadap serangan *cyber* seperti *DoS (Denial of Service)* dan *Brute-Force*. Dalam konteks ini, skripsi ini berusaha menggali Solusi keamanan jaringan dengan mengintegrasikan teknologi seperti *firewall*, *IDS (Intrusion Detection System)* dan pemanfaatan platform pesan seperti *WhatsApp*.

Proses penulisan skripsi ini melibatkan perjalanan panjang yang penuh dedikasi, tantangan, dan pembelajaran. Oleh karena itu, penulis ingin menyampaikan rasa terima kasih kepada Allah SWT atas rahmat dan petunjuk-Nya, kepada keluarga tercinta atas dukungan dan doa mereka, serta kepada pembimbing, teman-teman, dan semua pihak yang telah memberikan kontribusi dalam berbagai bentuk.

Semoga skripsi ini dapat memberikan kontribusi kecil terhadap pemahaman kita akan pentingnya peran pendidikan pada anak usia dini dan sekaligus memberikan wawasan terkait keamanan jaringan di era digital ini.

Akhir kata, penulis menyadari bahwa skripsi ini tidak sempurna. Oleh karena itu, kritik, saran, dan masukan dari pembaca sangat penulis harapkan untuk perbaikan di masa mendatang. Terima kasih atas segala dukungan, doa, dan kesempatan yang diberikan.

Yogyakarta, Mei 2024

Nanda Hernawati

DAFTAR ISI

	Hal
Halaman Cover.....	i
Halaman Judul.....	ii
Halaman Persetujuan.....	iii
Halaman Pengesahan	iv
Pernyataan Keaslian Skripsi.....	v
Halaman Persembahan	vi
Halaman Motto.....	viii
Kata Pengantar	ix
Daftar Isi.....	x
Daftar Gambar.....	xiii
Daftar Tabel	xv
Daftar Lampiran	xvi
Intisari	xvii
Abstract	xviii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan masalah.....	3
1.3 Ruang lingkup	4
1.4 Tujuan penelitian.....	4
1.5 Manfaat Penelitian	5
1.6 Sistematika Penulisan	5
BAB II TINJAUAN PUSTAKA DAN DASAR TEORI.....	8
2.1 Tinjauan Pustaka	8
2.2 Dasar Teori.....	10
2.2.1 Jaringan Komputer	10
2.2.2 Sistem Keamanan Jaringan	11
2.2.3 Firewall	11
2.2.4 MikroTik RouterBOARD	13
2.2.5 Denial of Service.....	13

2.2.6	Brute-Force	16
2.2.7	Intrusion Detection System	17
2.2.8	WhatsApp.....	19
2.2.9	Twilio	20
BAB III	METODE PENELITIAN.....	22
3.1	Analisis Kebutuhan	22
3.1.1	Kebutuhan Data Masukan	22
3.1.2	Kebutuhan Data Keluaran	22
3.1.3	Kebutuhan Perangkat Keras	23
3.1.4	Kebutuhan Perangkat Lunak	24
3.2	Prosedur dan Pengumpulan Data	24
3.3	Perancangan Sistem	25
3.3.1	Diagram Blok	25
3.3.2	Topologi Jaringan.....	26
3.3.3	Flowchart	28
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	34
4.1	Implementasi dan Pengujian Pengamanan.....	34
4.1.1	Konfigurasi Jaringan	34
4.1.2	Monitoring Jaringan dalam Keadaan Normal	35
4.1.3	Mencari Celah Jaringan.....	36
4.1.4	Brute-Force	38
4.1.5	<i>Denial Of Service</i>	40
4.1.6	Firewall RAW	44
4.1.7	Notifikasi WhatsApp.....	48
4.2	Hasil Pengujian Pengamanan	61
4.2.1	Hasil Pengamanan Brute-Force.....	61
4.2.2	Hasil Pengamanan Denial of Service	62
4.2.3	Notifikasi Serangan Melalui WhatsApp	69
BAB V	PENUTUP.....	80
5.1	Kesimpulan	80
5.2	Saran.....	81
	Daftar Pustaka	82

