# RANCANG BANGUN SISTEM KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM PADA EVENT VIRTUAL

**SKRIPSI**


**Oleh**

**Febri**

**190210090**



**PROGRAM STUDI TEKNIK INFORMATIKA**
**FAKULTAS TEKNIK DAN KOMPUTER**
**UNIVERSITAS PUTERA BATAM**

**TAHUN 2023**

# RANCANG BANGUN SISTEM KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM PADA EVENT VIRTUAL

**SKRIPSI**

**Untuk memenuhi salah satu syarat**

**memperoleh gelar Sarjana**


**Oleh**

**Febri**

**190210090**

**PROGRAM STUDI TEKNIK INFORMATIKA**
**FAKULTAS TEKNIK DAN KOMPUTER**
**UNIVERSITAS PUTERA BATAM**
**TAHUN 2023**

# SURAT PERNYATAAN ORISINALITAS

Yang bertanda tangan di bawah ini saya :

| | |
|---|---|
| Nama | : Febri |
| NPM | : 190210090 |
| Fakultas | : Teknik dan Komputer |
| Program Studi | : Teknik Informatika |

Menyatakan bahwa **"Skripsi"** yang saya buat dengan judul :

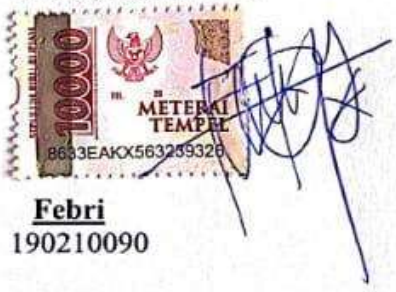
**RANCANG BANGUN SISTEM KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM PADA EVENT VIRTUAL**

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya, di dalam naskah Skripsi ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi ini digugurkan dan gelar akademik yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun

Batam, 10 Juli 2023




**Febri**
190210090



iii

# RANCANG BANGUN SISTEM KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM PADA EVENT VIRTUAL

**SKRIPSI**

**Untuk memenuhi salah satu syarat**
**memperoleh gelar Sarjana**

**Oleh**
**Febri**
**190210090**

**Telah disetujui oleh Pembimbing Pada tanggal**

**Seperti tertera di bawah ini**

**Batam, 22 Juli 2023**

**Ellbert Hutabri, S.kom., M.Kom.**
**Pembimbing**



iv

# ABSTRAK

Dalam perkembangan dan keamajuan teknologi pada saat sekarang ini, keamanan jaringan merupakan aspek yang sangat kritis dan harus diutamakan untuk melindungi sistem dan data dari ancaman serangan. Dalam penelitian ini peneliti akan merancag sebuah sistem keamanan jaringan Mikrotik yang efektif dengan menggunakan dua metode keamanan jaringan yakni *Firewall Filtering* dan *Port Knocking* dalam upaya meningkatkan keamanan jaringan. Metode *Firewall Filtering* digunakan untuk mengatur lalu lintas jaringan serta memblokir jaringan yang dianggap mencurigakan, selain itu metode *Port Knocking* berfungsi sebagai lapisan keamanan jaringan yang mana dengan adanya dua metode ini akan memberikan keamanan yang ekstra dikarenakan port yang dibuka saja yang dapat dituju oleh pengguna. Dalam penelitian ini sistem keamanan jaringan yang dirancang juga mencangkup notifikasi telegram sebagai bentuk pemberitahuan instan kepada *administrator* jaringan ketika terjadi suatu hal yang tidak biasa seperti akses yang mencurigakan atau percobaan *port knocking* yang gagal. Evaluasi kinerja dari sistem dilakukan dengan skenario uji coba serangan dan analisis dilakukan terhadap kemampuan sistem untuk mendeteksi dan memberikan notifikasi terkait kejadian tersebut. Dari hasil pengujian dapat dilihat penggunaan kombinasi *Fireawall Filtering* dan *Port Knocking* dapat memberikan perlindungan terhadap sistem keamanan jaringan Mikrotik dan notifikasi melalui aplikasi telegram akan memudahkan seoraang *administrator* jaringan dalam merespon ketika terjadinya suatu ancamana keamanan jaringan.

