

LAPORAN AKHIR

**IMPLEMENTASI KEAMANAN JARINGAN PADA ROUTER MIKROTIK
TERHADAP SERANGAN *BRUTE FORCE* PADA SERVER JURUSAN
TEKNIK KOMPUTER**



**Laporan Ini Disusun untuk Memenuhi Syarat Menyelesaikan Pendidikan
Diploma III Jurusan Teknik Komputer Politeknik Negeri Sriwijaya**

Oleh :

Evrianta Mauludy Alfarizi

061730700537

**JURUSAN TEKNIK KOMPUTER
POLITEKNIK NEGERI SRIWIJAYA**

2020

LEMBAR PENGESAHAN LAPORAN AKHIR
IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK
TERHADAP SERANGAN *BRUTE FORCE* PADA SERVER JURUSAN
TEKNIK KOMPUTER



EVRIANTA MAULUDY ALFARIZI


0617 3070 0537


Palembang, September 2020

Menyetujui,

Pembimbing II


Pembimbing I


Siamet Widodo, S.Kom., M.Kom.
NIP. 197305162002121001


Ali Firdaus, S.Kom., M.Kom.
NIP. 197010112001121001

Mengetahui,

Ketua Jurusan Teknik Komputer


Azwardi, S.T., M.T.
NIP. 197005232005011004

IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK
TERHADAP SERANGAN *BRUTE FORCE* PADA SERVER JURUSAN
TEKNIK KOMPUTER



Telah Diuji dan dipertahankan di depan dewan penguji pada sidang
Laporan Akhir pada Rabu, 19 Agustus 2020

Ketua Dewan penguji

Yelisa Mirza, S.T., M.Kom.
NIP. 196607121990031003

Anggota Dewan penguji

Meivi Darlies, S.Kom., M.Kom.
NIP. 197805152006041003

Alan Novi Tompusu, S.T., M.T.
NIP. 197611082000031002

Hartati Deviana, S.T., M.Kom.
NIP. 197405262008122001

Tanda Tangan

Palembang, September 2020
Mengetahui,
Ketua Jurusan Teknik Komputer

Azwardi, S.T., M.T.
NIP. 197005232005011004

MOTTO

“Dunia ini penuh dengan orang baik, jika kamu tidak bisa menemukannya jadilah salah satunya”

Kupersembahkan untuk :

- ❖ Kedua orang tuaku Bapak & Ibu
- ❖ Keluarga tercinta
- ❖ Dosen Jurusan Teknik Komputer
- ❖ Teman – Teman Seperjuangan
6CB
- ❖ Almamaterku

ABSTRAK

IMPLEMENTASI KEAMANAN JARINGAN PADA ROUTER MIKROTIK TERHADAP SERANGAN *BRUTE FORCE* PADA SERVER JURUSAN TEKNIK KOMPUTER

(Evrianta Mauludy Alfarizi, 2020 : 44 halaman)

Jaringan komputer dan internet merupakan kebutuhan bagi masyarakat. Banyaknya pengguna jaringan komputer dan internet menyebabkan keamanan pada jaringan komputer dan internet merupakan hal yang sangat dibutuhkan pada saat ini, khususnya di lingkungan Teknik Komputer. Salah satu serangan yang berbahaya pada jaringan komputer adalah serangan *brute force*. Serangan *brute force* adalah salah satu serangan yang berbahaya karena serangan tersebut bertujuan untuk membobol *username* dan *password* pada suatu *server* melalui router. Peneliti akan melakukan sebuah konfigurasi pada router untuk melakukan pencegahan terhadap serangan *brute force* dengan cara memblokir *ip address* penyerang selama 1 hari.

Kata Kunci : *keamanan jaringan, Brute force, Ip address*

ABSTRACT

IMPLEMENTATION OF NETWORK SECURITY ON MIKROTIK ROUTERS AGAINST BRUTE FORCE ATTACKS ON SERVERS IN THE DEPARTMENT OF COMPUTER ENGINEERING

(Evrianta Mauludy Alfarizi, 2020 : 44 Pages)

Computer and internet networks are a necessity for society. The large number of users of computer network and internet cause security in computer and internet network is very needed at this time, especially in computer engineering environment. One of the most dangerous attacks on computer networks is a brute force attack. Brute force attacks are one of the most dangerous attacks because they aim to break the username and password on a server via a router. Researchers will analyze the router to prevent brute force attacks by exiting the attacker's IP address for 1 day.

Keywords: *network security, Brute force, Ip address*

KATA PENGANTAR

Puji syukur Penulis haturkan kehadirat Allah SWT, atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan Laporan Akhir ini tepat pada waktunya dengan judul **“Implementasi Keamanan Jaringan pada Router Mikrotik Terhadap Serangan *Brute Force* pada Server Jurusan Teknik Komputer”**. Shalawat dan salam selalu tercurah kepada Rasulullah SAW, keluarganya, sahabatnya dan para pengikutnya hingga akhir zaman.

