

**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 MENGUNAKAN 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

**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**

ABSTRAK

Dalam perkembangan dan kemajuan 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 merancang 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 mencakup 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 *Firewall Filtering* dan *Port Knocking* dapat memberikan perlindungan terhadap sistem keamanan jaringan Mikrotik dan notifikasi melalui aplikasi telegram akan memudahkan seorang *administrator* jaringan dalam merespon ketika terjadinya suatu ancaman 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 kehadiran 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 program studi strata satu (SI) pada program studi Teknik Informatika di Universitas Putera Batam.


Peneliti menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa peneliti terima dengan senang hati. Dengan segala 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.

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 Prasetya 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

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 (<i>Hardware</i>)	21
2.1.6 Serangan Terhadap Perangkat Lunak (<i>Software</i>).....	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
4.1.1 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 <i>Local Area Network</i>	11
Gambar 2.2 <i>Metropolitan Area Network</i>	12
Gambar 2.3 <i>Wide Area Network</i>	13
Gambar 2.4 <i>Topologi Bus</i>	14
Gambar 2.5 <i>Topologi Ring</i>	15
Gambar 2.6 <i>Topologi Star</i>	16
Gambar 2.7 <i>Topologi Tree</i>	17
Gambar 2.8 <i>Topologi Mesh</i>	17
Gambar 2.9 <i>Topologi Hybrid</i>	18
Gambar 2.10 Mikrotik	26
Gambar 2.11 Cara kerja <i>Firewall</i>	30
Gambar 2.12 Proses <i>Port Knocking</i>	33
Gambar 2.13 Cara kerja API	35
Gambar 2.14 <i>FileZilla</i>	36
Gambar 2.15 <i>Putty</i>	37
Gambar 2.16 <i>Zenmap</i>	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 <i>Mendownload Winbox</i>	65
Gambar 4.2 Tampilan Awal <i>Login</i> ke Mikrotik	66
Gambar 4.3 <i>Home Tool Winbox</i>	67
Gambar 4.4 Skema Proses Pengalamatan Jaringan	68
Gambar 4.5 Konfigurasi <i>IP Addresses</i>	69
Gambar 4.6 Konfigurasi <i>DHCP Client</i>	70
Gambar 4.7 Status <i>DHCP client</i>	71
Gambar 4.8 Pengujian Jaringan dengan Tes Ping	72
Gambar 4.9 Konfigurasi NAT	73
Gambar 4.10 Konfigurasi <i>DHCP Server</i>	74
Gambar 4.11 Konfigurasi <i>Brute force SSH dan Telnet</i>	75
Gambar 4.12 <i>Brute force SSH dan Telnet</i>	76
Gambar 4.13 Konfigurasi <i>Brute force FTP</i>	77
Gambar 4.14 Pengujian <i>Brute force FTP</i>	78

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

DAFTAR TABEL

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

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan jaringan dapat dikatakan suatu hal yang vital dan harus diperhatikan karena itu merupakan hal yang sangat mendasar dalam keamanan jaringan, kelemahan di dalam jaringan komputer yang tidak dapat dilindungi tentunya dapat berdampak pada kerugian seperti kehilangan file data bahkan kerusakan sistem server, tidak maksimal dalam melayani *user* atau pengguna yang dapat menyebabkan kehilangan aset berharga suatu organisasi atau perusahaan. Keamanan jaringan harus sangat diperhatikan, tentunya dengan adanya perkembangan dari jaringan maka jenis ancaman serangan yang datang juga akan semakin canggih dan bervariasi terlebih jika jaringan lokal telah terhubung ke internet tentunya ancaman jaringan terhadap jaringan tersebut akan meningkat (Mulyanto et al., 2022).

Mengutip penelitian yang dilakukan (Saputro et al., 2020) belakangan ini ancaman serangan yang terjadi yakni *Port Scanning* dan *DDoS (Distributed Denial Of Service)* yang mana menurut *survey* Link 11 menunjukkan lonjakan peningkatan sebanyak 81% maksimal *bandwidth* yang di tujukan dalam mengatasi DDoS ini, sedangkan volume paket yang tertinggi sebanyak 19 *packet* dengan lebih dari 50Gbps. Sehingga pentingnya keamanan jaringan. Dalam jaringan komputer tentunya ini harus menjadi fokus utama terlebih jika mengadakan sebuah *event*

secara *virtual* tentunya ancaman serangan ini akan lebih beragam mengingat *event virtual* ini dilaksanakan secara *online*.

Event Virtual adalah sebuah acara yang dilakukan secara *online* melalui perangkat elektronik secara digital, seperti yang kita ketahui di masa era digital sekarang ini, dengan adanya perkembangan teknologi yang ada, tidak menutup kemungkinan bagi kita untuk melaksanakan sebuah kegiatan secara *online*. Dengan ini akan memberikan opsi alternatif dalam melakukan kegiatan. Proses mekanisme jaringan membutuhkan router sebagai penghubung ISP (*Internet Service Provider*) menuju *switch*, salah satu router yang akan digunakan yakni router mikrotik pada *event virtual*. Router mikrotik digunakan untuk management, filtering jaringan dengan tujuan untuk menjaga kestabilan, efektifitas serta tingkat keamanan pada saat digunakan (Aji & Diniati, 2021).

Router mikrotik berfungsi untuk meringankan pekerjaan *administrator* dalam *mengkonfigurasi*, *monitoring*, dan *troubleshooting* pada sebuah sistem (Hidayat et al., 2022). Saat mengimplementasikan dalam acara *event virtual*, konfigurasi berfungsi untuk mengkonfigurasi sistem sesuai dengan kebutuhan. Fungsi *monitoring* untuk melihat sebuah sistem berjalan pada saat pengujian maupun pada saat acara sedang berlangsung, akan tetapi hal tersebut tidaklah dapat dilakukan setiap saat dikarenakan terkendala oleh tempat yang tidak bisa dijaga setiap saat, khususnya pada perangkat router mikrotik. Permasalahan yang muncul adalah ketika *administrator* tidak dapat mengetahui jika terjadi gangguan-gangguan yang dapat menghambat dan mengurangi kinerja dari router mikrotik, seperti percobaan untuk memasuki sebuah sistem keamanan jaringan secara *illegal* (*Brute*

Force, SSH, Telnet) dan *Scanning* pada *port router mikrotik* (Desmira & Wiryadinata, 2022b). Serangan tersebut merupakan suatu langkah awal dalam upaya proses pencurian data atau merusak data, apabila hal tersebut terjadi pada router mikrotik tentu saja akan mengganggu kinerja dari router mikrotik tersebut.

PT. Shanaya Creativo Innovation merupakan sebuah perusahaan perorangan yang bergerak dibidang *IT Consultant* yang berdiri sejak tahun 2019. Perusahaan ini memberikan layanan berupa jasa yang berhubungan dengan permasalahan teknologi informasi yang ada di perusahaan tentunya ini akan memberikan dampak positif dalam jangka panjang. Tetapi terdapat beberapa permasalahan yang dihadapi di perusahaan yaitu ketika hendak memonitoring keamanan jaringan administrator jaringan diharuskan menggunakan komputer dan laptop dalam *memonitoring* jaringan tentunya ini tidaklah efektif. Maka peneliti ingin melakukan penelitian untuk memberikan perubahan dalam memonitoring keamanan jaringan menggunakan handphone dengan bantuan sosial media telegram.

Tahapan awal yang harus dilakukan adalah pemberian keamanan terhadap sistem router mikrotik. Penerapan fitur *port knocking* pada sistem login dengan autentifikasi kesepakatan dengan bertujuan untuk menghambat serta meminimalisir kemungkinan ketika terjadinya serangan *ssh, telnet* dan *winbox*, fitur *firewall* melakukan filtering terhadap jaringan apabila terdeteksi adanya kejanggalan pada saat proses login, melakukan pemblokiran ip secara otomatis, pengnonaktifan pada serangan dan pemberitahuan atau notifikasi serangan dengan memanfaatkan social media telegram sebagai platform yang terhubung ke router mikrotik terhadap

administrator (Rizal et al., 2020). Telegram merupakan sebuah aplikasi yang gratis, ringan dan bersifat multiplatform dengan kata lain telegram merupakan sebuah aplikasi yang bersifat *open source* yang memudahkan kita dalam membangun sebuah pengembangan bot telegram bagi para pengembang.

Telegram Bot API (*Application Programming Interface*) terdiri dari sebuah perintah dan objek yang diperlukan dalam menyelesaikan instalasi bot telegram. Dengan menggunakan antar muka yang ada, maka dengan otomatis perintah yang dimasukan akan dieksekusi secara mandiri dan membuat asisten yang akan melakukan fungsi yang diberikan kepada mereka ketika telegram di jalankan, yang mana terdapat beberapa keunggulan yang ditawarkan oleh telegram ketika pengguna mengoperasikannya yakni dapat mengirim ataupun menerima file dari robot maupun klien tentunya dengan keunggulan ini akan memudahkan pengguna dalam memonitoring setiap aktivitas dalam rancangan yang akan dibuat nantinya (Sastrawangsa, 2017).

Berdasarkan permasalahan yang sering alami ketika mengadakan sebuah *event* secara *virtual* maka peneliti akan melakukan sebuah penelitian yang berjudul Rancang bangun sistem keamanan jaringan mikrotik menggunakan *firewall filtering* dan *port knocking* dengan notifikasi telegram pada *event virtual* yang bertujuan dapat memudahkan pekerjaan *administrator* dalam menjaga keamanan sebuah sistem sehingga dapat meminimalisir serangan dan memfiltering jaringan yang mencurigakan serta melakukan autentifikasi serta memberikan notifikasi melalui bantuan sosial media telegram dalam upaya mengantisipasi serangan pada router mikrotik.

1.2 Identifikasi Masalah

Berdasarkan penjelasan yang dijabarkan pada latar belakang maka dapat diuraikan beberapa beberapa masalah pada penelitian ini :

1. Belum adanya sistem keamanan yang menjamin sebuah sistem dapat berjalan dengan aman
2. Belum terdapat sarana pendukung dalam mengembangkan sistem keamanan jaringan dalam sebuah event yang dilakukan secara virtual
3. Belum adanya sistem pengingat ketika terjadi sebuah serangan terhadap sistem.

1.3 Batasan Masalah

Dalam penelitian ini peneliti berfokus pada permasalahan yang akan dibahas supaya penelitian ini lebih efisien dan tepat sasaran sehingga mampu dipahami, maka peneliti membuat batasan masalah sebagai berikut:

1. Sistem yang dikembangkan hanya pada jaringan LAN (*Local Area Network*)
2. Sistem dirancang dengan menggunakan 4 user yakni pada virtual mesin sebagai router (mikrotik versi 7.1.1), *attacker 1 (Putty)*, *attacker 2 (Filezilla)*, dan *attacker 3 (Zenmap)*.
3. Penelitian ini hanya sampai tahap pengujian serangan pada sistem keamanan firewall filtering digunakan untuk mengatasi (*Port Scanning, Brute Force, ssh dan telnet*)
4. Penelitian ini hanya sampai tahap pengujian serangan pada sistem keamanan jaringan dan pengujian pada serangan (*ssh, telnet dan scanning*)

5. Notifikasi jika terjadi serangan melalui telegram versi 9.5.4

1.4 Rumusan Masalah

Berdasarkan latar belakang masalah maka dapat dijelaskan beberapa rumusan masalah dalam penelitian ini :

1. Bagaimana penerapan keamanan pada router mikrotik terhadap serangan jaringan ?
2. Bagaimana cara penerapan *filtering firewall* dan *port knocking* pada sebuah sistem ?
3. Bagaimana menjadikan telegram sebagai notifikasi sistem peringatan ?

1.5 Tujuan Penelitian

Dalam tujuan penelitian, peneliti akan memberikan gambaran dari setiap rancangan dari keamanan jaringan ini, yang mana tujuan dari penelitian ini adalah sebagai berikut:

1. Membuat sebuah rancang bangun sebuah sistem keamanan router mikrotik untuk mengantisipasi serangan terhadap pihak pihak yang tidak berhak dalam mengaksesnya
2. Menerapkan rancangan pada fitur fitur *filtering firewall*, *block ip*, *drop ip*, *port scanning*, *brute force*, *winbox*, *ssh* dan *telnet*
3. Implementasi telegram sebagai notifikasi awal dalam mengantisipasi serangan pada router mikrotik

1.6 Manfaat Penelitian

Dalam penelitian ini ditemukan manfaat-manfaat yang dapat memberi nilai tambahan teori pendukung bagi peneliti yang hendak mengangkat topik yang sama kedepannya berdasarkan beberapa aspek sebagai berikut :

1.6.1 Aspek Teoritis

Dengan adanya penelitian ini peneliti berharap dapat memberi dampak yang positif terhadap perusahaan atau organisasi lain yang membutuhkan referensi mengenai judul ini. Maka peneliti dapat menyebutkan beberapa aspek teoritis yang ada dalam penelitian ini :

1. Dengan adanya notifikasi melalui telegram maka akan mempercepat dalam upaya meminimalisir kemungkinan terjadinya penyerangan terhadap router mikrotik
2. Dapat mengetahui jika terjadinya penyerangan serta menjadi langkah dalam mengevaluasi dalam meningkatkan keamanan bagi administrator

1.6.2 Aspek Praktis

Dalam penelitian ini terdapat beberapa aspek praktis yang dalam dirasakan bagi beberapa pihak diantaranya :

1. Untuk Penyelenggara *event virtual* , dapat mengetahui serangan yang terjadi melalui notifikasi melalui social media telegram
2. Untuk Pembaca, menambah wawasan dan pengetahuan serta informasi mengenai keamanan router mikrotik berdasarkan penelitian yang dilakukan.