**Kata kunci:** Keamanan Jaringan, MikroTik, *Firewall Filtering, Port Knocking*, Notifikasi Telegram

## ABSTRACT

*In the development and advancement of technology at this time, network security is a very critical aspect and must be prioritized to protect systems and data from the threat of attack. In this study researchers will design an effective Mikrotik network security system using two network security methods namely Firewall Filtering and Port Knocking in an effort to improve network security. The Firewall Filtering method is used to manage network traffic and block networks that are considered suspicious, besides that the Port Knocking method functions as a layer of network security which with these two methods will provide extra security because only the ports that are opened can be addressed by the user. In this study the designed network security system also includes telegram notifications as a form of instant notification to network administrators when something unusual occurs, such as suspicious access or failed port knocking attempts. Performance evaluation of the system is carried out using attack test scenarios and analysis is carried out on the system's ability to detect and provide notifications regarding these events. From the test results it can be seen that the use of a combination of Firewall Filtering and Port Knocking can provide protection for the Mikrotik network security system and notifications via the Telegram application will make it easier for a network administrator to respond when a network security threat occurs.*



***Keywords:*** *Network Security, MikroTik, Firewall Filtering, Port Knocking, Telegram Notifications*

# KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa yang telah melimpahkan segala rahmat, dan karuniaNya, sehingga peneliti dapat menyelesaikan laporan tugas akhir dengan judul "Rancang Bangun Sistem Keamanan Jaringan Mikrotik Menggunakan Firewall Filtering dan Port Knocking Dengan Notifikasi Telegram Pada Event Virtual" yang merupakan salah satu persyaratan untuk menyelesaikan progam studi strata satu (SI) pada program studi Teknik Informatika di Universiras Putera Batam.

Peneliti menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa peneliti terima dengan senang hati. Dengan segela keterbatasan, peneliti menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, peneliti menyampaikan ucapan terimakasih kepada:

1. Ibu Dr. Nur Elfi Husda, S.Kom., M.SI. Rektor Universitas Putera Batam.
2. Bapak Welly Sugianto, S.T., M.M. Dekan Fakultas Teknik dan Komputer Universitas Putera Batam.
3. Bapak Andi Maslan, S.T., M.SI. Ketua Program Studi Manajemen Universitas Putera Batam.
4. Bapak Ellbert Hutabri, S.kom., M.Kom. selaku Pembimbing Skripsi Pada program Studi Teknik Informatika Universitas Putera Batam.
5. Dosen dan Staff Universitas Putera Batam.



vii

6. Pimpinan PT. Shanaya Creativo Innovation yang telah memberikan izin melakukan penelitian.
7. Kepala bidang IT PT.Shanaya Creativo Innovation.
8. Teristimewa kepada kedua Orangtua dan keluarga tercinta.
9. Ucapan terimakasih kepada teman seperjuangan Suwanda dan Rory Prasetia yang selalu memberikan masukan dan semangat dalam menyelesaikan penelitian ini.
10. Ucapan terimakasih kepada teman-teman seperjuangan satu angkatan yang telah mendukung untuk menyelesaikan penelitian ini

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya, Amin.