Lampiran	85
----------------	----

DAFTAR GAMBAR

Gambar 3.1 Diagram Blok Arsitektur Pengamanan Router MikroTik	26
Gambar 3.2 Topologi Jaringan.....	27
Gambar 3.3 Flowchart Serangan Brute-Force	28
Gambar 3.4 Flowchart Serangan Ping Flood	30
Gambar 3.5 Flowchart Serangan Syn Flood	31
Gambar 3.6 Flowchart Pengamanan Router MikroTik.....	32
Gambar 4.1 Resource MikroTik Keadaan Normal	36
Gambar 4.2 Scanning Network dengan Nmap.....	37
Gambar 4.3 Script Serangan Brute-Force dengan Hydra.....	38
Gambar 4.4 Hasil Serangan Brute-Force	39
Gambar 4.5 Script Serangan Ping Flood dengan Hping3	41
Gambar 4.6 Diagram Resource CPU MikroTik Saat Ping Flood Berjalan	42
Gambar 4.7 Script Serangan SYN Flood dengan Hping3	43
Gambar 4.8 Diagram Resource CPU MikroTik Saat SYN Flood Berjalan.....	44
Gambar 4.9 Rules Firewall RAW Checking SSH1 Brute-Force	45
Gambar 4.10 Rules Firewall RAW Checking SSH2 Brute-Force	45
Gambar 4.11 Rules Firewall RAW Checking SSH3 Brute-Force	45
Gambar 4.12 Rules Firewall RAW Input IP Attacker Brute-Force	46
Gambar 4.13 Rules Firewall RAW Drop IP Attacker Brute-Force	46
Gambar 4.14 Rules Firewall RAW Input IP Attacker Ping Flood.....	46
Gambar 4.15 Rules Firewall RAW Drop IP Attacker Ping Flood.....	47
Gambar 4.16 Rules Firewall RAW Drop IP Attacker Ping Flood.....	47
Gambar 4.17 Rules Firewall RAW Drop IP Attacker Ping Flood.....	48
Gambar 4.18 Scheduler Brute-Force Attack.....	48
Gambar 4.19 Scheduler Ping Flood Attack.....	52
Gambar 4.20 Scheduler SYN Flood Attack.....	56
Gambar 4.21 Hasil Pengamanan Brute-Force.....	61
Gambar 4.22 Diagram Resource CPU MikroTik Saat Ping Flood Percobaan Pertama.....	62
Gambar 4.23 Diagram Resource CPU MikroTik Saat Ping Flood Percobaan Kedua	63
Gambar 4.24 Diagram Resource CPU MikroTik Saat Ping Flood Percobaan Ketiga	64
Gambar 4.25 Diagram Resource CPU MikroTik Saat Ping Flood Percobaan Keempat	64
Gambar 4.26 Hasil Pengamanan Ping Flood	65
Gambar 4.27 Diagram Resource CPU MikroTik Saat SYN Flood Percobaan Pertama.....	66
Gambar 4.28 Diagram Resource CPU MikroTik Saat SYN Flood Percobaan Kedua	67

Gambar 4.29 Diagram Resource CPU MikroTik Saat SYN Flood Percobaan Ketiga	67
Gambar 4.30 Diagram Resource CPU MikroTik Saat SYN Flood Percobaan Keempat	68
Gambar 4.31 Hasil Pengamanan SYN Flood.....	69
Gambar 4.32 Join Sandbox Twilio	70
Gambar 4.33 Address List Serangan Brute Force Pertama.....	70
Gambar 4.34 Address List Serangan Brute Force Kedua	70
Gambar 4.35 Address List Serangan Brute Force Ketiga	71
Gambar 4.36 Notifikasi Serangan Brute Force	71
Gambar 4.37 Address List Serangan Ping Flood Pertama	72
Gambar 4.38 Address List Serangan Ping Flood Kedua	72
Gambar 4.39 Address List Serangan Ping Flood Ketiga	72
Gambar 4.40 Address List Serangan Ping Flood Keempat	72
Gambar 4.41 Notifikasi Serangan Ping Flood Pertama	73
Gambar 4.42 Notifikasi Serangan Ping Flood Kedua.....	73
Gambar 4.43 Notifikasi Serangan Ping Flood Ketiga.....	74
Gambar 4.44 Notifikasi Serangan Ping Flood Keempat.....	75
Gambar 4.45 Address List Serangan SYN Flood Pertama.....	75
Gambar 4.46 Address List Serangan SYN Flood Kedua.....	76
Gambar 4.47 Address List Serangan SYN Flood Ketiga.....	76
Gambar 4.48 Address List Serangan SYN Flood Keempat.....	76
Gambar 4.49 Notifikasi Serangan SYN Flood Pertama.....	77
Gambar 4.50 Notifikasi Serangan SYN Flood Kedua	77
Gambar 4.51 Notifikasi Serangan SYN Flood Ketiga	78
Gambar 4.52 Notifikasi Serangan SYN Flood Keempat	78