3. Untuk Univeritas, dapat menjadi referensi di perpustakaan
4. Untuk Peneliti, menjadi ilmu baru yang dapat digunakan dalam dunia kerja

BAB II

TINJAUAN PUSTAKA

2.1 Teori Dasar

2.1.1 Definisi Jaringan

Jaringan adalah sekumpulan sel yang memiliki bentuk serta struktur yang sama tetapi dengan fungsi yang berbeda yang mana jaringan telekomunikasi akan memberi izin untuk setiap node-node untuk saling bertukar informasi atau berbagi sumber daya (*resources*) (Fauzan & Purwanto, 2021).

Jaringan komputer adalah sekumpulan perangkat komputer yang terdiri dari *computer, hub, switch, router* serta perangkat jaringan komputer yang terhubung dengan media komunikasi lainnya yang mana nantinya akan bekerja sama dalam mencapai tujuan tertentu.

Beberapa pandangan para ahli mengenai jaringan komputer adalah sebagai berikut :

Menurut Dede sopandi yang dikutip oleh (Asnawi, 2018) jaringan komputer merupakan penggabungan dari teknologi telekomunikasi dengan teknologi komputer yang mana dari gabungan dua teknologi ini nantinya akan menghasilkan suatu pengolahan data yang meliputi pemakaian *s/w*, perangkat *h/w* yang mana database manajemen sistem akan dilakukan secara bersama sama.

Menurut Subramanian jaringan adalah pengolahan, pengaturan serta perincian yang bertujuan supaya setiap elemen pada jaringan dapat teratur dikelola

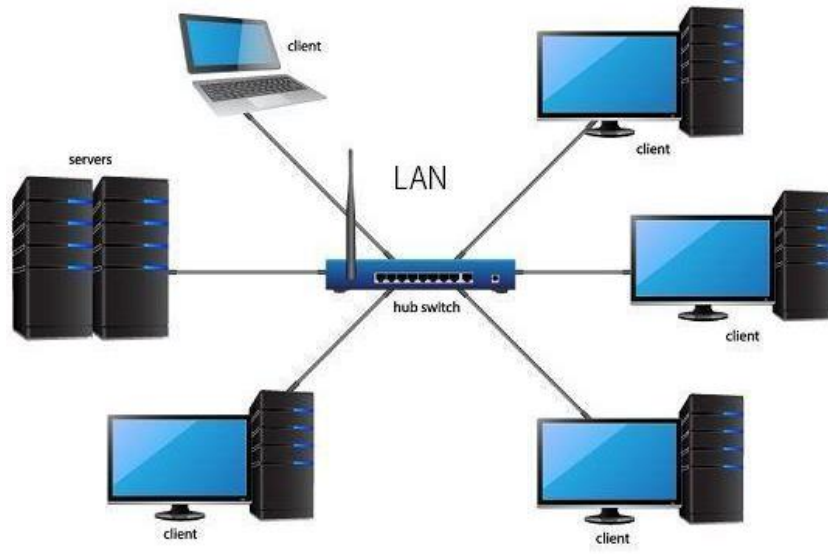
sehingga jaringan tersebut dapat digunakan sesuai dengan manajemen jaringan (Asnawi, 2018).

Berdasarkan pengertian jaringan menurut para ahli maka dapat disimpulkan jaringan adalah sistem yang melibatkan pengolahan, pengaturan dan perincian yang bertujuan untuk mengelola setiap elemen yang ada dalam jaringan secara teratur yang bertujuan untuk terbentuknya manajemen jaringan dan jaringan juga merupakan gabungan antara dua perangkat yaitu perangkat keras (*hardware*) dan perangkat lunak (*software*) serta dapat melakukan manajemen database secara bersama-sama untuk mencapai tujuan pengelolaan jaringan.

2.1.2 Jenis jenis jaringan

Jaringan komputer merupakan sebuah jaringan yang terdiri dari dua perangkat komputer yang saling terhubung sehingga dapat berbagi informasi, mengirim file dan bertukar data. Menurut (Samsumar & Hadi, 2018) dalam penelitiannya jaringan komputer dikelompokkan menjadi 3 bagian berdasarkan ruang cakupannya , yaitu sebagai berikut:

1. Local Area Network (LAN)

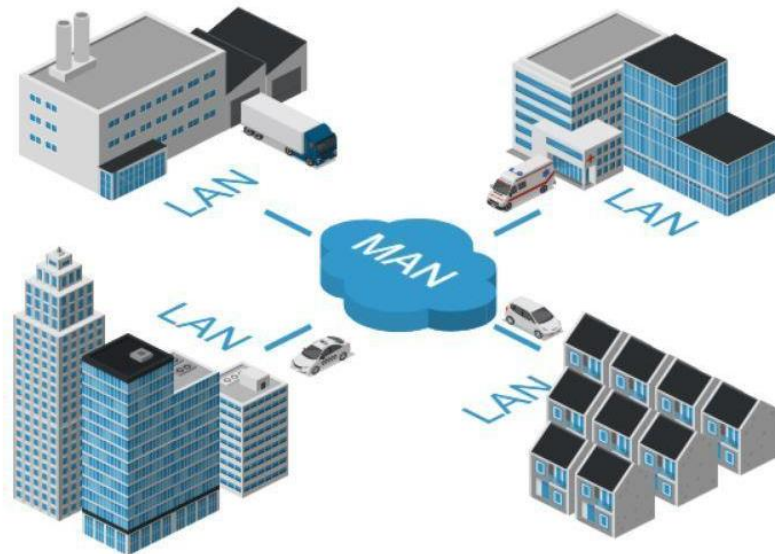


Gambar 2.1 *Local Area Network*
Sumber : (Samsumar & Hadi, 2018)

Local Area Network (LAN) adalah jenis jaringan yang berskala kecil yang mana ruang lingkungannya hanya didalam ruangan saja atau dalam gedung saja, dalam membangun jaringan LAN minimal harus mempunyai 2 buah komputer yang telah terinstall *lan card*. Biasanya jenis jaringan LAN ini sering dijumpai pada sekolah, rumah dan perkantoran, terdapat kelebihan menggunakan jaringan LAN sebagai berikut :

1. Jaringan LAN dapat dikelola pada jaringan yang lebih besar seperti WAN (*Wide Area Network*).
2. Berbagi data atau file dapat dilakukan dengan cepat dan mudah.
3. Tingkat kerusakan pada jaringan LAN cenderung lebih rendah.

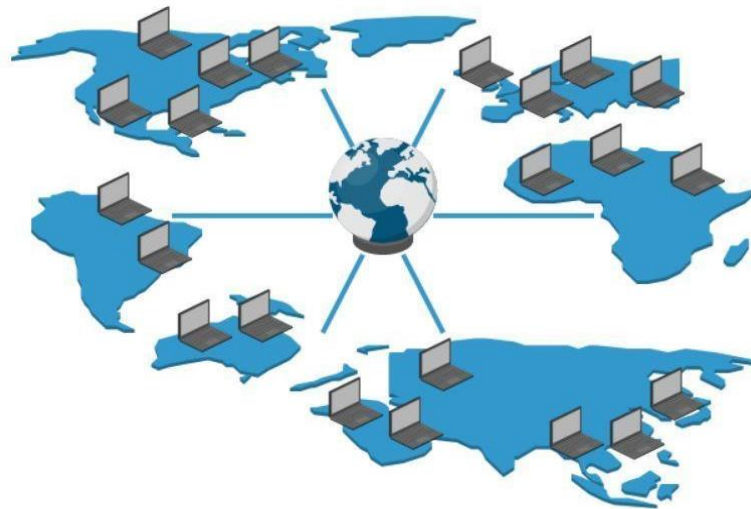
2. Metropolitan Area Network (MAN)



Gambar 2.2 Metropolitan Area Network
Sumber : (Samsumar & Hadi, 2018)

Metropolitan Area Network (MAN) merupakan pengembangan dari jaringan LAN yang mana ruang cakupannya itu sudah antar kota, jarak jaringan ini akan bergantung pada jangkauan panjang kabel yang digunakan, biasanya jaringan ini digunakan dalam satu kota dan antar kampus.

3. *Wide Area Network (WAN)*



Gambar 2.3 *Wide Area Network*
Sumber : (Samsumar & Hadi, 2018)

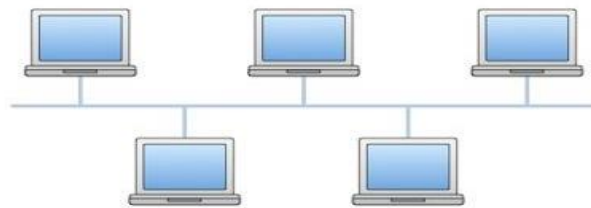
Merupakan sebuah jaringan yang cakupan jaringannya sudah luas dan jaringan wan ini juga gabungan dari jaringan LAN dan MAN. Jaringan wan ini telah memenuhi untuk kebutuhan public seperti jaringan pada perbankan, WAN menggunakan protokol internet NSP (*Network Service Provider*). Kelebihan jaringan WAN antara lain sebagai berikut :

1. Jaringan WAN telah dapat mengirimkan sebuah file dalam jarak yang cukup jauh dengan efisien diseluruh lokasi yang terhubung.
2. Keamanan jaringan WAN telah menggunakan keamanan lanjutan seperti VPN (*Virtual Private Network*) untuk mengenkripsi data yang dikirim melalui jaringan.

2.1.3 Topologi Jaringan

Menurut (Samsumar & Hadi, 2018) Topologi secara umum dibagi menjadi 6 bagian, diantaranya sebagai berikut :

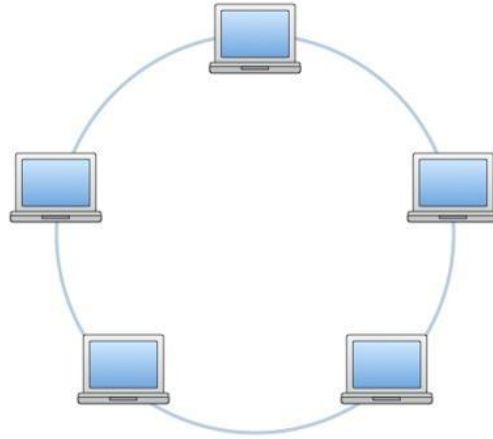
1. Topologi Bus



Gambar 2.4 *Topologi Bus*
Sumber : (Samsumar & Hadi, 2018)

Topologi bus merupakan sebuah topologi jaringan yang paling sederhana yang mana hanya menggunakan jenis kabel *coaxial* sepanjang node *client* dan konektor, topologi jenis ini hanya menggunakan sebuah jenis kabel utama sebagai tulang punggung (*backbone*). Keuntungan topologi ini adalah sebagai berikut : Karena hanya menggunakan satu jenis kabel maka topologi ini sangat mudah dikembangkan. Kerugian deteksi dan isolasi kesalahannya sangat kecil karena jalur lalu lintas yang padat yang menyebabkan apabila satu client rusak maka akan mempengaruhi jaringan yang lain.

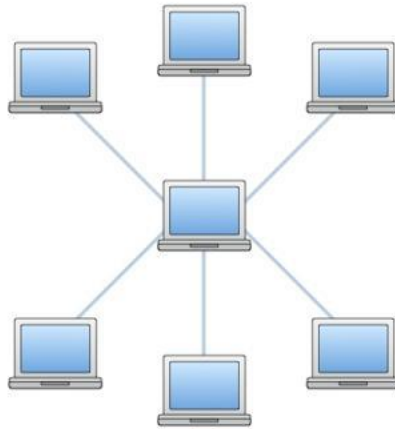
2. Topologi Ring



Gambar 2.5 *Topologi Ring*
Sumber : (Samsumar & Hadi, 2018)

Topologi Ring adalah salah satu jenis topologi jaringan komputer yang menghubungkan setiap perangkat secara langsung dengan dua perangkat lainnya sehingga membentuk sebuah cincin (lingkaran). Dimana data akan mengalir dalam satu arah melalui setiap perangkat dalam bentuk sinyal yang bergerak searah jarum jam atau berlawanan dengan arah jarum jam.

