

**ANALISIS IMPLEMENTASI KEAMANA JARINGAN MENGGUNAKAN
METODE PORT BLOCKING DI UNIVERSITAS MUHAMMADIYAH
SUMATERA UTARA**

(STUDI KASUS: IT UMSU)

SKRIPSI

DISUSUN OLEH

**RAMADHAN
NPM.1909010003**



UMSU

Unggul | Cerdas | Terpercaya

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**

MEDAN

2023

**ANALISIS IMPLEMENTASI KEAMANA JARINGAN MENGGUNAKAN
METODE PORT BLOCKING DI UNIVERSITAS MUHAMMADIYAH
SUMATERA UTARA
(STUDI KASUS: IT UMSU)**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
(S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer
dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara**

**RAMADHAN
NPM.1909010003**

**PROGRAM STUDI SISTEM INFOMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**

MEDAN

2023

LEMBAR PENGESAHAN

Judul Skripsi : Analisis Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking Di Universitas Muhammadiyah Sumatera Utara (Studi Kasus: IT Umsu)

Nama Mahasiswa : RAMADHAN

NPM : 1909010003

Program Studi : SISTEM INFORMASI

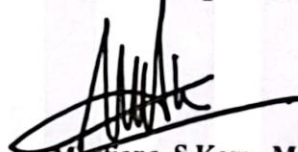
Menyetujui

Komisi Pembimbing


(Halim Mathana, S.T, M.Kom)


NIDN. 0121119102

Ketua Program Studi


(Marfiano, S.Kom., M.Kom)
NIDN. 0128029302



Dekan


(Dn Al-Khowarizmi, S.Kom., M.Kom.)
NIDN. 0127099201

Unggul | Cerdas | Terpercaya

PERNYATAAN ORISINALITAS

ANALISIS IMPLEMENTASI KEAMANA JARINGAN MENGGUNAKAN METODE PORT BLOCKING DI UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, Agustus 2023

Yang membuat pernyataan



RAMADHAN
NPM.1909010003

**PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS**

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama : RAMADHAN
NPM : 1909010003
Program Studi : Sistem Informasi (SI)
Karya Ilmiah : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif (*Non-Exclusive Royalty free Right*) atas penelitian skripsi saya yang berjudul:

**ANALISIS IMPLEMENTASI KEAMANA JARINGAN MENGGUNAKAN
METODE PORT BLOCKING DI UNIVERSITAS MUHAMMADIYAH
SUMATERA UTARA**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, Agustus 2023

Yang membuat pernyataan



RAMADHAN
NPM.1909010003

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap : RAMADHAN
Tempat dan Tanggal Lahir : TJ.SELAMAT, 19-11-2001
Alamat Rumah : DUSUN VIII DESA TJ.SELAMAT
Telepon/Faks/HP : 085762287724
E-mail : ramadanss3535@gmail.com
Instansi Tempat Kerja : -
Alamat Kantor : -

DATA PENDIDIKAN

SD : SD NEGERI 101783 SAENTIS TAMAT: 2013
SMP : SMP NEGERI 3 PERCUT SEI TUAN TAMAT: 2016
SMA : SMK NEGERI 1 PERCUT SEI TUAN TAMAT: 2019

KATA PENGANTAR



Assalammu'alaikum Wr.Wb

Dengan mengucapkan puji dan syukur penulis ucapkan kehadiran Allah SWT atas rahmad, hidayah dan karunia-Nya sehingga penulis dapat menyelesaikan Tesis ini, serta shalawat dan salam kehadiran junjungan Nabi Muhammad SAW yang syafaatnya kita harapkan di hari akhir kelak. Tesis ini disusun sebagai salah satu syarat untuk menyelesaikan pendidikan S-1 (Strata Satu) Program Sarjana Sistem Infoemasi Universitas Muhammadiyah Sumatera Utara Medan. Dengan Judul **“ANALISIS IMPLEMENTASI KEAMANA JARINGAN MENGGUNAKAN METODE PORT BLOCKING DI UNIVERSITAS MUHAMMADIYAH (STUDI KASUS: IT UMSU)”**

Penulis menyadari bahwa Skripsi ini masih jauh dari kesempurnaan karena masih banyak terdapat kesalahan dan kekurangan yang disebabkan keterbatasan kemampuan, untuk itu penulis mengharapkan kritik dan saran yang bersifat membangun serta petunjuk dari bapak/ibu dosen pembimbing dan rekan-rekan mahasiswa/i. Maka pada kesempatan ini dengan ketulusan hati penulis ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof Dr. Agussani, M.AP, Rektor Universitas Muhammadiyah Sumatera Utara.
2. Bapak Al-Khowarizmi, S.Kom., M.Kom., MTA, Dekan Fakultas Ilmu Komputer & Teknologi Informasi
3. Bapak Halim Maulana, S.T., M.Kom., MTA, SH., M.Hum, Wakil Dekan Fakultas Ilmu Komputer & Teknologi Informasi Universitas Muhammadiyah Sumatera Utara.

4. Bapak Halim Maulana, S.T., M.Kom., Dosen Pembimbing yang telah banyak mendukung penulis dalam memberikan ide, saran dan kritiknya.
5. Teristimewa Kepada Ayahanda Syaiful Bahri dan Ibunda Supriyati, serta keluarga besar yang telah menyayangi, memberi semangat baik moril maupun materil serta motivasi kepada penulis.
6. Seluruh Bapak/Ibu Dosen dan Staf pengajar Sistem Infomasi Universitas Muhammadiyah Sumatera Utara yang telah membekali penulis ilmu pengetahuan.
7. Seluruh pegawai di Universitas Muhammadiyah Sumatera Utara yang telah membantu penulis untuk mendapatkan data dan keterangan yang diperlukan dalam penyusunan Skripsi.
8. Teman Seperjuangan Ahmad Fajar Alfaravi, M. Arizky, Farhan Febrian, Aulil Mutaqim, serta teman-teman stambuk 2019 kelas A Siang Sistem Informasi Universitas Muhammadiyah Sumatera Utara.

Saya selaku penulis mengucapkan terima kasih kepada semua pihak, semoga Allah SWT melimpahkan Rahmat-Nya kepada kita semua, semoga kiranya Tesis ini dapat bermanfaat khususnya bagi penulis sendiri dan bagi siapa saja yang membacanya.

Wassalamualaikum Wr. Wb.

Medan, 24 Februari 2023

Penulis,

RAMADHAN
NPM.1909010003

**ANALISIS IMPLEMENTASI KEAMANA JARINGAN MENGGUNAKAN
METODE PORT BLOCKING DI UNIVERSITAS MUHAMMADIYAH
SUMATERA UTARA
(STUDI KASUS: IT UMSU)**

ABSTRAK

Aspek penting dari keamanan jaringan adalah menjaga integritas data dan memastikan ketersediaan layanan untuk digunakan secara aman oleh pengguna. Segala macam serangan dan upaya untuk menyalahgunakan sumber daya jaringan oleh pihak yang tidak berwenang harus diatasi untuk melindungi sistem keamanan jaringan. Jaringan komputer pada dasarnya memiliki kelemahan dalam keamanan, menghubungkan suatu komputer dengan komputer lainnya dapat memungkinkan seseorang atau pihak lain melalui jaringan tersebut dan dapat mengakses data bahkan dapat mengubah isi data tersebut. Router OS Mikrotik merupakan salah satu sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer menjadi router network, memiliki berbagai fitur yang dapat melakukan manajemen bandwidth serta mengamankan jaringan. Sistem firewall digunakan untuk mengatasi masalah ini, tetapi kesalahan tersebut disebabkan oleh serangan terhadap perangkat lunak tingkat aplikasi yang tidak dapat dilindungi oleh sistem firewall. Dalam penelitian ini, penerapan metode port blocking dalam keamanan jaringan telah diterapkan untuk mengatasi masalah privasi data. Metode pemblokiran port pada router proxy akan secara permanen memblokir port www dan port winbox menggunakan layanan yang disediakan oleh router proxy.

Kata Kunci : Keamanan Jaringan; Port Blocking; Mikrotik; Winbox

**ANALYSIS AND IMPLEMENTATION OF NETWORK SECURITY
APPLIED PORT BLOCKING METHOD IN MUHAMMADIYAH
UNIVERSITY, SUMATRA UTARA**

(CASE STUDY: IT UMSU)

ABSTRACT

An important aspect of network security is maintaining data integrity and ensuring the availability of services for safe use by users. All kinds of attacks and attempts to misuse network resources by unauthorized parties must be dealt with to protect the network security system. Computer networks basically have weaknesses in security, connecting a computer with another computer can allow someone or other parties to go through the network and be able to access data and even change the contents of the data. Router OS Mikrotik is an operating system and software that can be used to turn a computer into a network router, has various features that can perform bandwidth management and secure the network. A firewall system was used to solve this problem, but the error was caused by an attack on application-level software that the firewall system could not protect. In this study, the application of the port blocking method in network security has been successfully achieved to overcome data privacy problems. The port blocking method on the proxy router will permanently block the www port and winbox port using the services provided by the proxy router.