Batam ,10 Juli 2023

**Febri**
190210090



viii

# DAFTAR ISI

**HALAMAN SAMPUL** ..... **i**
**HALAMAN JUDUL** ..... **ii**
**SURAT PERNYATAAN** ..... **iii**
**HALAMAN PENGESAHAN** ..... **iv**
**ABSTRAK** ..... **v**
**ABSTRACT** ..... **vi**
**KATA PENGANTAR** ..... **vii**
**DAFTAR ISI** ..... **ix**
**DAFTAR GAMBAR** ..... **xii**
**DAFTAR TABEL** ..... **xiv**
**BAB I PENDAHULUAN**
1.1 Latar Belakang ..... 1
1.2 Identifikasi Masalah ..... 5
1.3 Batasan Masalah ..... 5
1.4 Rumusan Masalah ..... 6
1.5 Tujuan Penelitian ..... 6
1.6 Manfaat Penelitian ..... 7
1.6.1 Aspek Teoritis ..... 7
1.6.2 Aspek Praktis ..... 7
**BAB II TINJAUAN PUSTAKA**
2.1 Teori Dasar ..... 9
2.1.1 Definisi Jaringan ..... 9
2.1.2 Jenis jenis jaringan ..... 10
2.1.3 Topologi Jaringan ..... 14
2.1.4 Jenis serangan pada jaringan komputer ..... 18
2.1.5 Serangan Terhadap Perangkat keras *( Hardware )* ..... 21
2.1.6 Serangan Terhadap Perangkat Lunak *( Software )* ..... 22
2.1.7 Serangan Terhadap Basis Data ..... 24
2.2 Teori Khusus ..... 24

2.2.1 Keamanan Jaringan ..... 24
2.2.2 Mikrotik ..... 26
2.2.3 Keamanan Sistem Jaringan ..... 28
2.2.4 Firewall Filtering ..... 29
2.2.5 Port Knocking ..... 31
2.2.6 Telegram Bot ..... 33
2.3 Software pendukung ..... 36
2.4 Penelitian Terdahulu ..... 40
2.5 Kerangka pemikiran ..... 45
**BAB III METODE PENELITIAN**
3.1 Desain Penelitian ..... 48
3.1.1 Teknik Pengumpulan Data ..... 51
3.2 Analisis Jaringan Lama/ sedang berjalan ..... 53
3.3 Rancangan Jaringan yang diusulkan ..... 55
3.3.1 Metode demonstrasi ..... 56
3.3.2 Desain pengiriman alur informasi serangan ..... 56
3.3.3 Perangkat hardware yang digunakan ..... 57
3.3.4 Perangkat Software ..... 59
3.3.5 Spesifikasi Hardware dan Software ..... 60
3.4 Topologi jaringan ..... 61
3.5 Tahapan rencana implementasi ..... 62
3.4 Lokasi dan Jadwal Penelitian ..... 63
3.4.1 Lokasi penelitian ..... 63
3.4.2 Jadwal penelitian ..... 63
**BAB IV HASIL DAN PEMBAHASAN**
4.1 Konfigurasi Dasar Mikrotik ..... 65
41.1 Konfigurasi Winbox Basic ..... 65
4.1.2 Konfigurasi Tabel IP ..... 69
4.1.3 Konfigurasi DHCP Client ..... 69
4.1.5 Konfigurasi NAT ..... 72
4.1.4 Konfigurasi DHCP Server ..... 73
4.2. Konfigurasi Firewall Mikrotik ..... 75

4.2.1 Konfigurasi Firewall Rule Pada mikrotik ..... 75
4.2.2 Konfigurasi Log Mikrotik ..... 81
4.2.3 Konfigurasi API telegram ..... 82
4.3 Pengujian Serangan ..... 84
4.3.1 Pengujian serangan Brute force SSH dan telnet ..... 84
4.3.2 Pengujian serangan Brute Force FTP ..... 86
4.3.3 Pengujian serangan Port Scanning ..... 90
**BAB V KESIMPULAN DAN SARAN**
5.1 Kesimpulan ..... 93
5.2 Saran ..... 94
**DAFTAR PUSTAKA**
**LAMPIRAN**
Lampiran Coding
Lampiran Dokumentasi Penelitian
Lampiran Surat Penelitian
Lampiran Surat Balasan Penelitian
Lampiran Daftar Riwayat Hidup
Lampiran Turnitin Jurnal
Lampiran Turnitin Skripsi
Lampiran LOA Jurnal