Tujuan penulisan Laporan Akhir ini dibuat sebagai persyaratan kurikulum untuk menyelesaikan Program Studi Teknik Komputer di Politeknik Negeri Sriwijaya. Sebagian bahan penulisan diambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mengandung penulisan laporan. Pada kesempatan ini, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah memberikan segala kemudahan, bimbingan, pengarahan, dorongan, bantuan baik moril maupun materil selama penyusunan Laporan Akhir ini.

Ucapan terima kasih penulis tujukan kepada yang terhormat :

1. Orangtua dan saudari - saudari ku tercinta, yang telah memberikan doa dan restu serta dukungan yang sangat besar.
2. Bapak Dr. Ing. Ahmad Taqwa, M.T. selaku Direktur Politeknik Negeri Sriwijaya.
3. Bapak Azwardi, S.T., M.T. selaku Ketua Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
4. Bapak Slamet Widodo, S.Kom., M.Kom Selaku Pembimbing I yang telah membimbing saya dari awal sampai akhir pembuatan Laporan Akhir ini.
5. Bapak Ali Firdaus, S.Kom., M.Kom. Selaku Pembimbing II yang telah membimbing saya dari awal sampai akhir pembuatan Laporan Akhir ini.
6. Bapak/Ibu Dosen Jurusan Teknik Komputer Politeknik Negeri Sriwijaya.
7. Segenap teman-teman dan para sahabat yang telah memberikan motivasi dan dukungan dalam penyusunan Laporan Akhir ini.

Penulis menyadari sepenuhnya bahwa Laporan Akhir ini masih jauh dari kesempurnaan. Oleh karena itu, penulis mengharapkan saran dan kritik yang bersifat membangun demi kesempurnaan penulisan yang akan datang. Penulis berharap agar Laporan Akhir ini dapat dipahami, berguna dan bermanfaat bagi kita semua.

Palembang, September 2020

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
LEMBAR PENGESAHAN PEMBIMBING	ii
LEMBAR PENGESAHAN PENGUJI.....	iii
MOTTO	iv
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xv

BAB I PENDAHULUAN

1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan dan manfaat	2
1.4.1 Tujuan	2
1.4.1 Manfaat	3

BAB II TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu	4
2.2 Router MikroTik	4
2.3 <i>Firewall</i>	5
2.3.1 Jenis – jenis <i>firewall</i>	6
2.4 Keamanan Data Jaringan	7
2.5 <i>Password Cracking</i>	7
2.6 <i>Brute force</i>	8
2.6.1 Definisi <i>Brute force</i>	8
2.6.2 Definisi Serangan <i>Brute force</i>	9

2.6.3 Metode Serangan <i>Brute force</i>	10
2.7 <i>Flowchart</i>	11

BAB III RANCANG BANGUN

3.1 Perancangan Sistem	13
3.2 Diagram Alir Rancang Bangun Sistem	14
3.3 Analisis Kebutuhan	15
3.3.1 Router	15
3.3.2 Komputer <i>Remote</i>	15
3.3.3 Komputer Penyerang	16
3.4 Topologi Jaringan	16
3.5 Penginstalan Winbox	17
3.6 Membuat <i>user</i> yang akan diserang	19
3.7 <i>Install software</i> yang dibutuhkan	20

BAB IV HASIL DAN PEMBAHASAN

4.1 Tujuan Pengujian	22
4.2 Persiapan Pengujian.....	22
4.2.1 Memastikan Komputer Penyerang Terkoneksi.....	22
4.3 Melakukan Serangan <i>Brute Force</i>	23
4.3.1 Melakukan Serangan <i>Brute Force</i> pada <i>Port FTP</i>	23
4.3.2 Melakukan Serangan <i>Brute Force</i> pada <i>Port Telnet</i>	25
4.3.3 Melakukan Serangan <i>Brute Force</i> pada <i>Port SSH</i>	27
4.3.4 Melakukan Serangan <i>Brute Force</i> pada <i>OS Windows</i> ..	29
4.4 Melakukan Pencegahan Serangan <i>Brute Force</i>	30
4.4.1 Memblokir Serangan pada <i>Port FTP</i>	30
4.4.2 Memblokir Serangan pada <i>Port SSH & Telnet</i>	34
4.5 Hasil Pengujian.....	39