Keywords: Mikrotik; Network Security; Port Blocking; Winbox

DAFTAR ISI

	Halaman
LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS.....	iii
KATA PENGANTAR.....	vii
ABSTRAK.....	ix
ABSTRACT	x
DAFTAR ISI	xi
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang.....	1
1.2. Identifikasi Masalah	5
1.3. Batasan Masalah	5
1.4. Rumus Masalah	6
1.5. Tujuan Penelitian.....	6
1.6. Manfaat Penelitian.....	6
BAB II KAJIAN PUSTAKA	7
2.1. Landasan Teori	7
2.1.1. Implementasi.....	7
2.1.2. Sistem.....	8
2.1.3. Informasi	8
2.1.4. Sistem Informasi.....	9
2.1.5. Jaringan Komputer	9
2.1.6. Klasifikasi Jaringan Komputer	9
2.1.7. Topologi.....	14
2.1.8. Keamanan Jaringan	18
2.1.9. Bentuk Ancaman Jaringan Komputer	18
2.1.10. Metode Penyerangan Jaringan Komputer	19
2.1.11. Mikrotik.....	20
2.1.12. TCP/IP (Transmission Control Protokol/Internet Protocol)	21
2.1.13. Firewall	22

2.1.14. Network Address Translation (NAT)	23
2.1.15. Internet Service Provider (ISP).....	24
2.1.16. Router	24
2.1.17. Port Bloking	25
2.1.18. Winbox	28
2.1.19. Command Prompt (CMD)	28
2.2. Kerangka Berpikir Konseptual	29
2.3. Hipotesis.....	30
BAB III METODE PENELITIAN	31
3.1. Jenis Penelitian.....	31
3.2. Defenisi Operasional	31
3.3. Tempat dan Waktu Penelitian	32
3.4. Teknik Pengumpulan Sampel	32
3.5. Teknik Pengumpulan Data.....	32
3.6. Teknik Analisis Data.....	33
3.7. Model Implementasi	38
BAB IV HASIL DAN PEMBAHASAN.....	40
4.1 Deskripsi Data	40
4.2 Analisis Data	41
4.2.1 Konfigurasi Mikrotik.....	41
4.2.2 Pengujian Port Blocking.....	43
BAB V PENUTUP	47
5.1 Kesimpulan.....	47
5.2 Saran	48
DAFTAR PUSTAKA.....	49

DAFTAR TABEL

	Halaman
Tabel 3.1 Software dan Hardware	36
Tabel 4. 1 Kebutuhan Data Port Blocking	40
Tabel 4. 2 Hasil Pengujian Port Blocking	45

DAFTAR GAMBAR

	Halaman
Gambar 2.1. LAN	10
Gambar 2.2. MAN	11
Gambar 2.3. WAN	11
Gambar 2.4. WLAN.....	12
Gambar 2.5. Intranet	13
Gambar 2.6. Internet	14
Gambar 2.7. Topologi Bus	15
Gambar 2.8. Topologi Ring	15
Gambar 2.9. Topologi Star.....	16
Gambar 2.10. Topologi Linear	16
Gambar 2.11. Topologi Tree	17
Gambar 2.12. Topologi Mash	18
Gambar 2.13 Konseptual.....	30
Gambar 3.1 Flowmap Alur Penelitian	35
Gambar 3.2 Diagram block port blocking	36
Gambar 3.3 Port Blocking.....	37
Gambar 3.4 Topologi port blocking	37
Gambar 4. 1 Konfigurasi Blocking Port	41
Gambar 4. 2 Pemilihan Port	41
Gambar 4. 3 Konfigurasi Interface	42
Gambar 4. 4 Konfigurasi Ip Address	42
Gambar 4. 5 Konfigurasi DNS	43
Gambar 4. 6 Konfigurasi Route	43
Gambar 4. 7 Koneksi Winbox Sebelum diblock	44
Gambar 4. 8 Koneksi WWW Sebelum diblock	44
Gambar 4. 9 Koneksi Winbox Setelah di block	45
Gambar 4. 10 Koneksi WWW Setelah di block	45

BAB I

PENDAHULUAN

1.1.Latar Belakang

Keamanan jaringan (Sumardi, 2013) ialah komponen signifikan pada jaringan komputer. Kini jaringan komputer sangat penting dan banyak digunakan dalam pendidikan maupun dalam dunia pekerjaan. Dalam jaringan komputer itu sendiri ada hal yang sangat penting yaitu keamanan jaringan. Hal tersebut sangat vital dikarenakan kelemahan – kelemahan yang ada didalam jaringan komputer dapat dicuri jika keamanan jaringan tersebut lemah. Banyak organisasi maupun kelompok mengabaikan pentingnya keamanan dalam jaringan dan lebih mengutamakan tampilan. Tanpa disadari sistem dalam jaringan komputer mengalami masalah, sehingga keamanan jaringan memang penting untuk melindungi suatu jaringan dari malware maupun virus.

Dengan semakin banyaknya komputer (pengguna) yang terkoneksi ke dalam jaringan lokal atau publik di Universitas Muhammadiyah Sumatera Utara, kemungkinan munculnya ancaman dan serangan terhadap sistem keamanan jaringan tentu menjadi suatu hal yang tak terelakkan. Keamanan jaringan merujuk pada sistem yang digunakan untuk mencegah potensi ancaman dari luar yang dapat mengakibatkan kerusakan pada jaringan, sekaligus menghadapi ancaman internal seperti pencurian data perusahaan, penetrasi sistem akibat akses password oleh individu yang tidak berhak, serta berbagai jenis serangan dan upaya peretasan atau pemindaian. Hal ini dilakukan dengan memberikan perlindungan dan lapisan keamanan pada router *Mikrotik*. Perlindungan dan keselamatan di dalam pengaturan router *Mikrotik* memegang peranan yang sangat penting dalam menjaga

kestabilan jaringan komputer universitas. Secara khusus, guna melindungi keamanan *router Mikrotik* universitas dari usaha akses ilegal yang berupaya memasuki dan mengelola jaringan di dalamnya.

Berdasarkan penelitian yang menjelaskan tentang sistem keamanan jaringan yang dirancang menggunakan *firewall security port*. Dimana seringkali terjadi pencurian data yang memanfaatkan perangkat lain untuk bisa mengambil alih hak akses jaringan sehingga membutuhkan suatu sistem keamanan jaringan seperti penerapan *firewall security port*.

Penelitian yang menjelaskan tentang sistem yang menggunakan implementasi *traffic filtering* yang mengijinkan akses atau menutup akses *traffic* data yang masuk. Kasus sering terjadi di mana data diambil secara tidak sah dan jaringan mengalami kerusakan sehingga dibuat suatu sistem yang dapat melindungi data yang penting maka digunakanlah *firewall* dan *traffic filtering*. Dengan menerapkan dan merancang *firewall* serta penyaringan lalu lintas di dalam suatu infrastruktur jaringan perusahaan, kita bisa meningkatkan potensi keamanan, memanfaatkan fungsi yang disediakan pada perangkat *Cisco Router*.

Port adalah suatu tempat yang menjadi lalu lintas informasi untuk keluar masuk dari suatu komputer. Port blocking digunakan untuk mencegah lalu lintas informasi yang mengalir melalui port-port yang sudah ditetapkan rawan terhadap serangan virus. Perlindungan dan pengaturan akses ke port merupakan aspek yang vital pada layanan jaringan, yang tergabung dalam penyediaan layanan itu. Masalah ketahanan jaringan kerap muncul karena keberadaan *port* terlihat ataupun tindakan koneksi yang tidak sah. Kegagalan dalam langkah-langkah

autentikasi dan izin dapat mengakibatkan individu yang tidak sah untuk dengan mudah memasuki sistem dengan cara yang melanggar hukum.

Staf pengajar, tenaga kerja, dan mahasiswa menggunakan koneksi internet sebagai alat untuk mengakses informasi dan berkomunikasi. Meskipun internet memberikan sejumlah manfaat yang signifikan, kita juga perlu menyadari adanya konsekuensi negatifnya, seperti potensi infeksi oleh perangkat lunak berbahaya dan potensi serangan eksternal yang berisiko merusak sistem komputer serta mengganggu kinerja jaringan. Di pintu masuk yang tidak aktif dalam struktur jaringan, mereka bisa mendapatkan akses dengan mudah. Sistem komputer umumnya dilengkapi dengan *firewall* untuk menghambat gangguan semacam itu, walaupun dengan keterbatasan kemampuannya. Maka, diperlukan komponen ekstra yang bisa mendukung fungsi *firewall*. Sebuah alat yang membolehkan pelaksanaan kewajiban tersebut merupakan *router*. Pada pengenalan *router* tambahan, diinginkan tingkat perlindungan serta proteksi informasi komputasi di Universitas Muhammadiyah Sumatera Utara akan meningkat secara signifikan.

Masalah yang disebutkan di atas menjadi landasan untuk melindungi hak akses ke dalam sistem yang sedang dikembangkan, sehingga perlu diterapkan suatu pendekatan jaringan yang dapat memberikan tingkat keamanan yang memadai bagi pengguna sistem tersebut.

Analisis keamanan jaringan dalam penelitian ini menerapkan pendekatan port, yang bertujuan untuk menjaga, menyaring, membatasi, atau menolak koneksi jaringan antara segmen jaringan pribadi dan area luar yang tidak termasuk dalam cakupan mereka. Studi ini mengulas aspek keamanan jaringan melalui penerapan teknik *port knocking*, yang berfungsi sebagai mekanisme untuk membuka portal ke

port spesifik yang sebelumnya sudah dikecualikan dengan *firewall* dalam infrastruktur alat konektivitas. Metode ini diterapkan melalui pengiriman paket data ataupun sambungan yang bersifat istimewa. Tugas keamanan jaringan melibatkan penggunaan *port blocking* untuk memastikan autentikasi sebelum mengizinkan akses ke server, yang selanjutnya dipadukan melalui unsur *firewall IP sieve* serta pengaturan batas waktu transmisi dalam konfigurasi *router*.

Dalam penelitian ini, penyidik menerapkan pendekatan *blocking* sebagai langkah untuk menghalangi akses yang tidak sah dari pengguna yang tidak memiliki izin yang tepat. Mengimplementasikan regulasi dalam *firewall* sebagai penghalang terhadap pengguna yang tidak memiliki izin untuk mencapai jaringan tertentu. Tujuan inti merupakan menjaga sistem pada kemungkinan serangan yang bisa dieksploitasi melalui melaksanakan *skrining port* serta mengelola pembatasan izin pengguna. Karena itu, individu memiliki otorisasi sah yang diberikan izin absolut dalam mengelola pembukaan serta penutupan koneksi ke port yang sudah diatur.