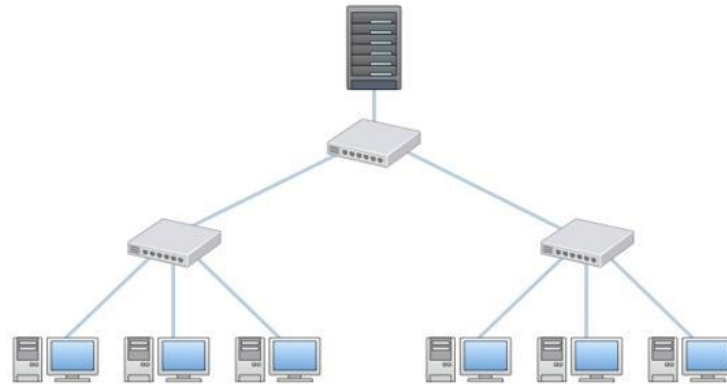
3. Topologi Star



Gambar 2.6 *Topologi Star*
Sumber : (Samsumar & Hadi, 2018)

Topologi star adalah salah satu jenis topologi jaringan komputer yang memiliki pusat distribusi atau simpul pusat (*hub/switch*) yang menghubungkan semua perangkat dalam jaringan secara langsung. Setiap perangkat dalam jaringan terhubung ke simpul pusat melalui kabel tunggal, sehingga membentuk struktur seperti bintang. Semua data yang dikirimkan dari satu perangkat akan dikirimkan terlebih dahulu ke simpul pusat sebelum diarahkan ke perangkat tujuan. Topologi jenis ini merupakan jenis topologi yang paling *fleksibel* karena setiap *client* tidak harus menunggu perintah dari *server* dan ketika ada penambahan ataupun pengurangan topologi ini tidak akan mengganggu bagian jaringan lain kerugian hanya saja akan memboros banyak kabel.

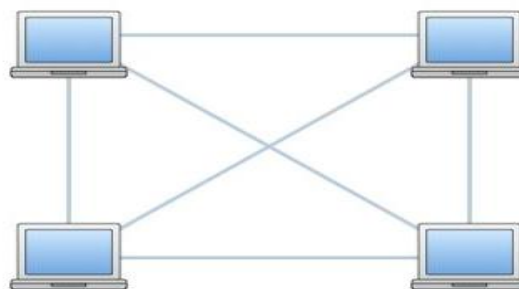
4. Topologi Tree



Gambar 2.7 *Topologi Tree*
Sumber : (Samsumar & Hadi, 2018)

Topologi Tree juga dikenal dengan topologi hierarki, yang mana topologi ini gabungan dari topologi bintang (*star*) dan topologi bus pada topologi ini setiap node akan bergantung pada node yang ada di atasnya, penerapan topologi jenis ini bisa dilakukan perusahaan yang mana dalam pengontrolan jaringan akan hanya dilakukan pada satu pusat saja.

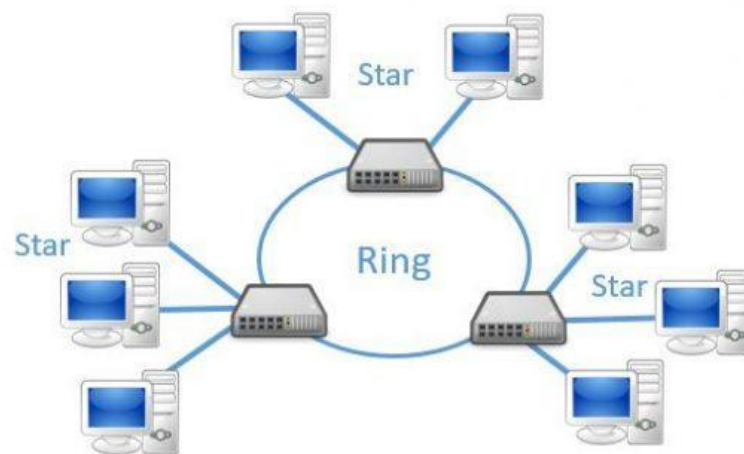
5. Topologi Mesh



Gambar 2.8 *Topologi Mesh*
Sumber : (Samsumar & Hadi, 2018)

Topologi yang setiap komputernya saling terkoneksi satu sama lain, penerapan topologi jenis ini biasanya pada jaringan WAN.

6. Topologi Hybrid



Gambar 2.9 *Topologi Hybrid*
Sumber : (Samsumar & Hadi, 2018)

Topologi Hybrid adalah kombinasi dari dua atau lebih jenis topologi jaringan yang berbeda dalam satu jaringan yang sama. Ketika digabungkan dua atau lebih topologi maka dia akan membentuk sebuah *topologi hybrid*.

2.1.4 Jenis serangan pada jaringan komputer

Di Sebuah perusahaan tentunya dalam melakukan serangkaian pekerjaan tentunya menggunakan jaringan dalam berbagi data informasi, tidak dapat dipungkiri lagi ini akan menjadi area yang sangat rentan terhadap berbagai jenis serangan. Dengan diciptakan perangkat yang dapat membatasi penggunaan jaringan serta memberikan keamanan pada jaringan yang terhubung pada perangkat tersebut

(*Network Switch*), akan tetapi dengan menggunakan jaringan *nirkabel* keamanan tersebut masih bisa di susupi oleh pihak secara tidak sah. Dua model jenis serangan pada jaringan komputer yakni serangan aktif dengan menggunakan *signal jammer* untuk mengganggu transmisi data dan model *pasif* yang berfokus pada penyadapan data (Prakasa, 2020).

Menurut (Prakasa, 2020) dalam penelitian yang dilakukan semakin berkembangnya kemajuan teknologi maka juga akan diikuti juga dengan perkembangan teknik penyerangan terhadap teknologi tersebut. Dapat dilihat dari berbagai serangan yang belakangan sering terjadi diantaranya serangan *malware* dimana seseorang memasukan sebuah virus seperti (*worm, trojan, ransomware dan spyware*) dan serangan *phising* dengan upaya untuk mendapatkan informasi sensitive seperti kata sandi dan nomor kartu kredit. Beberapa bentuk ancaman penyerangan yang sering terjadi dalam sistem keamanan jaringan mikrotik, yaitu :

2.1.4.1 Brute Force

Algoritma *brute force* adalah sebuah metode pencarian dan pemecahan masalah dengan mencoba semua kemungkinan kombinasi yang dilakukan secara berurutan untuk mencari solusi atau jawaban yang benar. Dalam konteks jaringan komputer, algoritma *brute force* digunakan oleh peretas dalam menebak atau untuk mendapatkan kata sandi atau kunci *enkripsi* yang tidak diketahui (Mulyanto et al., 2022).

Menurut (Syaifuddin et al., 2018) *Brute force* adalah sebuah upaya dalam menerka dan menebak kemungkinan kode atau *password* yang disembunyikan dan dengan tujuan tertentu, dalam melakukan *brute force*. Dapat disimpulkan bahwa

sebuah teknik yang dilakukan dengan cara menebak password dan mengkombinasikan semua kemungkinan password dengan menggunakan beberapa kemungkinan karakter, meskipun algoritma ini berhasil akan tetapi dalam melakukan serangan *brute force*, akan memakan waktu yang lama dikarenakan peretas akan menerka atau menebak kemungkinan kode yang di enkripsi secara berurutan. Tentunya ini tidak efektif untuk dilakukan.

2.1.4.2 Port Scanning

Port scanning merupakan sebuah teknik *hacking* yang dilakukan oleh pihak tertentu yang mana melakukan pembobolan terhadap website atau web server melalui *port* yang terbuka dan di eksekusi (Mulyanto et al., 2022). Dengan kata lain *port scanning* ini adalah sebuah teknik yang digunakan oleh pengguna untuk mencari dan mengidentifikasi port yang terbuka pada sistem komputer dan perangkat jaringan. Dalam dunia *cyber port scanning* sering digunakan oleh seorang hacker dalam mencari celah keamanan dalam sistem yang dapat dimasuki.

2.1.4.3 Secure Shell (SSH)

SSH (Secure Shell) merupakan protokol keamanan dan metode yang digunakan untuk mengamankan akses ke perangkat jaringan komputer dari jarak jauh. Pada SSH terdapat fitur yang disediakan yakni *enkripsi data*, *autentifikasi*, dan keamanan lainnya yang digunakan dalam melindungi informasi ketika berbagi informasi pada perangkat yang terhubung yang mana ini memungkinkan pengguna untuk mengakses, mengelola dan mengendalikan perangkat atau server dari jauh dengan aman (Desmira & Wiryadinata, 2022b).

Port SSH (Secure Shell) begitu populer di kalangan perusahaan besar di Indonesia karena begitu banyaknya perusahaan di Indonesia menggunakannya dalam keamanan jaringan komputer mereka, perbandingan penggunaan *port SSH* dalam penelitian ini yakni menggunakan metode *port knocking*. Adapun kelebihan dapat dilakukan dengan menggunakan SSH (*Secure Shell*) diantaranya pengguna dapat mengakses sebuah perangkat jaringan atau server dari lokasi yang jauh dengan menggunakan koneksi SSH dan pengguna juga dapat membentuk sebuah “*tunnel*” atau jalur yang aman antar dua perangkat dalam berbagi informasi (Desmira & Wiryadinata, 2022a).

2.1.5 Serangan Terhadap Perangkat keras (*Hardware*)

Serangan terhadap perangkat keras adalah upaya yang dilakukan oleh penyerang untuk merusak, meyakotase atau mendapatkan akses yang tidak sah ke perangkat keras fisik yang digunakan dalam sistem komputer atau jaringan. Serangan terhadap perangkat keras merupakan ancaman yang serius karena dapat menyebabkan kerusakan fisik, kegagalan perangkat dan pelanggaran keamanan data. Dalam penelitian yang dilakukan oleh Alves & Moris yang dikutip oleh (Prakasa, 2020) Menjelaskan Serangan *malware* terhadap perangkat keras, juga dikenal sebagai "*malware* berbasis perangkat keras" atau "*malware* tingkat rendah", adalah jenis serangan yang menargetkan tingkat perangkat keras fisik dalam sistem komputer. *Malware* semacam ini dapat menyusup ke dalam komponen perangkat keras, seperti BIOS (*Basic Input/Output System*), *firmware*, atau bagian lain dari *hardware*, dan menyebabkan kerusakan atau merusak operasi perangkat keras tersebut. Ini adalah jenis serangan yang lebih canggih dan jarang terjadi daripada

malware yang biasa kita kenal (seperti virus atau *worm* yang beroperasi di tingkat perangkat lunak).

2.1.6 Serangan Terhadap Perangkat Lunak (*Software*)

Terdapat beberapa serangan terhadap perangkat lunak (*software*) dikelompokkan sebagai berikut:

1. Serangan terhadap sistem operasi

Menurut (Prakasa, 2020) serangan terhadap sistem informasi sebagian besar menargetkan memori atau dikenal dengan istilah *memory-corruption vulnerability*, dan serangan *rowhammer* yang menyerang DRAM sehingga dapat mengakibatkan ketidakstabilan sistem operasi (*crash*) atau bahkan mengakibatkan *privileges escalation*. Dalam dibuktikan jika melakukan akses ke alamat memori yang terlarang dapat mengakibatkan pengguna bisa menjalankan aplikasi *setar administrator (root)*.

Ancaman serangan terhadap keamanan sistem operasi dapat dikatakan sebagai *CLKScrew* dalam istilah lainya dimana seorang *hacker* bertindak dengan cara mengganggu sistem kelistrikan melalui *software*. Terdapat beberapa serangan terhadap keamanan sistem operasi yang pernah terjadi diantaranya serangan yang terjadi pada sistem operasi pada tahun 2017 yang disebut serangan *WannaCry* adalah jenis serangan *ransomware* yang menyerang ribuan organisasi diseluruh dunia yang mana serangan ini mengeksploitasi kerentanan pada sistem operasi windows yang belum diperbaharui, juga termasuk windows XP yang sudah tidak didukung dan

serangan *NotPetya* pada tahun 2017, *NotPetya* merupakan jenis serangan *malware* yang menargetkan pada perusahaan-perusahaan besar diseluruh dunia yang mana serangan ini menggunakan kerentanan pada perangkat lunak akuntansi ukraina untuk menyebarkan virus dan merusak sistem.

2. Serangan terhadap layanan sistem operasi (*services*)

Pada layanan sistem operasi (servis) terdapat sebuah layanan yang berfungsi untuk memberikan layanan terhadap sistem, ancaman terhadap layanan sistem layanan yakni *Distributed Denial of Services (DDoS)* (Prajapati et al., 2019).