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka	9
Tabel 4.1 Konfigurasi Jaringan	35
Tabel 4.2 Script Scheduler On Event Brute-Force Attack	49
Tabel 4.3 Script Scheduler On Event Ping Flood Attack	53
Tabel 4.4 Script Scheduler On Event SYN Flood Attack	57

DAFTAR LAMPIRAN

Lampiran 1 : Kode Program Firewall RAW Brute-Force.....	85
Lampiran 2 : Kode Program Firewall RAW Ping Flood	85
Lampiran 3 : Kode Program Firewall RAW Syn Flood	85
Lampiran 4 : Kode Program Scheduler On Event Brute-Force Attack	86
Lampiran 5 : Kode Program Scheduler On Event Ping Flood Attack	87
Lampiran 6 : Kode Program Scheduler On Event Syn Flood Attack	88
Lampiran 7 : Berkas Admidistratif 1 Catatan Ujian Praskripsi	89
Lampiran 8 : Berkas Admidistratif 2 Ketetntuan Pendadaran	90
Lampiran 9 : Berkas Admidistratif 3 Catatan Pendadaran.....	91
Lampiran 10 : Berkas Admidistratif 4 Keputusan Hasil Ujian	92

Intisari

Dalam era digital yang terus berkembang, jaringan komputer menjadi infrastruktur yang mendukung berbagai aktivitas seperti bisnis, pendidikan, dan pemerintahan. Pertukaran data melalui jaringan membuat keamanan informasi menjadi prioritas, hal ini dikarenakan rentannya ketersediaan jaringan dan perangkat-perangkat terhadap serangan *cyber*. Router, sebagai perangkat inti dalam jaringan, menjadi fokus utama risiko keamanan terhadap serangan *cyber* seperti *Denial of Service* dan *Brute-Force*.

Menghadapi ancaman ini, keamanan jaringan menjadi suatu keharusan. *Intrusion Detection System* yang diintegrasikan dengan *firewall* dapat mendeteksi aktivitas mencurigakan dan memberikan peringatan kepada administrator jaringan. WhatsApp, sebagai platform pesan instan populer, dapat diintegrasikan dalam sistem keamanan jaringan.

Pengamanan ini dapat mengoptimalkan kinerja *Central Processing Unit* pada router MikroTik serta dengan notifikasi melalui WhatsApp memungkinkan respons cepat terhadap serangan, meminimalkan dampak dan menghemat waktu serta sumber daya. Dengan deteksi dini dan notifikasi segera, sistem keamanan diharapkan dapat mengurangi dampak serangan *Denial of Service* dan *Brute-Force* secara efektif.

Kata kunci: Jaringan Komputer, Router, *Denial of Service*, *Brute-Force*, *Firewall*, *Intrusion Detection System*, WhatsApp.

Abstract

In the ever-growing digital era, computer networks are the infrastructure that supports various activities such as business, education, and government. The exchange of data through networks makes information security a priority, this is due to the vulnerability of network availability and devices to cyber attacks. Routers, as the core device in the network, are the main focus of security risks against cyber attacks such as Denial of Service and Brute-Force.

Facing these threats, network security is a must. An Intrusion Detection System integrated with a firewall can detect suspicious activity and provide alerts to network administrators. WhatsApp, as a popular instant messaging platform, can be integrated in the network security system.

This security can optimize the performance of the Central Processing Unit on MikroTik routers and notifications through WhatsApp enable a quick response to attacks, minimizing impact and saving time and resources. With early detection and immediate notification, the security system is expected to effectively mitigate the impact of Denial of Service and Brute-Force attacks.

Keywords: Computer Network, Router, Denial of Service, Brute-Force, Firewall, Intrusion Detection System, WhatsApp.