Sebelumnya telah dilakukan beberapa penelitian oleh (Rizal et al., 2020); (Sumardi, 2013); (Irawan, 2015); (Brades & Irwansyah, 2022); dan (Lukman & Bachtia, 2016) yang dimana kelimanya berfokus pada tujuan dalam menyusun sistem keamanan komputer jaringan menggunakan strategi pemblokiran port dengan menggunakan metode penelitian observasi.

Dengan mempertimbangkan konteks yang sudah dipamparkan di atas, jadi bisa dihasilkan sebuah judul yang sesuai: **Analisis Implementasi Keamanan Jaringan menggunakan Metode Port Bloking Di Universitas Muhammadiyah Sumatera Utara**

1.2. Identifikasi Masalah

Dengan merujuk pada konteks yang telah diuraikan sebelumnya maka bisa diidentifikasi sejumlah permasalahan yaitu:

1. Apakah Sistem Keamanan Database server, Website dan Aplikasi yang masih sering dibobol atau dibajak?
2. Mengapa sistem keamanan jaringan komputer di Universitas Muhammadiyah Sumatera Utara yang masih kurang?
3. Bagaimana cara mengamankan sistem jaringan di Universitas Muhammadiyah Sumatera Utara?

1.3. Batasan Masalah

Untuk memastikan fokus pada penerapan keamanan jaringan menggunakan metode *port blocking*, berikut adalah batasan masalah yang telah ditentukan:

1. Penyidik hanya melaksanakan penggunaan *Port Blocking* pada *Mikrotik RouterBoard*
2. Penulis hanya menggunakan 1 laptop untuk mengimplementasikannya
3. Dalam uji coba pengtukan *port*, penyidik menggunakan *software PuTTY*, *Commend prompt*, serta *software Nmap*
4. Pengecekan port blocking hanya sekadar memakai *Ping*, *Telnet*, dan *Ssh*
5. Penyidik memanfaatkan *winbox*

1.4.Rumus Masalah

Dengan merujuk pada konteks yang sudah diuraikan sebelumnya, jadi bisa dirumuskan permasalahan yang dibahas pada studi ini,yakni:

1. Bagaimana pendekatan *port blocking* dapat menjaga keamanan akses ke *router mikrotik*?
2. Bagaimana proses meningkatkan efektivitas *firewall* dalam menjaga keamanan serta data komputer Universitas Muhammadiyah Sumatera Utara menjadi lebih baik?
3. Bagaimana cara menontaktifkan *port-port* yang terbuka pada *router mikrotik*?

1.5.Tujuan Penelitian

Dalam studi ini, terdapat sejumlah tujuan yang ingin dicapai, yakni:

1. Untuk meinplementasikan pendekatan *port bloking* dengan *router mikrotik*
2. Untuk mingkatkan keamanan pada *router mikrotik*
3. Untuk mengatasi risiko serangan terhadap *mikrotik*
4. Untuk menghalangi akses yang ilegal terhadap *router mikrotik*

1.6.Manfaat Penelitian

Dalam konteks ini, keuntungan dari studi ini bisa dijelaskan berikut ini:

1. Mampu meningkatkan tingkat keamanan dalam jaringan komputer.
2. Solusi bagi penggunaan *router MikroTik* yang melibatkan tindakan akses yang melanggar hukum.
3. Meningkatkan rasa keamanan bagi pengguna *router MikroTik*.

BAB II

KAJIAN PUSTAKA

2.1.Landasan Teori

2.1.1.Implementasi

Definisi implementasi dalam Kamus Besar Bahasa Indonesia mengacu pada realisasi serta pembelajaran. Dari segi asal-usul kata, berdasarkan Kamus Besar Webster, ungkapan implementasi berawal dari frasa Inggris yang disebut implementasi. Pada isi kamus besar *Webster*, istilah "*to implement*" diartikan sebagai "memberikan sarana untuk menjalankan (menyediakan cara untuk melakukan sesuatu)." (Rizal et al., 2020)

Menurut (Lukman & Bachtia, 2016) istilah "implementasi" merujuk pada tindakan, pelaksanaan, atau penerapan suatu sistem. Frasa penerapan ini mencerminkan bahwa pelaksanaan tidak sekadar tindakan, melainkan suatu tindakan yang direncanakan secara cermat dan dilakukan dengan sungguh-sungguh, dengan dasar pada riset atau norma tertentu, untuk mencapai tujuan tertentu. Berdasarkan (Sumardi, 2013) Penulis dalam buku bertajuk Dasar-Dasar Pengembangan Kurikulum mengemukakan bahwasanya implementasi mencakup pelaksanaan pemikiran, gagasan, strategi, atau penemuan melalui sikap konkret, yang pada akhirnya menghasilkan dampak signifikan, termasuk perubahan dalam kewawasan, keahlian, serta nilai juga sikap. Menurut penjelasan implementasi sebelumnya, maka bisa diambil kesimpulan bahwa penerapan adalah pelaksanaan pada unsur jaringan yang telah dirancang. Sistem tersebut diterapkan dengan tujuan mengatasi masalah tertentu, menyediakan layanan yang diperlukan, dan menghadirkan inovasi terkini pada pertumbuhan wawasan.

2.1.2. Sistem

Berdasarkan (Anggraeni, 2017) Sebuah sistem merupakan gabungan individu yang berkolaborasi sesuai dengan peraturan yang terorganisir dan terstruktur, dengan tujuan membentuk sebuah entitas yang menjalankan tugas tertentu demi mencapai tujuan tertentu. Sistem ini mencakup berbagai elemen yang melibatkan unsur-unsur seperti komponen sistem, batas sistem, konteks lingkungan eksternal, koneksi sistem, input sistem, output sistem, proses sistem, dan tujuan sistem.

2.1.3. Informasi

Informasi menurut (Sutabri, 2012) Merupakan langkah tambahan dalam memproses data yang telah diperkaya dengan nilai tambah. Data bisa digolongkan jadi tiga kategori, yakni:

- a. Informasi strategis, yang dipakai dalam pengambilan kebijakan tahan lama, melibatkan data luar, skema pertumbuhan bisnis, dan kebijakan yang terkait.
- b. Informasi taktis. memiliki tingkat kepraktisan yang tinggi ini diperlukan dalam meraih penepatan pada periode menengah, serupa data trend perdagangan yang bisa digunakan dalam perencanaan pemasaran.
- c. Informasi teknis. fakta ini sangat diperlukan dalam kepentingan kebutuhan keseharian, serupanya pemantauan stok, pengelolaan pengembalian penjualan, dan pelaporan keuangan harian.

Jadi, simpulannya, informasi merujuk pada data yang telah dianalisis, diproses, atau diinterpretasikan untuk mendukung proses pengambilan kebijakan.

2.1.4. Sistem Informasi

Sistem informasi merupakan suatu rangkaian yang memberikan data bagi manajemen dalam mengambil keputusan serta menggerakkan operasional perusahaan. Sistem tersebut merupakan gabungan dari individu, teknologi informasi, dan prosedur yang terstruktur (Anggraeni, 2019).

Sistem informasi merujuk pada gabungan yang terstruktur dari elemen-elemen seperti individu, perangkat keras, perangkat lunak, juga pangkalan data yang menghimpun, mengedit, serta menyampaikan data dalam konteks pada entitas organisasi.

2.1.5. Jaringan Komputer

Menurut (Syafrizal, 2020) jaringan komputer merupakan sekelompok "interkoneksi" yang berkaitan dua komputer otonom ataupun lebih melalui penggunaan alat transmisi, entah itu kabel atau tanpa kabel.

Dari penjelasan sebelumnya, bisa diringkas bahwasanya Jaringan Komputer merujuk pada komputasi yang beriringan terkoneksi melalui berbagai jenis saluran transmisi dengan tujuan untuk berbagi *data, facts, application software, and hardware*. Node merujuk pada komputasi, pencetak, ataupun alat lain yang terkoneksi dalam satu jaringan.

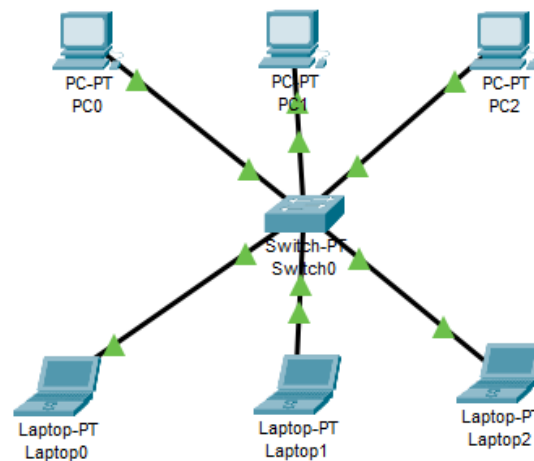
2.1.6. Klasifikasi Jaringan Komputer

Berdasarkan (Wahyono, 2017) jaringan komputer bisa digolongkan dalam berikut:

a. *Local Area Network* (LAN)

Jaringan komputer atau *Local area network* menurut (Suwarya, 2021) ialah secara umum kumpulan dari dari dua perangkat komputer atau

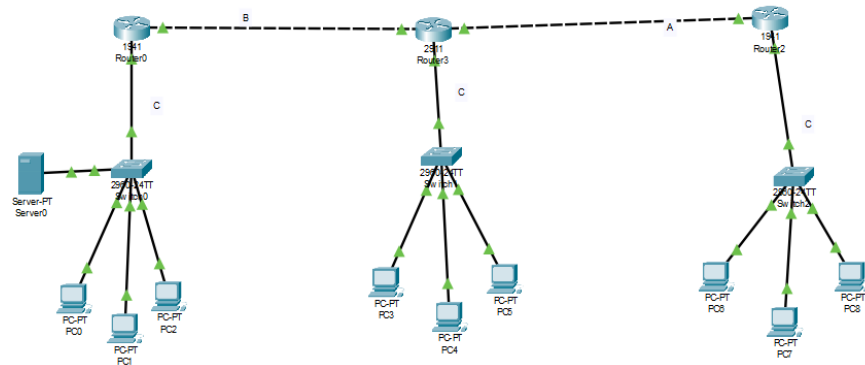
lebih yang terkoneksi satu sama lain baik secara fisik ataupun melalui data yang melibatkan area terbatas seperti jaringan kampus komputer, rumah, tempat kerja, atau hanya di ruangan. Jaringan lokal (LAN) awalnya dirancang untuk mengurangi biaya yang terkait dengan penggunaan perangkat bersama, namun seiring berjalannya waktu, perannya semakin berkembang. Banyak komputer yang terkoneksi satu sama lain dapat memanfaatkan satu saluran komunikasi bersama. Kerjasama dalam penggunaan saluran komunikasi adalah elemen sentral dalam meningkatkan efisiensi transformasi jaringan komputer menjadi entitas sebesar Internet.