Tujuan dari serangan ini adalah membuat kemacetan di layanan *service* (missal HTTP) sehingga tidak dapat melayani permintaan dari pengguna lainnya dan website tidak dapat diakses. Serangan lain yang pernah terjadi adalah serangan pada *secure shell (ssh)*, Teknik yang dilakukan untuk menyerang SSH adalah dengan melakukan *brute-force attack*. Teknik ini merupakan teknik yang sudah cukup lama digunakan dan dinilai kurang efektif, namun dengan adanya *botnet* teknik ini jauh lebih efektif dibandingkan dengan teknik sebelumnya. *Botnet* biasanya digunakan untuk melakukan serangan *cyber* termasuk serangan DDoS (*Distributed Denial of Service*), *spamming* dan pencurian data.

3. Serangan terhadap aplikasi

Serangan terhadap aplikasi adalah upaya yang dilakukan oleh penyerang untuk mengeksploitasi kerentanan dalam aplikasi perangkat lunak guna mendapatkan akses tidak sah, mencuri data, menyebabkan kerusakan, atau melakukan tindakan berbahaya lainnya. Aplikasi perangkat lunak adalah sasaran yang menarik bagi penyerang karena seringkali mengandung kerentanan yang dapat dimanfaatkan untuk memasuki sistem secara tidak sah (Prakasa, 2020).

2.1.7 Serangan Terhadap Basis Data

Serangan terhadap basis data adalah upaya yang dilakukan oleh penyerang untuk mengeksploitasi kerentanan dalam sistem basis data guna mendapatkan akses tidak sah, mencuri data sensitif, merusak atau mengubah data, atau menyebabkan gangguan pada operasi basis data. Basis data merupakan kumpulan data yang disimpan dalam sistem yang terstruktur, dan serangan terhadapnya dapat menyebabkan kerugian yang signifikan bagi organisasi atau individu yang terkena dampaknya (Prakasa, 2020).

2.2 Teori Khusus

2.2.1 Keamanan Jaringan

Keamanan jaringan merupakan suatu proses yang berkaitan dengan upaya untuk melakukan pencegahan, mengidentifikasi ancaman serangan keamanan jaringan serta menghentikan segala macam upaya yang dilakukan oleh penyusup untuk dapat masuk kedalam jaringan komputer serta sistem jaringan

Keamanan jaringan (*Network Security*) merupakan segala bentuk aktivitas yang dilakukan dalam mengamankan sebuah jaringan (*Network*), terlebih untuk melindungi *usability, availability, reliability, integrity* dan *safety* dari jaringan dan data. Tujuan dari *network security* adalah bagaimana upaya dalam mencegah dan menghentikan ancaman serangan (*threats*) agar tidak masuk dan menyebar di jaringan kita, yang mana untuk keamanan jaringan mencakup dari perangkat keras dan perangkat lunak (Fauzan & Purwanto, 2021).

Keamanan Jaringan komputer merupakan suatu proses dalam mencegah dan mengidentifikasi pengguna yang tidak berhak dalam mengakses jaringan komputer, untuk mengantisipasi dan mencegah ancaman keamanan jaringan komputer maka diperlukannya suatu langkah langkah dalam pencegahannya supaya penyusup tidak dapat masuk kedalam sistem jaringan.

Menurut (Amien, 2020) ada tiga aspek dalam keamanan jaringan antara lain sebagai berikut :

1. *Confidentiality*

Kerahasiaan (*Confidentiality*) menunjukkan bahwa sebuah informasi dan data hanya dapat diakses oleh pihak yang diberi izin untuk mengakses sebuah keamanan jaringan. Aspek kerahasiaan bertujuan untuk melindungi data dari akses yang tidak sah atau penyebaran yang tidak diizinkan.

2. *Integrity*

Integrity yaitu bagaimana seorang pengguna dapat memastikan suatu informasi atau data didalam jaringan tetap utuh, tidak diubah atau dimanipulasi secara tidak sah selama pengiriman ataupun penyimpanan.

Aspek dari *integrity* ini bertujuan untuk melindungi sebuah data dari modifikasi yang tidak sah, penyisipan data palsu atau perubahan data yang tidak di inginkan yang akan menyebabkan kerugian atau kerusakan.

3. *Availability*

Ketersediaan (*Availability*) dalam jaringan mengacu pada kemampuan sebuah sistem atau layanan jaringan untuk dapat beroperasi, aktif, dan dapat diakses oleh pengguna secara sah dan konsisten tanpa gangguan. Aspek *availability* ini mengacu pada pentingnya menjaga ketersediaan sebuah layanan dan sumber daya jaringan agar dapat diakses dan digunakan sesuai dengan kebutuhan.

2.2.2 Mikrotik



Gambar 2.10 Mikrotik
Sumber : (Ardianto, 2020)

Mikrotik merupakan sebuah sistem aplikasi router, yang di kenalkan dengan nama *mikrotik routerOs* yang dapat kita install di setiap komputer, namun tidak seperti sistem operasi sistem router lainnya yang mana hanya bisa di install pada

hardware tertentu saja, kelebihan dari router ini sendiri adalah mudah dikonfigurasi dan harga yang diberikan juga bervariasi sesuai dengan kebutuhan penggunanya. Serta mikrotik ini berfungsi dalam membagi koneksi internet ke beberapa pengguna (Ardianto, 2020).

Mikrotik merupakan sebuah perangkat jaringan komputer yang berupa *hardware* dan *software* yang berfungsi sebagai router, sebagai alat untuk *filtering*, *switching*, pengaturan *bandwidth*, dan *wireless access point* yang berguna untuk *client* maupun *server* sehingga sangat cocok untuk *routing* digunakan jaringan perusahaan bahkan juga dapat digunakan oleh ISP dan *provider hotspot* (Hidayat et al., 2022). Router mikrotik adalah satu solusi dari masalah keamanan jaringan komputer dikarenakan fitur-fitur yang terdapat pada router mikrotik dapat digunakan dalam manajemen jaringan, sebagai perangkat jaringan yang bersifat *open source* dikarenakan router mikrotik ini dapat disesuaikan dengan *network* yang berbeda yakni bisa digunakan untuk *cable network* maupun *wireless network* yang memungkinkan siapa saja dapat merubahnya sesuai dengan kebutuhannya (Tasanah Assakur et al., 2020). Beberapa pandangan para ahli mengenai mikrotik

Menurut Herlambang yang dikutip oleh (Asnawi, 2018) mikrotik Router OS adalah *Operating System* (OS) yang dirancang secara khusus sebagai jaringan router (*network router*), menggunakan *personal computer* yang dijadikan sebagai *network router* dengan cara memasang mikrotik router OS.

Menurut (Asnawi, 2018) awalnya mikrotik dikembangkan di suatu daerah yang bernama Latvia, yang dikembangkan oleh Jhon Trully dan anies, dengan dikembangkan nya mikrotik ini akan membuat router dapat diakses serta dapat

dikembangkan serta digunakan di seluruh dunia prinsip inilah yang ditanamkan oleh *John Trully* dan *Anies*.

2.2.3 Keamanan Sistem Jaringan

Keamanan sistem jaringan menurut merupakan segala bentuk upaya pencegahan serta mengidentifikasi pengguna jaringan yang tidak sah (penyusup) dalam mengakses jaringan. Sistem keamanan jaringan adalah kunci dalam menjaga kestabilan dan epektifitas jaringan (Wicaksono, 2022).

Dalam keamanan jaringan sistem lebih merujuk pada kumpulan perangkat keras, perangkat lunak, protokol, kebijakan dan prosedur yang digunakan dalam upaya melindungi jaringan komputer dari ancaman keamanan serta menjaga integritas, kerahasiaan dan ketersediaan data, dalam keamanan jaringan terdapat beberapa elemen yang saling bekerja sama dalam melindungi jaringan dari ancaman serangan yang dapat merugikan. Terdapat beberapa pemahaman tentang sistem dalam sudut pandang para ahli yaitu sebagai berikut :

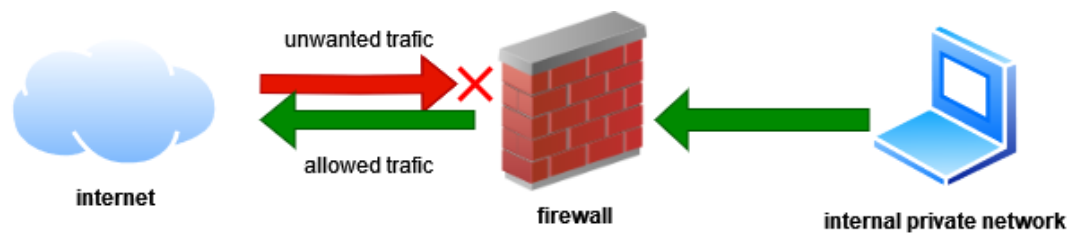
1. Menurut (Saputra et al., 2019) dalam Arifin Rahman menjelaskan sistem dalam kamus *Webster New Collegiate Dictionary* berpendapat bahwa sistem berasal dari bahasa Yunani yang mana “syn” dan “Histana” yang diartikan menempatkan bersama.
2. Menurut (Saputra et al., 2019) dalam Ludwig Von Bertalanffy sistem adalah kesatuan yang kompleks yang terdiri dari elemen-elemen yang saling berinteraksi secara saling bergantung sehingga membentuk satu kesatuan yang fungsional.

3. Menurut (Basuki, 2019) dalam Fagen Dan A.HALL menjelaskan sistem merupakan suatu kumpulan objek yang meliputi hubungan antara suatu objek dengan objek lain serta hubungan dengan sifat yang mereka miliki.

2.2.4 Firewall Filtering

Firewall merupakan jenis keamanan jaringan yang berguna untuk memfilter serta mengontrol lalu lintas jaringan yang masuk dan memblokir paket data yang dianggap mencurigakan, *firewall* juga digunakan untuk melindungi, membatasi dan menolak jaringan pribadi dengan jaringan luar yang terdeteksi dapat mengancam keamanan jaringan (Wicaksono, 2022). Jika ada pihak yang mencoba untuk melakukan pengaksesan maka sistem *firewall* akan otomatis memblokir pihak yang tidak bersangkutan tersebut oleh *firewall*, sistem kerja dari firewall sendiri akan mengikuti kebijakan yang dibuat oleh administrator jaringan.

Sistem kerja dari firewall menggunakan cara *studying the deployment rule-set*, dimana *the rule-set* dibuat dengan sedemikian rupa supaya setiap data yang masuk akan diperiksa oleh *firewall* dan dilakukan analisa setiap data yang keluar dengan sistem *rule-set*. *Filter firewall* mempunyai suatu ketentuan yang dibuat *rule-set* yang mana untuk dapat mengatur lalu lintas dari paket tersebut sebelum paket tersebut di izinkan masuk, *firewall filtering* juga dapat memblokir lalu lintas data yang masuk jika terdapat data yang mencurigakan. *The Rule-set* untuk *firewall* tersebut akan dikonversikan menjadi sebuah kode tertentu yang digunakan pada *firewall* sehingga nantinya perangkat komputer dapat mengeksekusi sesuai dengan perintah yang ada (Khadafi et al., 2019).



Gambar 2.11 Cara kerja *Firewall*

Sumber : (Data Penelitian, 2023)

Firewall merupakan sebuah bentuk pengamanan yang penting, akan tetapi pertahanan keamanan jaringan yang efektif juga memerlukan kombinasi dari berbagai teknologi serta praktik keamanan yang berlapis lapis untuk melindungi jaringan. *firewall* dapat dibedakan menjadi dua *hardware* dan *software* berikut penjelasannya :

1. *Firewall* berbasis *hardware*

Firewall berbasis *hardware* merupakan piranti perangkat keras yang berada dalam perangkat jaringan komputer seperti router. *Firewall* berbasis perangkat keras merupakan jenis *firewall* yang diimplementasikan dengan menggunakan perangkat keras khusus yang dirancang khusus untuk menyaring dan mengamankan lalu lintas jaringan. *Firewall* berbasis *hardware* memiliki perangkat fisik yang berdiri sendiri dan berfungsi sebagai pertahanan sendiri dalam keamanan jaringan (Gregorius Hendita Artha Kusuma, 2022).

2. *Firewall* berbasis *software*

Firewall berbasis perangkat lunak adalah jenis *firewall* yang diimplementasikan dengan menggunakan perangkat lunak yang berjalan di atas sistem operasi komputer yang mana fungsi dari *firewall* berbasis perangkat lunak

untuk menyaring serta mengamankan lalu lintas jaringan. *Firewall* berbasis *software* biasanya melindungi *trafik inbound* dan juga *outbound*, selain itu juga dapat menghindarkan sistem dari berbagai macam virus seperti *trojan* dan *worm* (Gregorius Hendita Artha Kusuma, 2022).