# DAFTAR GAMBAR


Gambar 2.1 *Local Area Network* ..... 11
Gambar 2.2 *Metropolitan Area Network* ..... 12
Gambar 2.3 *Wide Area Network* ..... 13
Gambar 2.4 *Topologi Bus* ..... 14
Gambar 2.5 *Topologi Ring* ..... 15
Gambar 2.6 *Topologi Star* ..... 16
Gambar 2.7 *Topologi Tree* ..... 17
Gambar 2.8 *Topologi Mesh* ..... 17
Gambar 2.9 *Topologi Hybrid* ..... 18
Gambar 2.10 Mikrotik ..... 26
Gambar 2.11 Cara kerja *Firewall* ..... 30
Gambar 2.12 Proses *Port Knocking* ..... 33
Gambar 2.13 Cara kerja API ..... 35
Gambar 2.14 *FileZilla* ..... 36
Gambar 2.15 *Putty* ..... 37
Gambar 2.16 *Zenmap* ..... 38
Gambar 2.17 Kerangka pemikiran ..... 45
Gambar 3.1 Metode Penelitian ..... 48
Gambar 3.2 Analisis Jaringan Lama ..... 53
Gambar 3.3 Sistem Jaringan Baru ..... 55
Gambar 3.4 Desain Pengiriman Alur Informasi Serangan ..... 57
Gambar 3.5 Topologi Jaringan ..... 61
Gambar 3.6 Lokasi Penelitian ..... 63
Gambar 4.1 Situs Untuk *Mendownload Winbox* ..... 65
Gambar 4.2 Tampilan Awal *Login* ke Mikrotik ..... 66
Gambar 4.3 *Home Tool Winbox* ..... 67
Gambar 4.4 Skema Proses Pengalamatan Jaringan ..... 68
Gambar 4.5 Konfigurasi IP *Addresses* ..... 69
Gambar 4.6 Konfigurasi *DHCP Client* ..... 70
Gambar 4.7 Status *DHCP client* ..... 71
Gambar 4.8 Pengujian Jaringan dengan Tes Ping ..... 72
Gambar 4.9 Konfigurasi NAT ..... 73
Gambar 4.10 Konfigurasi *DHCP Server* ..... 74
Gambar 4.11 Konfigurasi *Brute force SSH dan Telnet* ..... 75
Gambar 4.12 *Brute force SSH* dan *Telnet* ..... 76
Gambar 4.13 Konfigurasi *Brute force FTP* ..... 77
Gambar 4.14 Pengujian *Brute force FTP* ..... 78

Gambar 4.15 Konfigurasi *Port Scanning* ..... 79
Gambar 4.16 Pengujian *Port Scanning* ..... 80
Gambar 4.17 Konfigurasi *Log Mikrotik* ..... 81
Gambar 4.18 *Chat BotFather* ..... 82
Gambar 4.19 *Chat Get Id Bot* ..... 83
Gambar 4.20 *Putty* Konfigurasi ..... 84
Gambar 4.21 Memasukan *Username* dan *Pasword* ..... 85
Gambar 4.22 Pemberitahuan Pada *Log Winbox* ..... 85
Gambar 4.23 Notifikasi Telegram *Brute force SSH* dan *Telnet* ..... 86
Gambar 4.24 Pengujian Serangan *Brute force FTP* ..... 87
Gambar 4.25 Pemberitahuan Serangan *Brute force FTP* ..... 88
Gambar 4.26 *Log Mikrotik* Serangan *Brute force FTP* ..... 88
Gambar 4.27 Notifikasi Telegram Serangan *Brute force FTP* ..... 89
Gambar 4.28 Pengujian *Port Scanning* ..... 90
Gambar 4.29 Port yang terbuka ..... 91
Gambar 4.30 Serangan *Port Scanning* ..... 92
Gambar 4.31 Notifikasi Telegram Serangan *Port Scanning* ..... 92

# DAFTAR TABEL

Tabel 3. 1 Perangkat *Hardware* yang digunakan ..... 58
Tabel 3. 2 Jadwal Penelitian ..... 64
Tabel 4. 1 *Topologi IP address* ..... 68
Tabel 4. 2 Konfigurasi API Telegram ..... 83