Ilustrasi 2.1. LAN

b. *Metropolitan Area Network (MAN)*

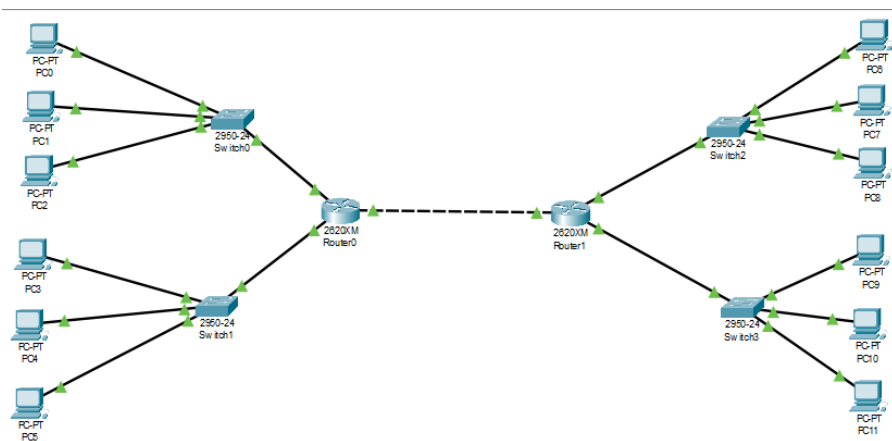
Merupakan sistem komputer tingkat sedang yang terdiri wilayah sebagaimana yang terdapat di dalam kota besar. Mengaitkan satu lokasi perkantoran dengan lokasi perkantoran lainnya atau satu pusat perbelanjaan dengan lainnya, dan sebagainya.



Ilustrasi 2.2. MAN

c. *Wide Area Network (WAN)*

Ini merupakan jaringan komputer yang melintasi batas negara atau benua yang luasnya mencakup wilayah yang luas. Seringkali dikenal sebagai Jaringan Area Global (*Global Area Network* atau GAN), ini adalah jaringan komputer yang mencakup seluruh planet.

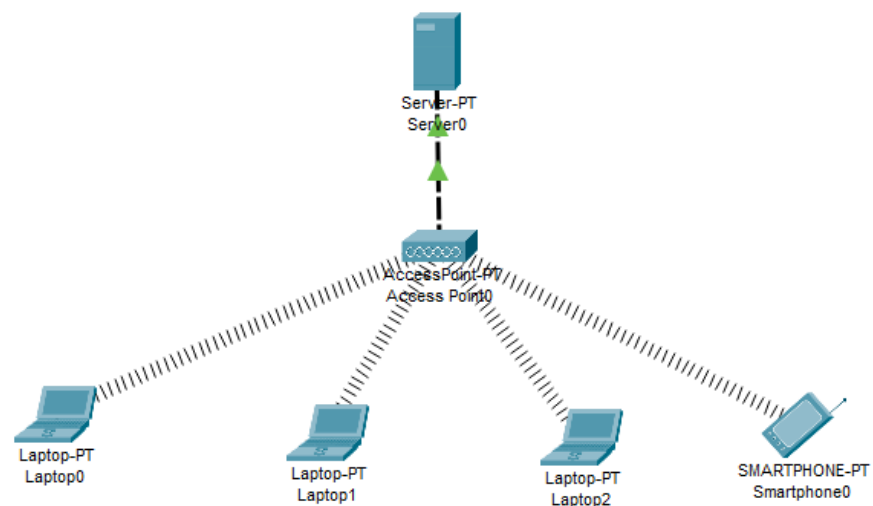


Ilustrasi 2.3. WAN

d. *Wireless Local Area Network (WLAN)*

WLAN merupakan alat interaksi informasi yang sangat adaptif, yang diimplementasikan sebagai peningkatan pada opsi pengganti dalam *Wireless LAN*. Melalui memanfaatkan ilmu jaringan nirkabel

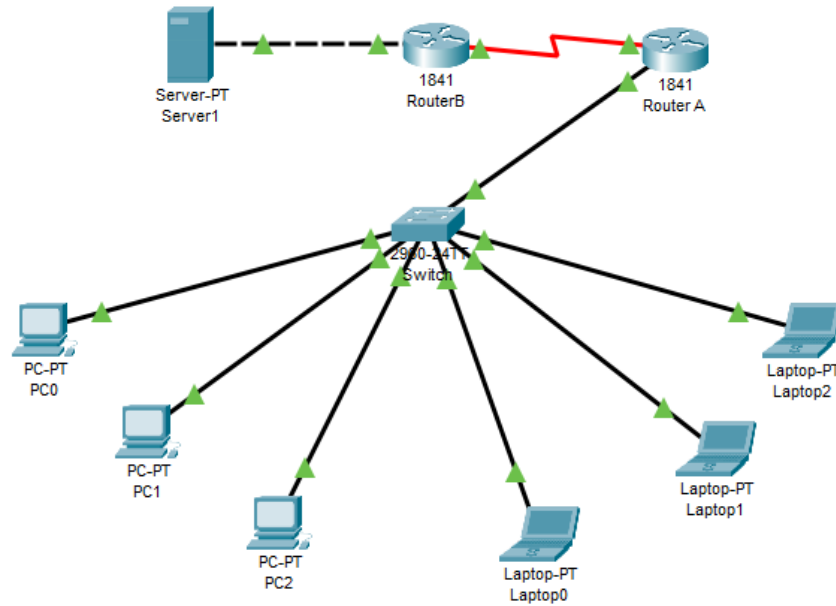
berbasis radio *frequency*, data dikirim serta diterima melalui medium udara. Sinyal radio yang dipancarkan oleh Wi-Fi adapter seperti *Access Point* (AP) bisa diakses dengan seluruh perangkat Wi-Fi yang berada di sekelilingnya, termasuk perangkat yang berada dalam cakupan ruangan atau gedung, yang dapat membuat informasi mudah diakses oleh pihak lain.



Ilustrasi 2.4. WLAN

e. Intranet

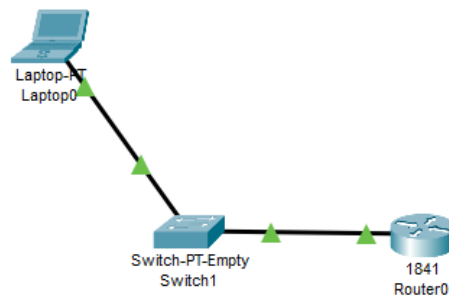
Intranet ialah sebuah sistem komputer jaringan yang terdiri dari LAN serta jaringan WAN, yang juga digunakan untuk akses lebih luas secara global. Intranet bisa dijelaskan sebagai sistem yang menyediakan layanan internet dalam ruang lingkup lokal bagi segolongan user komputer yang berkaitan melalui jaringan LAN atau WAN. Umumnya, Intranet hanya menghubungkan satu organisasi dalam batasan wilayah jaringan lokal (LAN/WAN) tersebut.



Ilustrasi 2.5. Intranet

f. Internet

Internet adalah hasil dari penggabungan berbagai jaringan lokal (LAN) serta WAN yang terdapat di seluruh bumi, menciptakan suatu infrastruktur jaringan yang memiliki jangkauan global yang lebih besar. Saat biasanya jaringan internet mengaplikasikan protokol TCP/IP untuk mengirimkan paket data. Internet berasal dari istilah "*Interconnected Network*," merujuk pada koneksi berbagai jaringan komputer global yang saling terhubung untuk menciptakan komunikasi global.