2.2.5 Port Knocking

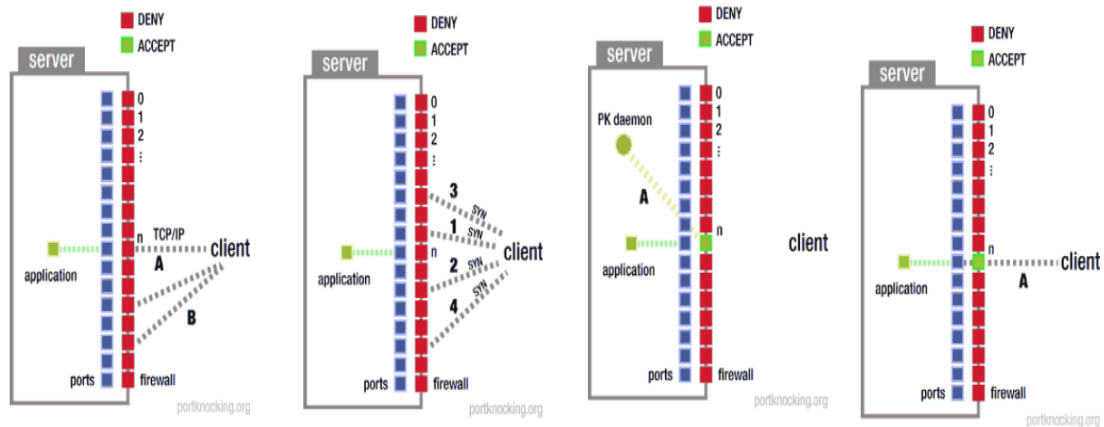
Menurut (Mulyanto et al., 2021) *Port Knocking* Merupakan suatu metode yang digunakan dalam upaya meningkatkan keamanan pada lapisan utama pada jaringan, serta memberikan perlindungan terhadap keamanan jaringan dari ancaman serangan jaringan seperti serangan *scripts kiddies* dan serangan *port scanning*. Dan memberikan hak akses terhadap pengguna untuk mengakses port yang dibuka dan menutup port kembali dan menggunakan *firewall* untuk menghapus *rule* yang pernah di eksekusi sebelumnya.

Menurut (Saputro et al., 2020) *port knocking* merupakan sebuah teknik keamanan jaringan yang digunakan untuk menyembunyikan layanan jaringan dari pemeriksaan secara rutin yang dilakukan oleh penyusup atau penyerang. Teknik tersebut bertujuan untuk mengaktifkan akses ke port tertentu setelah urutan koneksi yang tepat ke port -port dengan pola yang telah ditentukan sebelumnya sehingga ini mengharuskan pengguna untuk selalu memberikan keamanan ekstra terhadap port yang terbuka sehingga dapat mencegah terjadinya pencurian data.

Port knocking merupakan suatu metode yang digunakan dalam mengotorisasi sebuah pengguna berdasarkan *firewall* untuk dapat melakukan komunikasi melalui port, yang mana metode *port knocking* ini menggunakan sistem autentifikasi dalam pengiriman sebuah data atau file, dimana informasi yang

dikirimkan akan dikodekan bahkan di enkripsi sesuai dengan urutan nomor port, urutan ini disebut juga dengan *knock* (ketukan).

Alur kerja dari *port knocking* sendiri dapat dijelaskan berdasarkan gambar berikut, pada gambar 2.12 sebagaimana diketahui sebuah komputer server tidak akan menyediakan port terbuka untuk pengguna jaringan dan *server* juga akan mengawasi segala macam upaya untuk koneksi dapat masuk ke dalamnya. Untuk memulai koneksi *client*, dimulai dengan cara koneksi ke *server* dengan beberapa urutan ke *well-defined set of ports*, yang mana akan mengirimkan paket SYN atau *synchronous* ke *port* yang telah ditetapkan sebelumnya dalam *knock* atau ketukan. Proses *knock* inilah yang menyebabkan sebuah *port* mengetuknya, sedangkan yang terjadi pada *server*, yaitu *server* tidak akan memberikan respons terlebih dahulu kepada *client* selama *fase knock*, namun secara tidak diketahui dari *server* akan menerjemahkan yaitu *decodes* dan *decrypt* pada serangkaian urutan *port-port* untuk dapat diperiksa otentifikasinya. Maka server akan mengeksekusi perintah yang diterima sehingga server dapat merespon dan klien dapat melakukan transfer data (Khadafi et al., 2019).



Gambar 2.12 Proses *Port Knocking*
Sumber : (Khadafi et al., 2019)

2.2.6 Telegram Bot

Telegram merupakan sebuah aplikasi bersifat *open source* yang dapat kita download melalui playstore dengan gratis telegram lebih berfokus pada kecepatan dan keamanan. Telegram adalah sebuah aplikasi instan yang populer yang dapat menyediakan layanan pesan teks, panggilan suara, panggilan video serta berbagi file, didalam telegram kita juga dapat membuat group dengan beranggotakan sebanyak 5000 orang atau bisa juga *channel broadcasting* untuk pengguna secara terbatas (Fernando et al., 2020).

Beberapa fitur yang ditawarkan oleh telegram messenger sebagai berikut :

1. Menyediakan keamanan pesan dengan dienkripsi end-to-end dan fitur penghapusan pesan otomatis.
2. Dapat mengatur penghapusan pesan dengan waktu yang ditentukan.
3. Menyimpan file dalam *cloud*.
4. Telegram dapat digunakan diberbagai platfrom seperti android, Ios, windows, macOS dan versi web.

Menurut (Fernando et al., 2020) terdapat dua jenis API yang dapat digunakan oleh pengembang sebagai berikut :

1. Bot API memungkinkan seorang pengembang untuk dapat menghubungkan Bot ke dalam sistem telegram. Telegram *Bots* merupakan program atau skrip pada komputer yang dijalankan di platform telegram dan berfungsi untuk memberikan layanan dan interaksi dengan pengguna lain dalam pesan teks, gambar maupun video.
2. API Telegram memungkinkan pengembang untuk membuat klien telegram yang mereka inginkan. API telegram bersifat *open source* yang mana para pengembang dapat dengan mudah membangun aplikasi di platform telegram.

API (*Application Programming Interface*) merupakan sebuah antarmuka yang memberikan kemudahan bagi pada pengikat, mitra maupun pihak ketiga dalam membangun atau mengembangkan sebuah aplikasi seperti aplikasi Iphone dengan cepat. API Telegram dan Facebook merupakan dua contoh aplikasi yang sudah terkenal, selain itu API juga bermakna sekumpulan perintah, fungsi, protokol, dan objek yang dibuat oleh seorang *programmer* sehingga perangkat tersebut mampu berinteraksi dengan sistem *eksternal*. Adapun manfaat dan kegunaan API secara khusus akan dirasakan oleh *developer* dikarenakan API mampu meningkatkan *efisiensi waktu, fleksibilitas*, serta menghemat biaya (Hidayat et al., 2022). Cara kerja API (*Application Programming Interface*) dapat dilihat pada gambar berikut :



Gambar 2.13 Cara kerja API
Sumber : (Hidayat et al., 2022)

Berdasarkan gambar diatas dapat dijelaskan sebagai berikut :

1. Aplikasi akan mengakses API, kemudian API akan merespon dengan melakukan pekerjaan setelah user/pengguna membuka aplikasi
2. API akan mengirimkan permintaan ke *server*, setelah aplikasi berhasil mengakses alamat API, permintaan akan diteruskan ke server pengguna, sehingga API akan memberikan perintah untuk mengirimkan data sesuai *request* yang diminta oleh aplikasi.
3. Server akan merespon permintaan dari API jika permintaan data tersebut sesuai maka server akan mengirimkan data API berupa respon
4. Terakhir API akan memberikan informasi sesuai dengan permintaan aplikasi, seperti informasi yang diberikan ke aplikasi sehingga dapat diakses oleh pengguna

2.3 Software pendukung

1. FileZilla



Gambar 2.14 FileZilla
Sumber : (Rafi & Saudi, 2021)

FileZilla merupakan sebuah aplikasi pengiriman file yang bersifat *open source* dengan antar muka yang intuitif serta dengan fitur yang tersedia membuat aplikasi ini mudah digunakan. *Filezilla* juga dapat memungkinkan pengguna untuk *mentransfer file* antar komputer lokal dan server dalam jangkauan jarak jauh secara cepat dan aman.

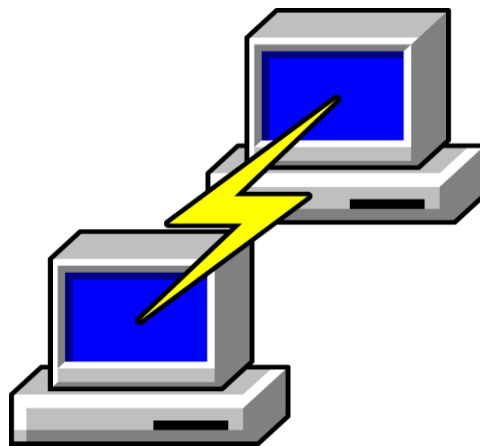
Menurut (Rafi & Saudi, 2021) dalam penelitiannya menjelaskan *filezilla* adalah sebuah aplikasi jaringan yang digunakan untuk mengirim file melalui jaringan lokal dan juga internet melalui protokol FTP, yang mana aplikasi ini dikembangkan oleh tim Kosse dengan keunggulan dalam segi kenyamanan dan kecepatan dalam proses *transfer file*. Ada beberapa fitur yang ditawarkan pada aplikasi *FileZilla* diantaranya sebagai berikut:

1. Pada aplikasi *FileZilla* memungkinkan manajemen situs membuat daftar rincian situs FTP dan koneksinya seperti nomor yang dipakai pada port,

portokol yang digunakan serta menggunakan protokol anonim atau regular.

2. *Log* pesan yang ditampilkan diatas pada atas jendela aplikasi yang berfungsi untuk menampilkan perintah yang dikirim oleh *FileZilla* serta respon yang terima oleh server.
3. Pada aplikasi *FileZilla* tampilan dari file dan folder muncul pada bagian bawah *log* pesan
4. Antrian transfer data yang ditampilkan dibagian bawah untuk mengetahui status dari pengiriman data apakah aktif atau status pengiriman masih secara *real time*.

2. Putty



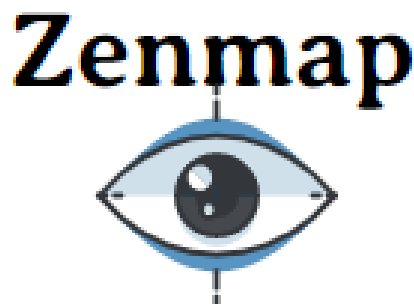
Gambar 2.15 *Putty*
Sumber : (Mulyanto et al., 2021)

Putty merupakan sebuah perangkat jaringan komputer yang dapat menghubungkan antara komputer lokal dengan komputer lain dengan jarak yang cukup jauh menggunakan sebuah protokol jaringan seperti *SSH*, *Telnet*, *rlogin*, dan

serial. Program pada *putty* lebih banyak digunakan oleh pengguna menengah keatas yang mana dapat digunakan untuk banyak hal yang berhubungan dengan jaringan seperti melakukan simulasi keamanan jaringan dan memantau keamanan jaringan (Mulyanto et al., 2021).

Konfigurasi pada aplikasi *Putty* dengan cara melakukan pengelolaan perangkat dari jarak jauh melalui konsol yang disediakan oleh protokol SSH atau telnet. Dalam penggunaan aplikasi *putty* pengguna harus memiliki izin yang sah dari pihak yang akan diakses.

3. Zenmap



Gambar 2.16 *Zenmap*
Sumber : (Wicaksono, 2022)

Zenmap merupakan sebuah aplikasi grafis yang banyak digunakan untuk memindai jaringan serta menganalisa keamanan jaringan. *Zenmap* merupakan sebuah aplikasi layanan jaringan yang bersifat terbuka dan tersedia untuk berbagai sistem operasi seperti *windows*, *macOS*, dan *Linux* (Wicaksono, 2022). Terdapat beberapa fitur pada aplikasi *zenmap* diantaranya sebagai berikut :

1. Pemindaian jaringan, pengguna dapat melakukan pemindaian ke host atau rentang ip tertentu dan zenmap akan memberikan informasi mengenai terhadap perangkat yang terhubung seperti alamat IP, port yang terbuka, dan layanan yang dijalankan.
2. Pemindaian port dengan aplikasi zenmap pengguna dapat melakukan pemindaian terhadap host dan jaringan tertentu sehingga ini akan membantu pengguna dalam mengidentifikasi potensi kerentanan dan dapat mengambil tindakan untuk mengamankan jaringan.
3. Pemetaan jaringan, ini akan membantu pengguna dalam memahami struktur jaringan dan mengidentifikasi titik rawan yang perlu diperhatikan.
4. Analisa keamanan , dengan aplikasi zenmap pengguna akan dengan mudah dapat menganalisa keamanan jaringan seperti mengetahui celah yang rentan terhadap keamanan dan memberikan informasi untuk untuk pengujian keamanan lebih lanjut.
5. Pelaporan dan penyimpanan hasil, aplikasi zenmap menyediakan fitur untuk menyimpan hasil pemindaian dalam bentuk file tentunya hal ini dapat dimanfaatkan untuk analisa lebih lanjut bagi seorang administrator jaringan.