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan.....	44
5.2 Saran	44

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

Gambar 2.1	Router	5
Gambar 3.1	Blok Diagram	13
Gambar 3.2	<i>Flowchart</i>	14
Gambar 3.3	Gambar Topologi Jaringan.....	16
Gambar 3.4	Pencarian Winbox di browser	17
Gambar 3.5	Web untuk mendownload Winbox.....	17
Gambar 3.6	Menu <i>download</i> pada mikrotik.com	18
Gambar 3.7	Menu untuk mengunduh Winbox.....	18
Gambar 3.8	Mengunduh Winbox	18
Gambar 3.9	Hasil <i>download</i>	18
Gambar 3.10	Winbox yang sudah terunduh di <i>PC</i>	19
Gambar 3.11	Tampilan winbox ketika dibuka.....	19
Gambar 3.12	Daftar User yang akan diserang	20
Gambar 3.13	Menginstall <i>software</i> medusa.....	21
Gambar 3.14	Menginstall <i>software</i> hydra.....	21
Gambar 4.1	Komputer penyerang melakukan ping ke router	21
Gambar 4.2	Melakukan serangan <i>brute force</i> pada <i>port FTP</i>	23
Gambar 4.3	Serangan <i>brute force</i> pada <i>Port FTP</i> berhasil.....	24
Gambar 4.4	Serangan <i>brute force</i> pada <i>Port FTP</i> terdeteksi pada <i>Winbox</i>	24
Gambar 4.5	Melakukan serangan <i>brute force</i> pada <i>port Telnet</i>	25
Gambar 4.6	Serangan <i>brute force</i> pada <i>Port Telnet</i> berhasil.....	25
Gambar 4.7	Serangan <i>brute force</i> pada <i>Port Telnet</i> terdeteksi pada <i>Winbox</i> ...	26

Gambar 4.8	Melakukan serangan <i>brute force</i> pada <i>port SSH</i>	27
Gambar 4.9	Serangan <i>brute force</i> pada <i>Port SSH</i> berhasil	28
Gambar 4.10	Serangan <i>brute force</i> pada <i>Port SSH</i> terdeteksi pada <i>Winbox</i>	28
Gambar 4.11	Serangan <i>brute force</i> menggunakan <i>OS Windows</i>	29
Gambar 4.12	Perintah masuk menu <i>firewall</i>	30
Gambar 4.13	Perintah Konfigurasi <i>firewall port FTP</i> pertama	31
Gambar 4.14	<i>Firewall port FTP</i> pertama berhasil dibuat.....	31
Gambar 4.15	Perintah Konfigurasi <i>firewall port FTP</i> kedua	32
Gambar 4.16	<i>Firewall port FTP</i> kedua berhasil dibuat	32
Gambar 4.17	Perintah Konfigurasi <i>firewall port FTP</i> ketiga	33
Gambar 4.18	<i>Firewall port FTP</i> ketiga berhasil dibuat.....	33
Gambar 4.19	Perintah Konfigurasi <i>firewall port SSH dan Telnet</i> pertama.....	34
Gambar 4.20	<i>Firewall port SSH dan Telnet</i> pertama berhasil dibuat	35
Gambar 4.21	Perintah Konfigurasi <i>firewall port SSH dan Telnet</i> kedua.....	35
Gambar 4.22	<i>Firewall port SSH dan Telnet</i> kedua berhasil dibuat	36
Gambar 4.23	Perintah Konfigurasi <i>firewall port SSH dan Telnet</i> ketiga.....	36
Gambar 4.24	<i>Firewall port SSH dan Telnet</i> ketiga berhasil dibuat	37
Gambar 4.25	Perintah Konfigurasi <i>firewall port SSH dan Telnet</i> keempat.....	37
Gambar 4.26	<i>Firewall port SSH dan Telnet</i> keempat berhasil dibuat	38
Gambar 4.27	Perintah Konfigurasi <i>firewall port SSH dan Telnet</i> kelima.....	38
Gambar 4.28	<i>Firewall port SSH dan Telnet</i> kelima berhasil dibuat	39
Gambar 4.29	Serangan <i>brute force</i> pada <i>port FTP</i> berhasil dicegah.....	40
Gambar 4.30	<i>Ip address</i> penyerang <i>port FTP</i> telah terblokir	40

Gambar 4.31	Serangan <i>brute force</i> pada <i>port Telnet</i> berhasil dicegah	41
Gambar 4.32	<i>Ip address</i> penyerang <i>port Telnet</i> telah terblokir	42
Gambar 4.33	Serangan <i>brute force</i> pada <i>port SSH</i> berhasil dicegah	42
Gambar 4.34	<i>Ip address</i> penyerang <i>port SSH</i> telah terblokir	43

DAFTAR TABEL

Tabel 2.1	Simbol Diagram <i>Flowchart</i>	11
Tabel 3.1	Spesifikasi Router	15
Tabel 3.2	Spesifikasi Komputer <i>Remote</i>	15
Tabel 3.3	Spesifikasi Komputer Penyerang	16