Ilustrasi 2.6. Internet

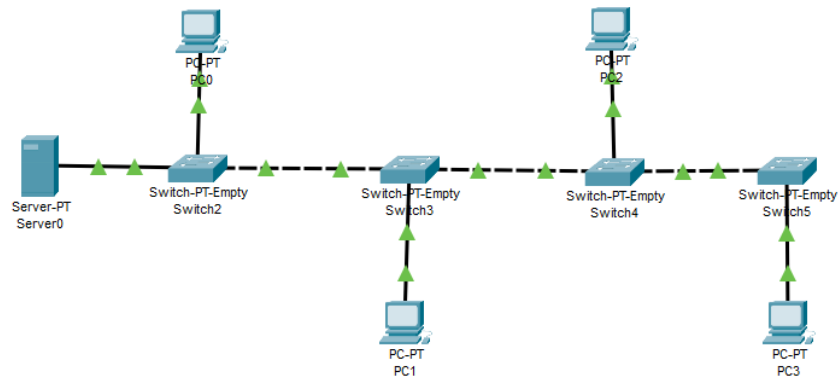
2.1.7. Topologi

Topologi jaringan ataupun struktur sistem adalah representasi perancangan relasi antara komputer pada *Local Area Network* yang biasanya memanfaatkan kabel dalam alat transmisinya, dilengkapi melalui konektor, kartu *Ethernet*, serta alat pendukung lainnya. (Syafrizal, 2020)

Terdapat berbagai tipe Topologi yang mengatur hubungan komputer dalam jaringan lokal, antara lain:

a. Topologi Bus

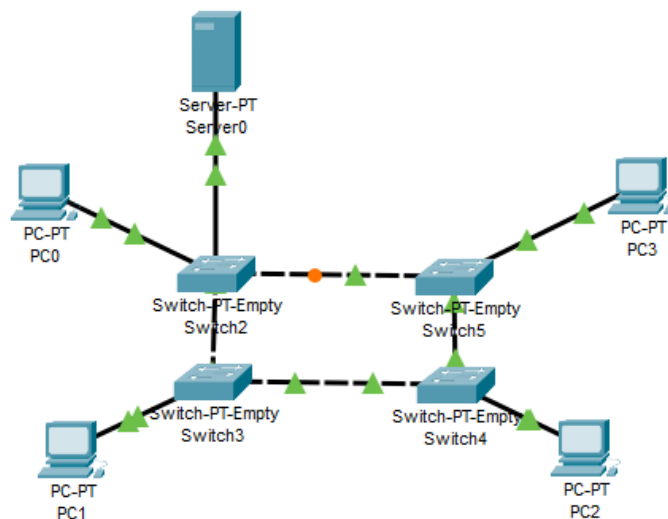
Topologi Bus merupakan struktur sistem yang terdiri dari satu kord panjang dengan dua ujungnya yang tertutup, dan terdapat node-node yang terhubung di sepanjang kabel tersebut. Sinyal dalam kabel pada topologi ini mengalir satu arah, yang membuatnya rentan terhadap potensi tabrakan.



Ilustrasi 2.7. Topologi Bus

b. Topologi Ring

Topologi cincin atau ring merupakan jenis pengaturan sistem yang membentuk lingkaran tertutup dengan node-node di dalamnya. Data mengalir dalam dua arah dalam topologi ini, yang membantu menghindari tabrakan (*collision*) dan memfasilitasi transfer data yang efisien.

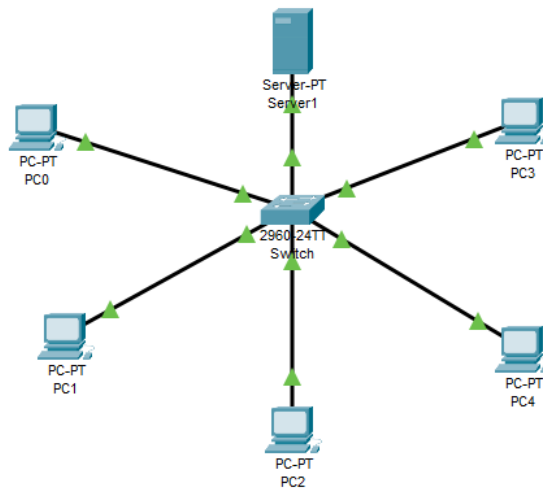


Ilustrasi 2.8. Topologi Ring

c. Topologi Star

Fitur utama dari struktur jaringan ini adalah saat node (stasiun) berinteraksi secara langsung dengan stasiun lainnya melalui node pusat

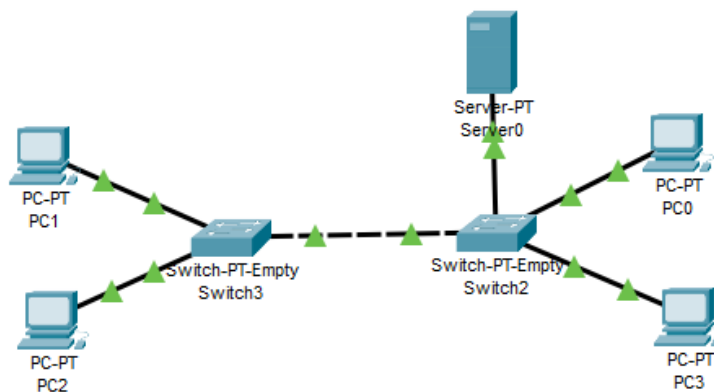
(hub/switch) sentral, lalu data lalu lintas mengalir dari node ke node pusat dan selanjutnya diteruskan ke stasiun tujuan. Apabila terjadi gangguan pada salah satu bagian kabel, maka jaringan lainnya akan tetap beroperasi tanpa terganggu.



Ilustrasi 2.9. Topologi Star

d. Topologi Daisy-Chain (Linear)

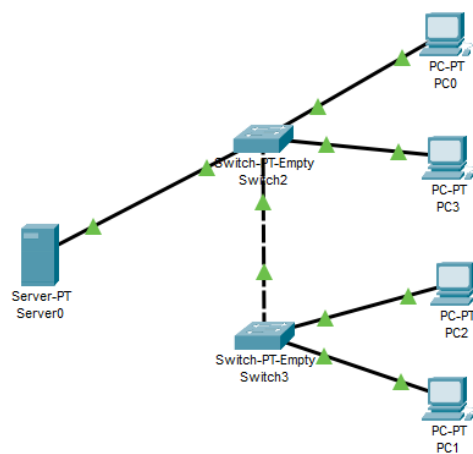
Topologi ini mewakili transisi dari struktur topologi bus dan topologi ring, di mana setiap simpul terhubung secara langsung dengan dua simpul lainnya melalui segmen kabel, namun segmen ini membentuk saluran, bukan sirkuit tertutup. Antar komputer seperti terhubung secara seri



Ilustrasi 2.10. Topologi Linear

e. Topologi *Tree*

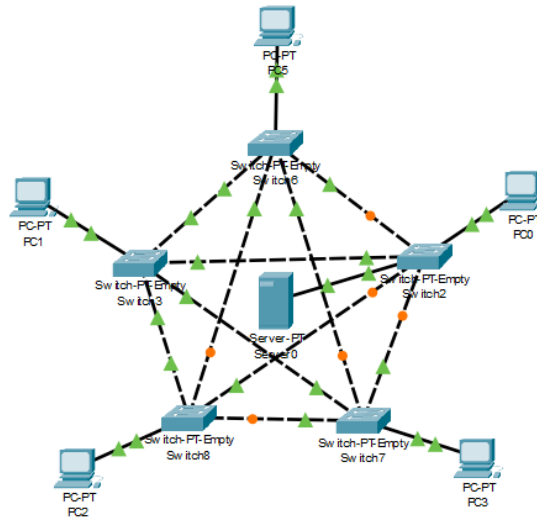
Tidak semua stasiun memiliki posisi yang setara. Stasiun dengan posisi yang lebih tinggi memiliki kendali atas stasiun yang berada di bawahnya, sehingga jaringan sangat bergantung pada stasiun dengan posisi lebih tinggi (topologi hierarki), sementara stasiun yang memiliki posisi yang sama dikenal sebagai tree topology.



Ilustrasi 2.11. Topologi Tree

f. Topologi *Mesh* dan *Full Connected*

Topologi jaringan ini adalah koneksi sepenuhnya antara semua pusat. Terdapat sebuah rumus yang bisa digunakan untuk menentukan jumlah saluran yang dibutuhkan untuk membentuk jaringan mesh. Rumus ini adalah dengan mengurangkan 1 dari jumlah pusat ($n-1$, di mana n adalah jumlah pusat yang ada). Kompleksitas jaringan meningkat seiring dengan peningkatan jumlah pusat yang terhubung.



Ilustrasi 2.12. Topologi Mash

2.1.8. Keamanan Jaringan

Keamanan jaringan merupakan konsep yang luas dan mencakup berbagai aspek, termasuk teknologi, perangkat, dan prosedur. Dalam ungkapan yang lebih simpel, sistem keamanan jaringan merujuk pada tahapan yang diambil untuk mengidentifikasi dan mencegah akses jaringan oleh individu yang tidak memiliki izin. Tujuan utama dari sistem keamanan jaringan ini adalah untuk mencegah potensi ancaman seperti pencurian data dan kerusakan fisik pada perangkat komputer. Beberapa ilustrasi insiden dalam bidang keamanan jaringan termasuk aktivitas seperti peretasan (*hacking*), pemindaian port (*port scanning*), serta serangan penolakan layanan terdistribusi (*distributed denial of service/DDoS*). (Huthaeen, 2015).

2.1.9. Bentuk Ancaman Jaringan Komputer

Dalam penjelasan yang diberikan oleh (Lukman & Bachtia, 2016) diungkapkan bahwa jaringan komputer menghadapi berbagai bentuk ancaman yang

ditujukan pada sumber daya fisik serta logis yang mendukung kelangsungan jaringan itu. sejumlah contoh bentuk ancaman tersebut termasuk:

- a. *Sniffer*, potensi risiko terhadap perangkat yang mampu mengawasi perkembangan suatu proses.
- b. *Spoofing*, menggunakan komputer untuk mengeksploitasi (dengan mengganti identitas atau alamat ip)
- c. *Preacking*, perilaku ancaman mengakibatkan penurunan tingkat keamanan pada sistem telepon.
- d. *Remote Attack*, segala jenis serangan mengenai sebuah perangkat yang dilakukan dengan penyerang dari jarak jauh di luar sistem jaringan atau media transmisi, di mana penyerang tidak mempunyai kendali atas perangkat tersebut.
- e. *Hole*, kondisi di mana perangkat lunak ataupun perangkat keras dapat dijangkau pada individu yang tidak memiliki izin ataupun terjadi peningkatan dalam tingkat akses tanpa melalui tahapan otorisasi.
- f. *Hacker*, seseorang yang secara rahasia mempelajari sistem yang seringkali rumit untuk kemudian mengelolanya dan berbagi hasil eksperimennya, seorang hacker tidak melakukan kerusakan pada sistem.
- g. *Cracker*, individu yang dengan rahasia memperdalam pemahamannya tentang sistem, biasanya bertindak dengan niat yang tidak baik, muncul sebagai hasil dari naluri manusia yang senantiasa didorong untuk menciptakan atau mengganggu.