Dengan adanya beberapa fitur yang terdapat pada aplikasi zenmap tentunya ini akan memberikan kemudahan kepada administrator jaringan dalam mengidentifikasi serta menganalisis dan memperbaiki kerentanan yang ada dalam jaringan.

2.4 Penelitian Terdahulu

Dalam penelitian ini terdapat beberapa artikel jurnal yang menjadi acuan dalam melakukan penelitian ini diantaranya sebagai berikut :

1. Nama pengarang (Fahana et al., 2017). Judul: Pemanfaatan Telegram Sebagai Notifikasi Serangan Untuk Keperluan Forensik Jaringan. Tahun: 2017. E-ISSN : 2579-5341. Forensik jaringan merupakan hal yang sangat penting dalam mengidentifikasi dan mengatasi serangan *cyber* pada jaringan. Penelitian ini memanfaatkan platform telegram dalam memberikan pemberitahuan secara instan dan cepat dan penggunaan *snort* berguna untuk merekam serangan *Distributed Denial of Services (DDoS)* serta *traffic* data yang tersimpan di router yang tersimpan di *log* dan diteruskan ke aplikasi telegram instant *messaging* sebagai notifikasi untuk mengingatkan *administrator*. Telegram tidak hanya dapat digunakan sebagai notifikasi tetapi juga dapat digunakan sebagai tahap forensik jaringan untuk memperkuat bukti adanya penyerangan sebagai proses pengumpulan data untuk keperluan persidangan. Hasil dari penelitian ini akan memberikan keamanan ekstra pada jaringan dikarenakan telegram akan memberikan notifikasi jika terjadi serangan.
2. Nama pengarang (Hidayat et al., 2022). Judul: Bot Monitoring Jaringan Pada BMT Mentari Lampung Timur Menggunakan Mikrotik Dan API Telegram. Tahun: 2022. E-ISSN : 2620-3030, ISSN : 2620-3022. Notifikasi dalam jaringan merupakan hal yang sangat penting dalam memberikan

informasi terkini kepada *administrator* jaringan tentang kondisi server dan router. Metode penelitian yang digunakan dalam penelitian ini menggunakan metode *DIO Network Lifecycle* yang terdiri dari tahapan *design*, implementasi, dan operasi. Hasil dari penelitian menghasilkan BOT monitoring jaringan BMT Mentari Lampung Timur dengan menggunakan mikrotik dan API telegram. Sistem ini akan sangat membantu seorang administrator jaringan dalam mengelola dan memberikan notifikasi saat koneksi ke server BMT ketika mengalami masalah down atau up. Dengan demikian dengan adanya sistem notifikasi ini akan memberikan kemudahan bagi administrator jaringan dalam mengatasi permasalahan jaringan dengan cepat.

3. Nama pengarang (Fernando et al., 2020). Judul: Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang. Tahun: 2020. ISSN : 2722-4619, E-ISSN : 2722-4600. Monitoring keamanan jaringan pada infrastruktur T.I kota padang dilakukan dengan cara *real-time* dengan memonitoring kesehatan jaringan, status perangkat dan performa sistem. Dengan menggunakan platform telegram seorang administrator jaringan dapat menerima pemberitahuan instan tentang gangguan jaringan, masalah server atau ancaman serangan yang dapat terjadi sewaktu waktu. Dengan adanya sistem monitoring dan notifikasi , dinas komunikasi dan informatika kota padang dapat meningkatkan ketersediaan, keandalan, dan kinerja jaringan serta mengurangi waktu

downtime yang dapat mempengaruhi layanan pada sistem. Dengan adanya dukungan dari telegram akan memberikan kemudahan bagi dinas kota padang dalam menghadapi ancaman yang muncul.

4. Nama pengarang (Khadafi et al., 2019). Judul: Implementasi Firewall dan Port Knocking Sebagai Keamanan Data Transfer Pada FTP Server Berbasis Linux Ubuntu Server. Tahun: 2019. ISSN : 2615-6539. FTP (*File Transfer Protocol*) server yang menyediakan layanan transfer file antar mesin komputer dalam sebuah jaringan. FTP beroperasi pada lapisan layer OSI dengan menggunakan port 21 TCP (Transmission Control Protocol) sebagai port standar untuk dapat menginisialisasi koneksi transfer file antar klien dan sever. Untuk dapat meningkatkan keamanan FTP server dapat dengan menggunakan firewall untuk menutup port yang terbuka dan menggunakan port knocking dalam upaya meningkatkan kemanan yang mana ketika pengguna ingin mengakses ke layanan FTP maka di butuhkan otentifikasi. Dari hasil pengujian menunjukkan bahwa *rule-set* firewall yang diimplementasikan dapat menyembunyikan informasi mengenai port yang terbuka sehingga dapat mengurangi resiko serangan.

5. Nama pengarang (Iqbal et al., 2020). Judul : Analisa Dan Simulasi Keamanan Jaringan Ubuntu Server Dengan Port Knocking, Honeypot, IpTables, Icmp. Tahun: 2020. E-ISSN : 2615-8442. Keamanan jaringan komputer sangat penting dalam upaya melindungi kerahasiaan data dan

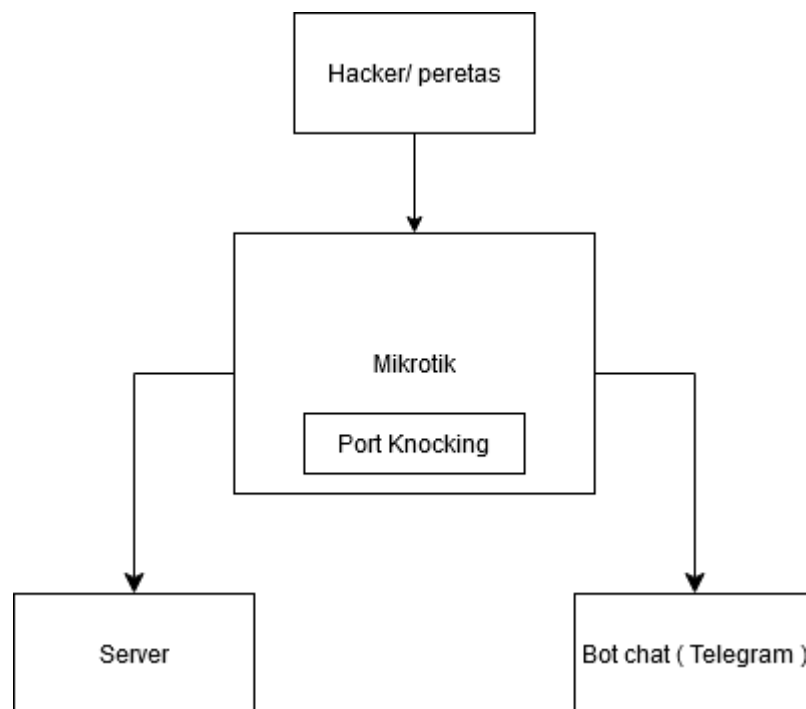
informasi pada server , serangan yang sering terjadi terhadap server seperti *brute force* dan *scan port*, dengan maraknya penyerangan maka server memerlukan perlindungan dengan menggunakan *firewall filtering* tapi ini kurang efektif dikarenakan *firewall* ini akan memblok siapa saja yang mencoba masuk tanpa terkecuali termasuk administrator. Dalam penelitian ini peneliti mengimplementasikan metode *port knocking* yang digabungkan dengan *Honeypot*, *Iptables* dan *ICMP* untuk meningkatkan keamanan server. *Iptables* digunakan untuk memfilter aturan port yang akan diizinkan sehingga paket port yang di tentukan saja yang dapat masuk ke server. *Port knocking* untuk memberikan *otentifikasi* dengan memberikan kode rahasia untuk dapat mengakses layanan ke *server* dan *honeypot* untuk mengalihkan *port service* ke port tiruan yang terbuka untuk mengetahui upaya ancaman serangan yang dilakukan pada *server* serta *ICMP* digunakan sebagai *ping request* untuk mengakses *server*.

6. Nama pengarang (Saputro et al., 2020). Judul : Demilitarized Zone And Port Knocking Methods For Computer Network Security. Tahun : 2020. E-ISSN 2615-8442. Dengan perkembangan dalam bidang komunikasi tentunya akan merubah seluruh aspek yang bergantung pada jaringan komputer dikarenakan perkembangan yang ada saat ini. Semakin *public* bergantung pada jaringan internet maka akan semakin besar pula potensi serangan terjadi. Teknik keamanan jaringan DMZ (*Demilitarized Zone*) dan *Port knocking* adalah dua pendekatan yang dapat diimplementasikan dalam

jaringan lokal maupun interlokal untuk meningkatkan keamanan server dan router dari serangan potensial. DMZ adalah jaringan yang berada diantara jaringan *internal (inside)* dan jaringan *eksternal (outside)* dan *port knocking* merupakan teknik yang memerlukan pengguna melakukan rangkaian koneksi ke port-port tertentu dengan urutan dan pola tertentu sebelum akses ke server atau router diberikan. Kedua teknik ini dapat memberikan keamanan tambahan pada server utama dan router, terutama dari serangan *DDoS* dan *port scanning*. Dengan menggunakan teknik keamanan ini hal yang harus diperhatikan dan dipertimbangkan yakni pada sisi seperti ruang penyimpanan fisik dan sistem enkripsi password pada server. Keamanan di area *inside* (dalam) juga harus menjadi perhatian utama karena teknik keamanan di DMZ dan *Port knocking* hanya melindungi area *outside* (luar).

2.5 Kerangka pemikiran

Penelitian tentang rancang bangun keamanan jaringan mikrotik menggunakan *firewall filtering* dan *port knocking* dengan notifikasi telegram yang mana menempatkan mikrotik router sebagai *server*, diperlukan suatu kerangka pemikiran mengenai rancang bangun keamanan jaringan supaya suatu perencanaan dapat berjalan dengan baik.



Gambar 2.17 Kerangka pemikiran
Sumber : (Data Penelitian, 2023)

Beberapa tahapan dalam kerangka pemikiran dalam rancang bangun sistem keamanan sebagai berikut :

1. *Hacker* / peretas

Ketika *hacker* mencoba untuk melakukan *port scanning*, *brute force* terhadap sistem keamanan jaringan mikrotik maka sistem keamanan jaringan mikrotik akan langsung merespon serangan tersebut dengan mengirimkan notifikasi ke aplikasi telegram

2. Mikrotik

Pada mikrotik administrator jaringan akan membatasi akses jaringan pada host yang diizinkan saja serta melakukan konfigurasi terhadap port knocking dengan mengubah aturan *firewall* secara dinamis yang mana pengaturan *firewall* ini berguna untuk memblokir akses yang tidak valid

3. Port knocking

Merupakan tahapan yang penting karena kita harus menentukan port yang dapat digunakan dalam *port knocking* dan *firewall* hanya akan aktif jika pola *port knocking* yang valid terdeteksi. Menggabungkan komponen komponen yang ada dalam merancang keamanan sistem jaringan mikrotik. Membangun keamanan pada jaringan mikrotik dengan menggunakan *firewall filtering* dan *port knocking*, serta menentukan batasan terhadap izin pengaksesan *port knocking* untuk membatasi kemungkinan percobaan mengakses secara illegal atau tidak sah.

4. Server

Server akan mengidentifikasi host yang dapat diakses melalui port knocking serta membuat skema *port knocking* yang tepat. Memilih dan mengkonfigurasi perangkat mikrotik sebagai *firewall*

5. Bot chat (Telegram)

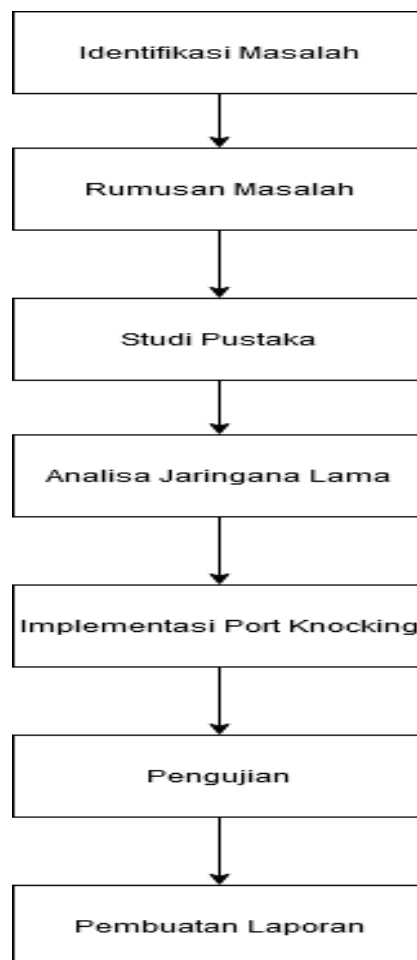
Mengkonfigurasi mikrotik untuk mengirimkan notifikasi melalui telegram menggunakan API bot serta membuat *skrip* yang akan mengirimkan notifikasi ke telegram ketika terjadi akses yang tidak valid terdeteksi. Melakukan pengujian terhadap sistem keamanan untuk memastikan keberhasilan *port knocking* dan notifikasi telegram dan memantau log keamanan mikrotik untuk mendeteksi serangan atau percobaan akses yang mencurigakan.