2.1.10. Metode Penyerangan Jaringan Komputer

- a. *Eavesdropping*, menerima salinan pesan tanpa izin.

- b. *Masquerading*, mengirim atau menerima komunikasi dengan menggunakan identitas yang tidak sah tanpa persetujuan.
- c. *Message Tampering*, mengintersep atau menangkap pesan lalu mengubah kontennya sebelum disampaikan kepada penerima aslinya. “man in the middle attack” ialah teknik manipulasi pesan yang terjadi dengan mengintersep pesan awal pada tahap pertukaran kunci enkripsi saat membentuk kanal keamanan. Si penyerang memasukkan suatu kunci tambahan yang memungkinkannya untuk menguraikan pesan berikutnya sebelum pesan tersebut dienkripsi oleh penerima.
- d. *Replaying*, memelihara pesan yang telah terperangkap untuk penggunaan di masa mendatang.
- e. *Denial of Service*, mengalirkan pesan secara berlebihan ke dalam saluran atau sumber lain dengan tujuan menghambat akses pengguna lainnya.

2.1.11. Mikrotik

Mikrotik menurut (Nucahyo et al., 2021) ialah sebuah program perangkat yang dirancang khusus untuk digunakan pada *router*. Mikrotik dapat digunakan dalam dua varian, baik sebagai perangkat keras maupun sebagai perangkat lunak. Dalam konteks perangkat keras, biasanya Mikrotik sudah terpasang pada suatu papan tertentu, sementara dalam format perangkat lunak, perlu diinstal terlebih dahulu di komputer.

Pada tahun 1995, pendirian Mikrotik dimulai dengan fokus awalnya mengarah kepada penyedia layanan Internet (Internet Service Provider, ISP) yang menggunakan teknologi nirkabel dalam memberikan pelayanan kepada pelanggan mereka. Kini, MikroTik telah menghadirkan layanannya kepada sejumlah besar

penyedia layanan Internet nirkabel di berbagai negara di seluruh dunia, dan juga memiliki popularitas yang besar di Indonesia. Mikrotik dalam lingkup perangkat keras yang berasal dari *Personal Computer* (PC) dikenal karena tingkat keandalannya yang tinggi, kemampuan pengendalian yang berkualitas, dan fleksibilitasnya dalam mengelola beragam jenis data dan proses *routing*. Mikrotik, yang awalnya dirancang sebagai *router* berbasis komputer, memiliki banyak manfaat bagi penyedia layanan internet yang ingin mengoperasikan berbagai aplikasi, mulai dari yang paling sederhana hingga yang lebih canggih. Luar dari fungsi *routing*, Mikrotik juga memiliki kemampuan dalam mengelola kapasitas akses (seperti *bandwidth*, *firewall*, titik akses nirkabel (WiFi), tautan *backhaul*, sistem hotspot, server Jaringan Pribadi Virtual, dan berbagai fitur lainnya.) MikroTik bukanlah perangkat lunak yang dapat diakses secara bebas, untuk menggunakan semua fiturnya, perlu memperoleh lisensi resmi dari MikroTik dengan membayar biaya yang sesuai. Mikrotik dikenali sebagai 'Tingkat' dalam penamaan lisensinya.

2.1.12. TCP/IP (Transmission Control Protokol/Internet Protocol)

Protokol merupakan pedoman resmi yang menentukan langkah-langkah yang wajib dijalankan saat melakukan pengiriman dan penerimaan data. Protokol memastikan beragam elemen seperti jenis komunikasi, durasi, rangkaian langkah, dan pengawasan kesalahan yang digunakan dalam jaringan. *Protokol Kontrol Transmisi/Protokol Internet* (TCP/IP) adalah standar yang digunakan untuk memfasilitasi pertukaran data antara komputer dalam jaringan. Protokol ini ialah protokol yang dipergunakan untuk mengakses Internet dan digunakan dalam komunikasi yang bersifat global. Protokol TCP/IP terbagi menjadi dua protokol

yang berbeda. TCP/IP menerapkan pendekatan berlapis saat mengembangkan protokol ini. Dengan menerapkan pendekatan bertingkat ini, memungkinkan pembuatan sejumlah layanan kecil yang didesain khusus untuk tugas-tugas tertentu.

TCP/IP terbentang meliputi lima tingkatan, yaitu:

- a. Pada Layer Aplikasi, berbagai aplikasi seperti FTP, Telnet, SMTP, dan NFS beroperasi.
- b. Pada Layer Transport, TCP dan UDP memperkaya paket dengan informasi transportasi dan mengantarkannya ke Layer Internet.
- c. Layer Internet, ialah tahap yang mengambil paket data dari lapisan transport, kemudian melengkapinya dengan informasi alamat sebelum menyampaikannya ke lapisan antarmuka jaringan.
- d. Pada Layer Network Interface, data dikirimkan ke layer fisik melalui perangkat jaringan.
- e. Layer Physical, bagian dari infrastruktur kabel yang berperan dalam pengiriman dan penerimaan data.

TCP/IP dikirimkan ke setiap jaringan lokal dalam bentuk subnet yang telah dialokasikan alamat untuk masing-masingnya .IP yang menggunakan alamat disebut sebagai Alamat IP. Alamat IP ini dimanfaatkan untuk mengenali subnet dan host secara logis di dalam jaringan TCP/IP. (Wahyuddin S et al., 2023)

2.1.13. Firewall

Menurut (Farunudin, 2013) *Firewall* merupakan sebuah regulasi yang diterapkan pada *hardware*, *software*, atau sistem, dengan maksud melindungi dan mengamankan, entah melalui penyaringan, pembatasan, atau penolakan koneksi dari jaringan eksternal seperti internet. Karena *firewall* sering digunakan untuk

menjaga keamanan jaringan, perangkat tersebut juga berperan sebagai titik keluar yang menghubungkan jaringan yang diamankannya dengan jaringan lainnya, yang umumnya disebut sebagai *gateway*.

2.1.13.1. Tipe-Tipe Firewall

Firewall bisa kita bedakan menurut metode ataupun teknik *firewall* tersebut bekerja. berbagai jenis *firewall* yang tersedia:

1. *Packet Filtering Gateway*

Dapat dijelaskan sebagai sistem *firewall* yang bertugas menyaring paket-paket yang berasal dari luar jaringan dengan tujuan melindunginya."

2. *Application Level Gateway*

Firewall ini juga dikenal sebagai *firewall proxy*. Cara kerjanya tidak hanya didasarkan pada atribut paket seperti sumber dan tujuan, tetapi juga mampu menganalisis isi dari paket tersebut.

3. *Circuit Level Gateway*

Firewall ini akan memantau tahapan awal dari koneksi TCP yang sering disebut sebagai 'TCP *handshaking*' untuk mengevaluasi apakah sesi koneksi tersebut diizinkan atau tidak.

2.1.14. Network Address Translation (NAT)

Merupakan suatu teknik yang memungkinkan beberapa komputer terhubung ke internet melalui satu alamat IP. Banyak orang yang mengadopsi pendekatan ini karena alasan terbatasnya ketersediaan alamat IP, kebutuhan akan tingkat keamanan, serta kemudahan dan fleksibilitas dalam mengelola jaringan.

AT juga dapat diartikan sebagai perubahan alamat IP menjadi alamat yang berbeda, dan ketika paket data dialihkan menggunakan NAT pada suatu jalur, Maka

sebab itu, ketika paket data kembali dari tujuannya, link ini akan mengingat sumber asal paket tersebut, sehingga interaksi komunikasi dapat berjalan sebagaimana mestinya (Hadi, 2016).

2.1.15. Internet Service Provider (ISP)

Merupakan lembaga atau entitas bisnis yang menyelenggarakan layanan konektivitas internet serta berbagai layanan terkait lainnya. Dalam rangka memperoleh akses ke internet, ISP sebenarnya berfungsi serupa dengan pelanggan, yang berarti bahwa ISP tersebut memperoleh konektivitas internetnya dari ISP yang memiliki jaringan lebih besar (*upstream ISP*), yang bisa berbasis di tingkat nasional maupun internasional. Informasi ini diungkapkan dengan (Istiana, 2019).

2.1.16. Router

Menurut (Tahir, 2023) *Router* ialah perangkat pada jaringan komputer yang mengirimkan paket data ke tujuannya melalui jaringan atau internet dengan menggunakan proses yang disebut *routing*. Contohnya, dalam suatu jaringan warnet, *router* berperan sebagai pintu gerbang yang menghubungkan LAN di warnet dengan jaringan lainnya. Prinsip operasi *router* serupa dengan *bridge* dalam jaringan, di mana *router* dapat mengalirkan paket data jaringan dan memiliki kemampuan untuk mempartisi jaringan ke dalam segmen-segmen ataupun menggabungkan bagian-bagian jaringan. *Router* ialah suatu perangkat yang dimanfaatkan dalam jaringan komputer untuk mengirimkan informasi ke jaringan lain dengan kecepatan, ketepatan, dan efisiensi yang lebih tinggi. *Router* berperan dalam mengalihkan paket-paket data dari satu jaringan ke jaringan lainnya (termasuk LAN ke LAN atau LAN ke WAN), memungkinkan perangkat host dalam suatu jaringan untuk berinteraksi dengan perangkat host di jaringan lainnya.

Perangkat *router* menghubungkan jaringan-jaringan tersebut di tingkat jaringan pada model OSI, sehingga dari segi teknis, router adalah Gerbang Layer 3. Secara umum, *Router* dapat dibagi menjadi dua jenis, yakni Statis dan Dinamis.

2.1.17. Port Bloking

Fajar (2021) Port Blocking merupakan strategi keamanan yang diterapkan di perangkat MikroTik dengan menghentikan akses ke sejumlah port khusus. Tujuan dari tindakan ini adalah untuk mencegah adanya pertukaran data melalui port-port yang telah diidentifikasi, seperti untuk mencegah penyebaran virus atau jenis malware seperti *nimda* atau *conflicker*.

Selanjutnya, berdasarkan Rizal (2020), disebutkan bahwa *Port Blocking* adalah suatu metode keamanan yang diterapkan dalam infrastruktur jaringan MikroTik. Inti dari metode ini adalah untuk menghambat akses secara permanen ke *port-port www* dan *winbox* yang digunakan oleh server MikroTik. Dengan menerapkan strategi ini, user tidak dapat terhubung ke server MikroTik bahkan ketika mencoba mengirim paket ke alamat IP khusus MikroTik.

Dalam studi yang dilaksanakan dengan Irawan (2019), terdapat analisis perbandingan setelah menerapkan sistem keamanan jaringan menggunakan metode *Blocking Port*. Hasilnya adalah penurunan jumlah virus yang memasuki sistem melalui internet dan jaringan lokal, peningkatan stabilitas jaringan, dan peningkatan stabilitas koneksi internet. Irawan juga menarik kesimpulan bahwa pendekatan ini memiliki potensi untuk mengurangi risiko penetrasi malware dan serangan eksternal yang berpotensi menyebabkan gangguan pada jaringan lokal.

Sumardi dan Triyono (2018) juga menjelaskan dalam penelitian mereka bahwa tujuan dari metode *port blocking* ialah dalam menghentikan akses ke port-

port yang tidak digunakan sehingga jaringan komputer lokal mendapatkan tingkat perlindungan yang lebih baik. Dalam pelaksanaan tindakan pembatasan port yang diterapkan oleh Sumardi & Triyono, mereka merancang serta menerapkan perangkat keras berupa PC *Router*, dan menggunakan perangkat lunak Linux Mikrotik 2.9.27. Temuan studi ini menyimpulkan bahwa PC *Router* Mikrotik dapat efektif digunakan dalam menghentikan akses pada port yang tidak aktif dalam jaringan komputer.

Istilah pembatasan port (*port blocking*) merujuk kepada tindakan Penyedia Layanan Internet (ISP) dalam mengidentifikasi lalu lintas Internet berdasarkan kombinasi nomor *port* dan protokol transport, lalu menutup akses sepenuhnya. Membatasi akses ke *port* berdampak pada arus data yang terkait dengan gabungan khusus nomor *port* dan protokol transport di ISP tersebut, tanpa memperhatikan alamat *IP* asal atau tujuan (Bitag, 2013).

Ryansyah dan Maulana (2018) menyatakan bahwa dengan penerapan metode seperti *Port Blocking*, dapat mengurangi jumlah lalu lintas jaringan di perusahaan besar, dengan penerapan metode ini, kecemasan setiap pengguna yang terhubung ke jaringan dapat diminimalkan, meningkatkan keamanan, kecepatan, dan stabilitas jaringan, administrator memiliki pengetahuan tentang *port* yang perlu dibuka dan ditutup, dan juga dapat berperan sebagai lapisan kedua dalam memblokir akses malware ke jaringan.

Pada perangkat router MikroTik, kita dapat menggunakan fungsi filter *firewall* untuk mencegah *port* dan protokol yang dimanfaatkan oleh *malware WannaCry* dalam penyebarannya. Malware ini menyerang dengan metode mengenkripsi data pada komputer yang terkena. Dalam istilah lain, apabila sistem

terjangkit malware, file atau data di komputer korban menjadi tidak dapat diakses. Untuk memulihkan akses ke data-data tersebut, pembuat malware meminta sejumlah uang tebusan. Maka itu, pendekatan keamanan dengan *blocking port* adalah satu antara pendekatan yang efektif untuk menanggulangi malware (Citraweb, 2021).

Berdasarkan Pratiwi & Akbi (2018:387) Efektivitas dalam memblokir akses *port* yang rentan terhadap penetrasi virus ke dalam jaringan adalah tujuan dari tindakan penghalangan *malware* pada port. Mengkonfigurasi pemblokiran *port* menggunakan perangkat MikroTik dengan memaksimalkan fitur *firewall*. Fungsi ini beroperasi untuk menyaring koneksi dalam jaringan. Apabila *firewall* telah diatur secara otomatis, semua *port* yang telah diblokir atau difilter tidak bisa diakses oleh klien. *Port* yang tidak mengalami penyaringan oleh perangkat Mikrotik, ketika klien meminta akses ke *server*, *server* akan memberikan respons sesuai dengan permintaan yang diajukan oleh klien. Pratiwi dan Akbi mendeskripsikan bahwa *blocking port* ini merupakan pendekatan yang sangat efektif, karena mampu mengurangi kemungkinan virus masuk melalui *port* yang tidak aman ke dalam suatu jaringan.

Maka *Port blocking* merupakan pendekatan keamanan jaringan yang biasanya digunakan dalam konfigurasi jaringan MikroTik. Tujuannya ialah untuk menghentikan akses atau memblokir jalur komunikasi tertentu, seperti *Winbox* atau *www*, sehingga pengguna tidak dapat mengakses server MikroTik. Metode *Port Blocking* merupakan satu antara pendekatan dalam mengamankan jaringan dengan tujuan mencegah dan melindungi jaringan dari potensi serangan malware dan virus yang berusaha untuk masuk ke dalam sistem jaringan.

2.1.18. Winbox

Winbox merupakan perangkat lunak atau utilitas yang digunakan untuk mengendalikan server mikrotik melalui antarmuka pengguna grafis (GUI). Apabila melakukan konfigurasi pada perangkat MikroTik dalam mode teks melalui PC utama, namun untuk mode GUI menggunakan *Winbox*, kita melakukan konfigurasi MikroTik melalui komputer klien.

Menurut Prakoso (2019) disebutkan bahwa *Winbox* sering menjadi pilihan utama dalam mengonfigurasi perangkat MikroTik. Hal ini disebabkan oleh kemudahan penggunaannya dan keuntungan dari tidak perlu menghafal perintah-perintah konsol. Memperoleh aplikasi *Winbox* dapat dilakukan dengan mengunduhnya atau mengaksesnya melalui perangkat MikroTik. Tahapnya adalah membuka peramban web dan memasukkan alamat ke dalam bilah alamat peramban (*address bar*).

Prakoso (2019) menjelaskan peran utama *Winbox*, yaitu untuk mengkonfigurasi perangkat Mikrotik. Jadi, inti dari fungsi *Winbox* adalah untuk mengatur atau mengelola perangkat Mikrotik menggunakan antarmuka grafis (GUI) yang dapat diakses melalui tampilan desktop. Selain itu, untuk merinci lebih lanjut fungsi *Winbox*, kita dapat menyebutkan:

- a. Konfigurasi *router* MikroTik.
- b. Untuk *setting bandwidth* jaringan *internet*.
- c. Guna *setting blokir* sebuah situs.

2.1.19. Command Prompt (CMD)

Berdasarkan (Syafrizal, 2020) *Command Prompt*, juga dikenal sebagai CMD, adalah sebuah jendela di sistem operasi *Windows* yang digunakan untuk mengakses

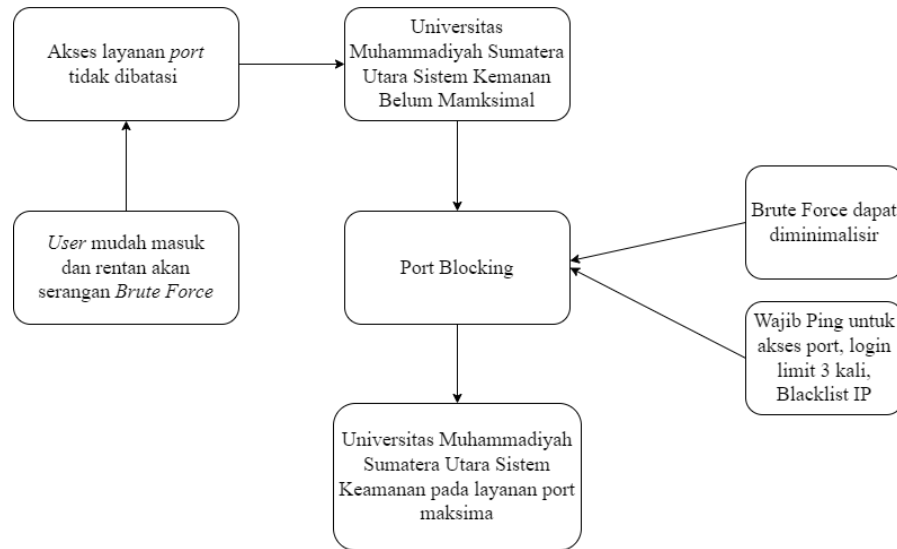
dan mengendalikan berbagai aspek dari sistem Windows. CMD bertugas menjalankan perintah-perintah yang diberikan oleh pengguna untuk mengakses informasi tentang sistem operasi *Windows*.

(Brades & Irwansyah, 2022) Dalam artikelnya dijelaskan bahwa *Command Prompt* ialah antarmuka baris perintah yang disediakan dengan sistem operasi *Windows*. Pada sistem operasi *Linux*, seringkali disebut sebagai 'root' atau 'administrator,' yang memiliki kontrol penuh atas sistem. *Command Prompt* berfungsi sebagai wadah untuk menjalankan perintah atau input. Banyak dari perintah yang dimanfaatkan untuk mengotomatisasi pekerjaan melalui skrip dan *file batch*, dengan tujuan melaksanakan tugas *administratif* dan menyelesaikan berbagai jenis masalah umum yang muncul di sistem operasi *Windows*.