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Proses pada metode penelitian menggunakan beberapa tahapan yang dalam melakukan penelitian seperti digambarkan pada gambar berikut :



Gambar 3.1 Metode Penelitian
Sumber : (Data Penelitian, 2023)

Penjelasan mengenai proses pada metode penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :

1. Identifikasi masalah

Pada fase ini pendekatan dilakukan berkenaan dengan hal yang berkaitan dengan permasalahan yang sering terjadi di perusahaan atau instansi. Penelitian ini meliputi hal yang berkaitan dengan perangkat keras (*hardware*), perangkat lunak (*software*) dan berbagai bentuk ancaman serangan terhadap keamanan jaringan komputer sehingga masalah tersebut nantinya dapat diselesaikan dalam penelitian ini.

2. Perumusan masalah

Pada tahapan ini peneliti merumuskan masalah yang ada menjadi bagian yang lebih rinci sehingga masalah yang ada dapat diurutkan secara spesifik dan terperinci yang mana nantinya masalah tersebut dapat dijawab dengan melalui penelitian yang dilakukan.

3. Studi pustaka

Melakukan penelitian terhadap keamanan jaringan mikrotik sehingga dapat ditentukan langkah dalam rancang bangun jaringan mikrotik dan didapatkan gambaran komprehensif tentang hal apa saja yang telah ada sebagai teori yang mendasari dalam penelitian ini

4. Analisis jaringan lama

1. Melakukan analisis terhadap ancaman serangan terhadap sistem jaringan lama, dan pemodelan terhadap sistem jaringan baru.

2. Menjelaskan sistem kinerja jaringan lama sehingga dapat diambil kesimpulan untuk perbaikan terhadap sistem baru yang akan diusulkan
3. Perancangan desain antarmuka untuk sistem keamanan jaringan mikrotik yang baru yang akan dibangun.

5. Implementasi port knocking

Melakukan perencanaan dan langkah langkah yang dapat digunakan dalam menjaga keamanan jaringan sesuai dengan prinsip dasar dari *port knocking* yakni mendefinisikan suatu metode komunikasi antara dua komputer, yang mana suatu informasi dikirimkan secara *encode* dalam bentuk koneksi ke *port port* dalam urutan tertentu. Langkah langkah implementasi port knocking :

1. Dengan menentukan urutan *port knocking* yang akan digunakan seorang *administrator* jaringan akan dengan mudah dalam menjaga keamanan jaringan.
2. Dengan memberi ketentuan seperti memberikan durasi waktu terhadap hak izin dalam mengakses *port knocking* dengan benar, sehingga ketika terjadinya percobaan serangan maka seorang *administrator* jaringan dapat mengantisipasinya.
3. Membuka port tertentu untuk pihak yang berhak mengaksesnya saja, sehingga untuk keamanan akan berfokus pada port yang terbuka saja.

6. Pengujian

Jalankan pengujian terhadap sistem yang telah dirancang seperti melakukan percobaan untuk masuk ke sistem keamanan jaringan dengan paksa dan melihat ketika hal tersebut dilakukan apakah ada notifikasi ke aplikasi telegram kita yang kita gunakan sebagai pihak ketiga dalam pengujian ini. Uji semua konten yang ada apakah bekerja sesuai fitur dan fungsinya masing masing. Adapun langkah langkah dalam skenario pengujian sebagai berikut :

1. Menyiapkan skenario ancaman terhadap keamanan jaringan dan melakukan pengujian terhadap sistem keamanan jaringan untuk memastikan keberhasilan port knocking dan notifikasi telegram
2. Memantau *log* keamanan mikrotik dalam upaya mendeteksi serangan atau percobaan akses yang mencurigakan.

7. Pembuatan laporan

Membuat laporan mengenai rancangan dan hasil dari pengujian dengan menyertakan lampiran dari penelitian.

3.1.1 Teknik Pengumpulan Data

Dalam penelitian ini peneliti menggunakan dua cara dalam menggali informasi yaitu dengan melakukan observasi dan wawancara dengan tujuan untuk mendapatkan informasi yang berkaitan dengan tujuan penelitian ini. Dalam penelitian ini yang menjadi narasumber merupakan Bpk. Suwanda yang merupakan

direktur dari perusahaan PT. Shanaya Creativo Innovation adapun hal yang menjadi acuan dalam pengumpulan data ini adalah sebagai berikut :

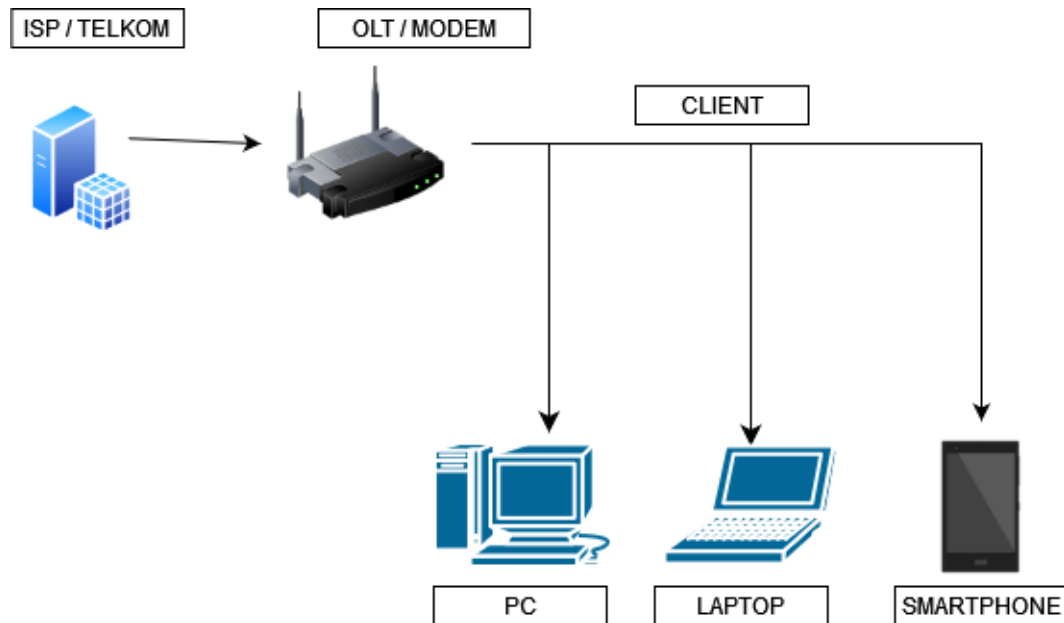
1. Observasi

Tahapan observasi dengan mendatangi perusahaan untuk melakukan pengamatan guna mendapatkan informasi yang diperlukan dalam penelitian ini. Pada tahapan observasi peneliti langsung mendatangi PT Shanaya Creativo Innovation guna untuk melihat dan mengamati kemungkinan resiko yang berkaitan dengan keamanan mikrotik di perusahaan ini serta mengumpulkan informasi yang menjadi titik fokus dalam penelitian.

2. Wawancara

Dalam penelitian ini, penulis melakukan wawancara bersama bapak Suwanda selaku direktur perusahaan, dengan mengajukan beberapa pertanyaan secara lisan dan tertulis guna untuk memperoleh informasi mendalam dan lengkap mengenai hal yang berkaitan dengan hal yang akan diteliti.

3.2 Analisis Jaringan Lama/ sedang berjalan



Gambar 3.2 Analisis Jaringan Lama
Sumber : (Data Penelitian, 2023)

Pada gambar diatas, proses keamanan yang berjalan pada PT. Shanaya Creativo Innovation pada bagian IT yang bertugas pada keamanan jaringan perusahaan, yang mana sistem yang diterapkan masih menggunakan sistem yang lama yaitu melakukan keamanan sistem yang masih menggunakan Laptop/PC (*Personal Computer*) dalam memantau lalu lintas jaringan yang sedang berjalan.

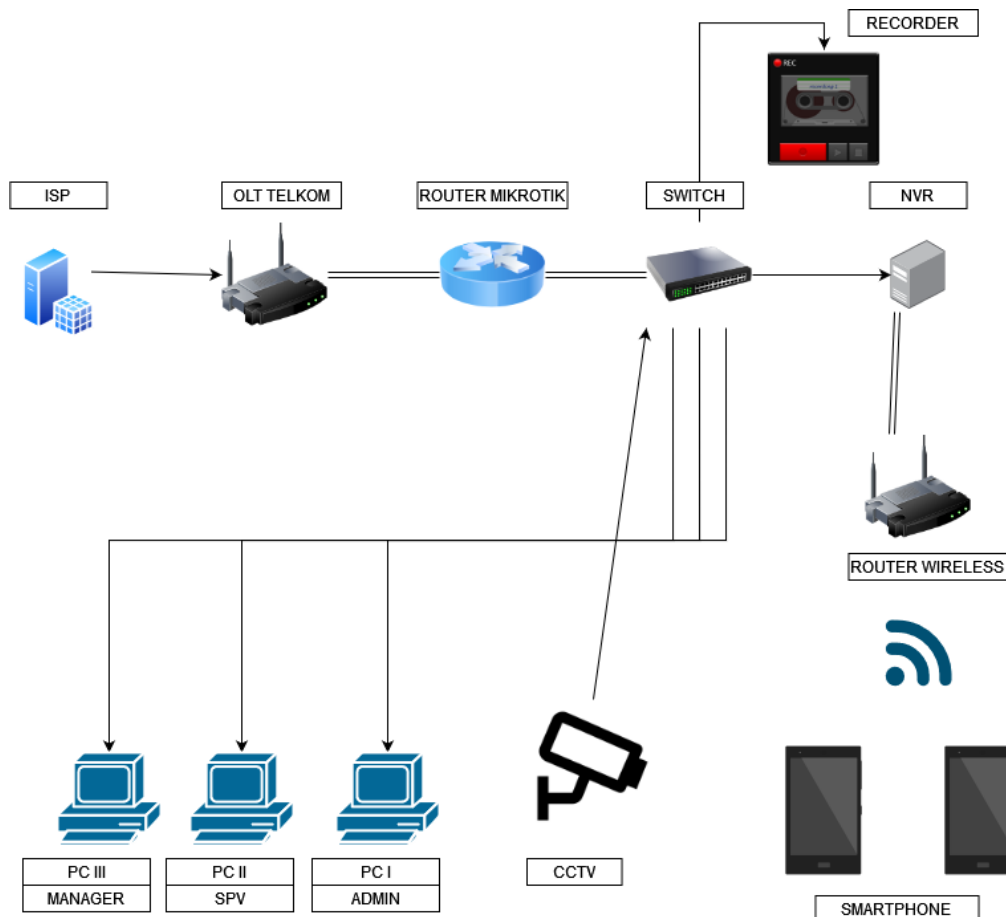
Proses pemantauan keamanan jaringan mikrotik untuk keperluan sebuah event pada PT. Shanaya Creativo Innovation masih menggunakan *personal computer* (PC) dengan langkah langkah sebagai berikut :

1. Langkah pertama para administrator jaringan akan masuk ke sistem server untuk memantau keamanan jaringan.
2. Selama memantau keamanan jaringan, para administrator harus selalu *standby* di depan komputer
3. Para administrator jaringan harus selalu ada di kantor untuk memantau keamanan jaringan.

Beberapa kelemahan ketika memonitoring keamanan jaringan menggunakan jaringan yang sedang berjalan diantaranya sebagai berikut :

1. Jaringan lama tidak menggunakan router mikrotik
2. Hanya megandalkan layanan dari ISP (*Internet Service Provider*)
3. Adanya potensi percobaan pembobolan keamanan jaringan di perusahaan.

3.3 Rancangan Jaringan yang diusulkan



Gambar 3.3 Sistem Jaringan Baru
Sumber : (Data Penelitian, 2023)

Pada gambar diatas ada beberapa usulan sistem keamanan jaringan di usulkan oleh peneliti, sehingga dapat memudahkan kinerja dari administrator jaringan yaitu dengan cara dengan menambahkan sebuah perangkat tambahan smartphone, yang mana nantinya peneliti akan mengimplementasikan API mikrotik untuk management sebuah router mikrotik yang berfungsi untuk membangun antarmuka antara dua perangkat yang berbeda. Jadi seorang *administrator* jaringan

nantinya dapat memantau sistem keamanan jaringan perusahaan melalui aplikasi telegram. Ketika ada pihak yang mencoba untuk masuk kedalam sistem keamanan jaringan mikrotik maka administrator jaringan akan mendapatkan notifikasi berupa laporan mengenai jenis serangan, port tujuan, IP address penyerang, IP address server serta waktu terjadinya serangan.

3.3.1 Metode demonstrasi

Suatu metode yang digunakan untuk mendemonstrasikan sebuah proses atau langkah langkah dalam penelitian yaitu menyiapkan alat yang akan digunakan dalam uji coba, menyiapkan objek penelitian, melakukan demonstrasi, mengamati serta menganalisis hasil yang didapat. Metode demonstrasi untuk mengetahui sejauh mana sebuah aplikasi dapat membantu seorang administrator ketika mengkonfigurasi suatu jaringan, sehingga dapat mengefisienkan waktu dalam melakukan suatu pekerjaan.

3.3.2 Desain pengiriman alur informasi serangan

Tahapan alur pengiriman informasi jika terjadi serangan terhadap sistem keamanan jaringan mikrotik, alur pengiriman informasi serangan pada perancangan *Intrusion Detection System* (IDS) dengan menggunakan snort yang nantinya akan mengirimkan notifikasi peringatan jika terdapat indikasi serangan dengan mengirimkan notifikasi pada aplikasi telegram, untuk dapat menghubungkan antara sistem dengan snort maka dibutuhkan sebuah *trigger* yakni dengan memanfaatkan sebuah API (*Application Programming Interface*). Aplikasi tersebut dibuat dengan menggunakan bahasa program PHP dengan tujuan supaya telegram dapat

terhubung dan memeriksa informasi mengenai data data penyerang, untuk desain pengiriman informasi dapat kita lihat dari gambar berikut .





Gambar 3.4 Desain Pengiriman Alur Informasi Serangan
Sumber : (Data Penelitian, 2023)

Apps interface dirancang untuk dapat mendapatkan informasi mengenai pihak yang mencoba untuk mengakses sistem keamanan jaringan mikrotik, dengan ketentuan sistem akan memblokir IP pengguna apabila telah salah dapat melakukan login terhadap sistem sebanyak 3 kali. Informasi yang akan dikirimkan ke telegram berdasarkan jenis serangan, port tujuan, IP address penyerang, IP address server serta waktu terjadinya serangan.


3.3.3 Perangkat hardware yang digunakan

Adapun perangkat hardware yang digunakan oleh PT. Shanaya Creativo Innovation dalam konfigurasi jaringan sebagai berikut:

Tabel 3. 1 Perangkat *Hardware* yang digunakan

No	Perangkat keras (<i>Hardware</i>)	Model	Keterangan	Gambar
1	Server	OLT Fujitomo E04L3 10G, 4 PON	Sebagai pusat untuk mengkonfigurasi jaringan serta memantau lalu lintas jaringan	
2	Router (mikrotik)	router mikrotik RB941-2nD-TC HAP Lite	Sebuah perangkat keras komputer yang berfungsi sebagai penghubung terhadap dua bahkan lebih terhadap jaringan yang berbeda	

Tabel 3.1 Perangkat *Hardware* yang digunakan (Lanjutan)

3	Smartphone	Infinix Hot 11s	Smartphone berguna untuk membantu dalam memonitoring jaringan komputer	
4	Telephone Analog	KX- TS505MX	Digunakan sebagai telephone analog di meja karyawan	

Sumber : (Data Penelitian, 2023)

3.3.4 Perangkat Software

Adapun beberapa perangkat lunak (*software*) yang digunakan dalam membangun jaringan ini antara lain sebagai berikut :

1. Mikrotik

Sebuah sistem operasi yang berbasis perangkat lunak yang digunakan untuk mengubah komputer menjadi router jaringan, dari segi biaya router juga lebih hemat. Ada beberapa fitur yang diberikan oleh mikrotik seperti:

1. Mikrotik telah menerapkan sistem *autentifikasi* dan konfigurasi jaringan lokal
2. pengelolaan yang terpusat
3. tidak hanya untuk jaringan kabel saja tapi juga dapat digunakan untuk jaringan *wireless*
4. bisa berperan sebagai hotspot

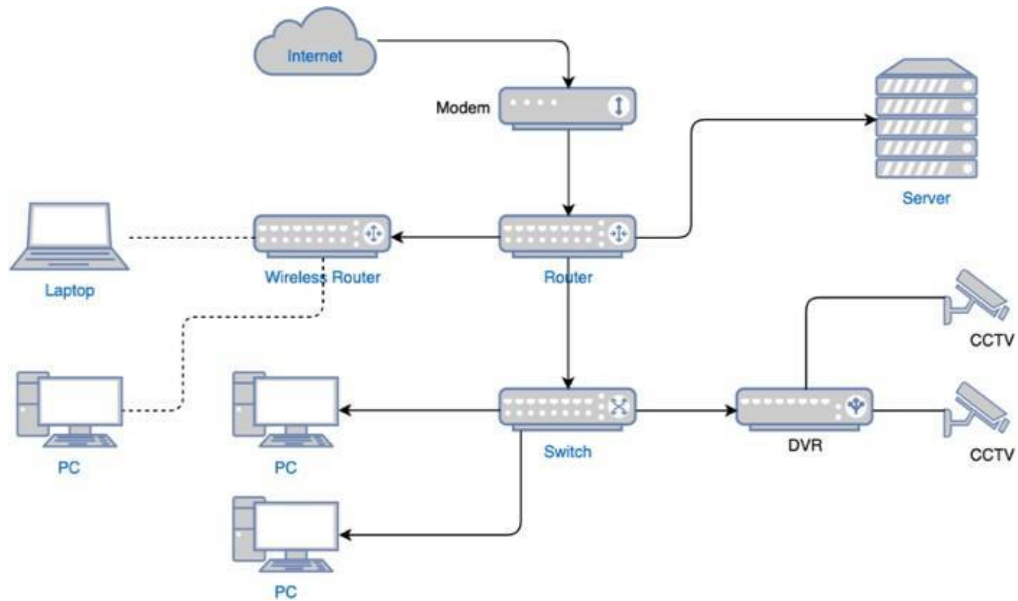
2. Library API

Digunakan untuk menciptakan sebuah aplikasi berbasis *mobile* yang digunakan management sebuah router mikrotik, yang nantinya dalam membantau jaringan bisa melalui komputer dan secara *mobile*.

3.3.5 Spesifikasi Hardware dan Software

Simulasi sistem keamanan jaringan mikrotik untuk event virtual akan menggunakan beberapa perangkat keras (*hardware*) dan perangkat lunak (*software*), yang mana disini sistem akan dioperasikan dengan 4 user pada virtual mesin sebagai router. Disini menggunakan mikrotik dengan versi 7.1.1, *attacker 1* (*FileZilla*), *attacker 2* (*Putty*), *attacker 3* (*Zenmap*) *log server* dan telegram *gateway*, administratornya (windows 10) dan winbox versi 3.34

3.4 Topologi jaringan



Gambar 3.5 Topologi Jaringan
Sumber : (Data Penelitian, 2023)

Peneliti menggunakan topologi star dalam melakukan konfigurasi jaringan dan melakukan konektivitas antara *smartphone* dengan mikrotik. Topologi star merupakan sebuah topologi jaringan komputer yang terdiri dari konvergensi melalui titik (*node*) tengah ke setiap titik (*node*) yang terhubung. Topologi star memanfaatkan fitur dari mikrotik yang sudah *built-in wifi*, sehingga *smartphone* dapat dengan langsung terkoneksi ke mikrotik, sedangkan komputer/laptop nantinya akan menggunakan kabel UTP untuk mengkoneksikannya yang dapat *memonitoring traffic* pada mikrotik.

3.5 Tahapan rencana implementasi

Beberapa tahapan perencanaan dalam mengimplementasikan sistem keamanan yang akan dirancang. Adapun tahapan implementasinya sebagai berikut:

1. Menyiapkan perangkat mikrotik yang akan digunakan sebagai *firewall* serta hak akses *administrator* ke perangkat tersebut.
2. Mengkonfigurasi mikrotik
 - a. Melakukan konfigurasi basic pada mikrotik yaitu membuat *dhcp client* dan *dhcp service* serta melakukan proses NAT (*Network Addressing Translation*) agar *client* mendapatkan akses internet.
 - b. Membuat kebijakan keamanan yang akan diterapkan di *firewall* mikrotik
 - c. Membuat aturan untuk pemblokiran bagi pihak yang tidak dapat mengakses dengan valid
 - d. Membuat aturan *firewall* dinamis sehingga dapat membuka akses *port knocking* setelah berhasil
3. Mengkonfigurasi *port knocking*

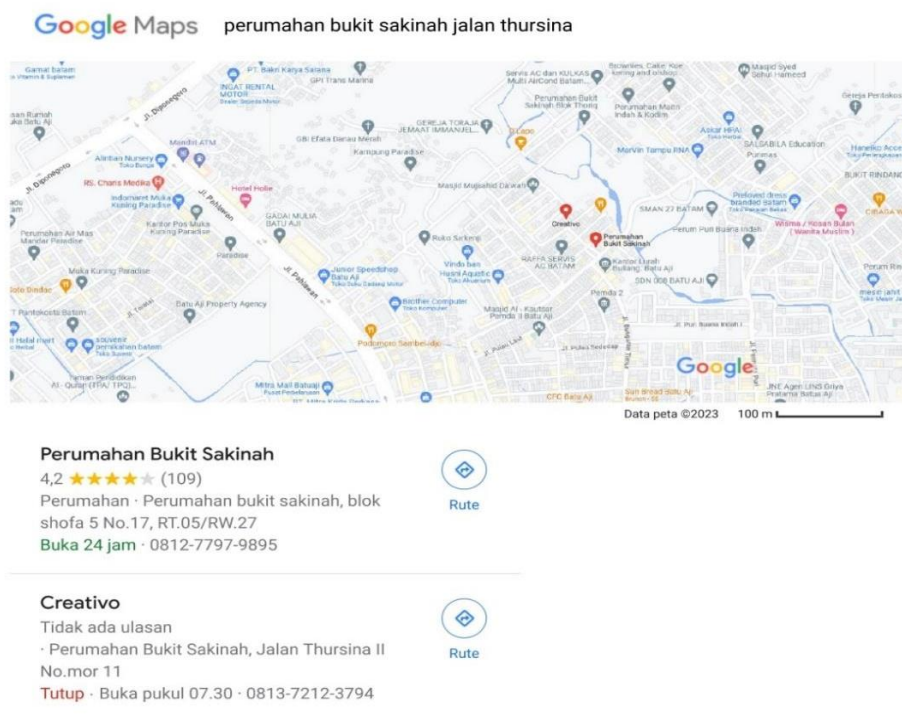
Mengatur lama waktu yang diizinkan dalam mengakses *port knocking* setelah berhasil
4. Integrasi notifikasi telegram

Mengkonfigurasi mikrotik untuk dapat mengirimkan notifikasi melalui telegram menggunakan API bot

3.4 Lokasi dan Jadwal Penelitian

3.4.1 Lokasi penelitian

PT. Shanaya Creativo Innovation merupakan sebuah perusahaan perorangan yang bergerak dibidang *IT Consultant* yang beralamatkan di perumahan bukit Sakinah jalan thursina 2 no 11, kec Sagulung, Kota Batam, Prov. Kepulauan Riau.



Gambar 3.6 Lokasi Penelitian
Sumber : (Data Penelitian, 2023)

3.4.2 Jadwal penelitian

Penelitian ini dilaksanakan di PT Shanaya Creativo Innovation yang beralamat di perumahan Bukit Sakinah jalan thursina 2 no 11, kec Sagulung, Batu Aji. Lokasi ini dipilih karena akan mempermudah peneliti dalam melakukan

penelitian dan perancangan alat. Waktu yang dihabiskan dalam melakukan penelitian ini selama lebih kurang 6 bulan, berawal dari bulan Maret 2023 sampai dengan Agustus 2023. Adapun kegiatan yang dilakukan selama penelitian dapat dilihat dalam tabel 3.2.

Tabel 3. 2 Jadwal Penelitian

Kegiatan	Waktu pelaksanaan																							
	Maret 2023				April 2023				Mei 2023				Juni 2023				Juli 2023				Agustus 2023			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Judul	■	■																						
Bab I			■	■																				
Bab II					■	■	■	■																
Bab III									■	■	■	■												
Bab IV													■	■	■	■								
Bab V																	■	■	■	■				
Pengumpulan Skripsi																					■	■	■	■

Sumber : (Data Penelitian, 2023)