Command Prompt, yang juga secara resmi dikenal sebagai *Windows Command Processor*, seringkali merujuk sebagai shell command atau menggunakan nama file *cmd.exe*. *Command Prompt* dapat diakses pada semua sistem operasi yang menggunakan dasar *Windows NT*, termasuk *Windows 10*, *Windows 8*, *Windows 7*, *Windows Vista*, *Windows XP*, *Windows 2000*, dan juga *Windows Server 2012/2008/2003*.

2.2.Kerangka Berpikir Konseptual

Struktur pemikiran konseptual merujuk pada model konseptual yang menggambarkan hubungan antara teori dan berbagai elemen yang telah diidentifikasi sebagai isu utama. Maka sebab itu, dalam konteks penelitian ini, kami akan mengacu pada struktur pemikiran konseptual yang melibatkan:



Ilustrasi 2.13 Konseptual

2.3.Hipotesis

Hipotesis implementasi *port blocking* mikrotik di Universitas Muhammadiyah Sumatera Utara adalah dengan meimplementasikan *port blocking* ini, akan mengoptimalkan serta mengamankan jaringan yang berlokasi di Universitas Muhammadiyah Sumatera Utara Medan. Juga meningkatkan rasa aman bagi para pengguna.

BAB III

METODE PENELITIAN

3.1. Jenis Penelitian

Strategi penelitian memiliki peran yang signifikan dalam sebuah penelitian karena membantu peneliti dalam memudahkan jalannya penelitian. Lebih dari itu, strategi penelitian juga dapat berkontribusi pada peningkatan mutu penelitian yang sedang dilakukan. Metode yang digunakan dalam strategi studi ini merupakan fenomenologi dengan pendekatan yang bersifat kualitatif. Berdasarkan (Juliandi et al., 2014) Riset kualitatif ialah pendekatan analisis yang didasarkan pada prinsip filsafat serta digunakan untuk menginvestigasi situasi ilmiah (eksperimen) di mana peneliti berperan sebagai alat, metode pengumpulan data, serta analisis yang lebih fokus pada interpretasi makna. Teknik Fenomenologi merupakan varian dari analisis kualitatif.

Pada studi ini, penyidik menerapkan teknik riset deskriptif, yang fokusnya ialah mengilustrasikan secara kualitatif objek yang akan dibahas, sesuai dengan realitas di lapangan, seperti analisis implementasi port blocking mikrotik di Universitas Muhammadiyah Sumatera Utara.

3.2. Defenisi Operasional

Berdasarkan (Juliandi et al., 2014) pembuatan definisi operasional bertujuan untuk menyederhanakan proses pengumpulan data, mencegah perbedaan interpretasi, dan menetapkan batasan pada cakupan variabel.

3.3.Tempat dan Waktu Penelitian

3.3.1. Tempat Penelitian

Studi ini dilaksanakan di Universitas Muhammdiyah Sumatera Utara Jalan Muctar Basri No. 3, Glugur Darat II, Kec Medan Timur.

3.4.Teknik Pengumpulan Sampel

Dalam riset ini, penyidik menerapkan teknik pengambilan contoh acak yang didasarkan pada wilayah (*Cluster Random Sampling*). Metode ini ialah pendekatan pengambilan sampel dalam bentuk kelompok. Pengambilan contoh semacam ini dilaksanakan berdasarkan wilayah khusus, dengan fokus memeriksa aspek tertentu di berbagai bagian pada sebuah entitas organisasi. Sugiyono, (2018). Pada studi ini penulis memakai sampel dengan gedung Rektor Universitas Muhammadiyah Sumatera Utara di *server*.

3.5. Teknik Pengumpulan Data

Pendekatan yang dipakai dengan penyidik demi melaksanakan Keamanan jaringan *port bloking* mikrotik pada Universitas Muhammadiyah Sumatera utara yakni:

a. Observasi

Pengamatan ialah tindakan mengamati secara langsung. Observasi ini melibatkan pemantauan infrastruktur jaringan di Universitas Mummadiyah Sumatera Utara.

b. Diskusi dan Wawancara

Melakukan perbincangan serta wawancara langsung dengan administrator jaringan serta staf terkait dalam mendiskusikan aspek yang relevan dengan objek peninjauan.

c. Studi Pustaka

Agar bisa mengakses informasi teoritis, langkahnya adalah dengan memeriksa literatur yang berkaitan dengan pengamatan yang dilakukan oleh penulis. Penulis melakukan penelusuran referensi dalam buku serta jurnal yang relevan dengan isu yang dibahasnya.

3.6. Teknik Analisis Data

Analisis informasi berdasarkan Sugiyono, (2018) merupakan proses terstruktur dalam mengeksplorasi dan mengorganisir informasi yang diperoleh melalui wawancara, observasi di lapangan, dan pengumpulan dokumen. Proses ini melibatkan pengelompokan data, penguraian menjadi unit-unit terpisah, sintesis, pengorganisasian dalam pola tertentu, penekanan pada aspek-aspek yang relevan, serta pembuatan kesimpulan agar dapat dipahami dengan baik dengan peneliti maupun pihak lainnya.

1. Reduksi Data

Berdasarkan Sugiyono, (2018) yang di maksud reduksi data merupakan tindakan merangkum informasi dengan memilih elemen kunci, memusatkan perhatian pada aspek penting yang relevan dengan topik riset, mengidentifikasi pola serta tema yang relevan, yang pada akhirnya menghasilkan ilustrasi yang lebih terfokus dan memudahkan proses pengumpulan data berikutnya. Proses pengurangan data akan dikendalikan

oleh sasaran yang telah ditetapkan sebelumnya dan hendak dicapai. Reduksi data juga merupakan suatu tindakan pemikiran yang kritis, yang membutuhkan kecerdasan serta pemahaman yang mendalam dan luas. Dalam proses pengurangan data ini, penyidik berupaya untuk menyusun rangkuman dari temuan wawancara dengan narasumber, fokus pada penyederhanaan, mengabstraksi, serta melakukan transformasi terhadap data yang diperoleh.

2. Penyajian Data

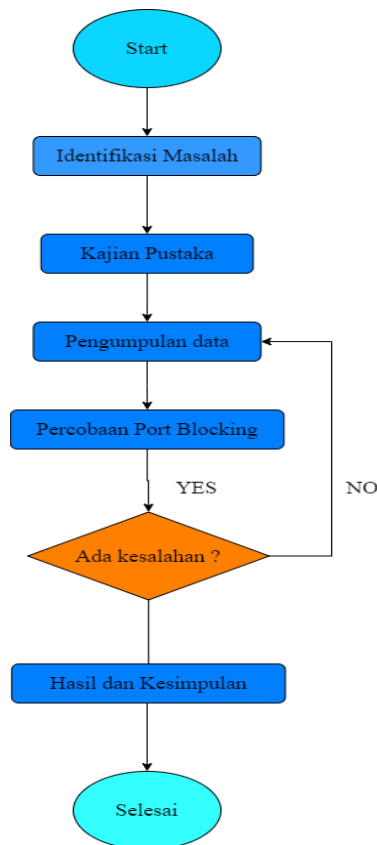
Setelah proses reduksi data selesai, langkah berikutnya adalah mengungkapkan informasi yang ada. Dalam konteks penelitian kualitatif, data dapat dipaparkan melalui berbagai cara seperti deskripsi ringkas, grafik, relasi antar kategori, diagram alir, dan metode serupa. Namun, dalam penelitian kualitatif, yang paling umum digunakan untuk mengungkapkan data adalah melalui narasi teks. Dengan cara data tersebut disajikan, data akan diatur dengan baik dan disusun sedemikian rupa untuk memudahkan pemahaman Sugiyono, (2018). Dalam menggambarkan data ini, penyidik akan memaparkan informasi dari temuan analisis yang dilakukan bersama para responden terkait efisiensi program CSR serta tanggung jawab sosial, dengan data ini diperoleh melalui tahapan wawancara dengan responden.

3. Penarikan Kesimpulan

Tahap akhir dalam analisis riset kualitatif adalah menyusun kesimpulan. Berdasarkan pendapat Sugiyono, (2018) Kesimpulan pada riset kualitatif mencakup temuan yang sebelumnya tidak pernah diidentifikasi. Temuan

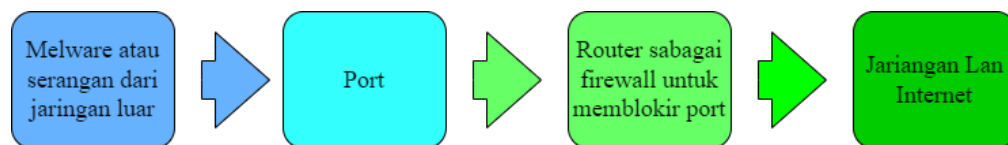
dapat berupa penjelasan atau gambaran dari suatu objek yang sebelumnya kurang begitu jelas, namun menjadi lebih terang setelah dilakukan penelitian.

Sistem keamanan dengan *port blocking* membolehkan pengguna dalam berkomunikasi dengan *server* MikroTik di dalam jaringan lokal, dengan syarat bahwa pengguna yang terhubung telah melewati proses verifikasi dari sistem keamanan MikroTik. Pada konteks penelitian ini, kerangka pemikiran yang digambarkan dalam Gambar 3.1 menguraikan pelaksanaan serta hasil pengujian keamanan jaringan lokal dengan menerapkan pendekatan *port blocking*. Tujuan dari studi ini ialah mengimplementasikan pendekatan jaringan yang sesuai serta mudah diterapkan pada jaringan lokal.



Gambar 3.1 Flowmap Alur Penelitian

Diagram blok arsitektur *port blocking* dapat ditemukan pada Gambar 3.2, yang menunjukkan struktur pemblokiran port. Sistem keamanan jaringan yang telah dikembangkan melibatkan beragam komponen perangkat keras dan perangkat lunak, sebagaimana tercantum dalam Tabel 3.2. Langkah selanjutnya adalah menyusun desain keamanan jaringan lokal menggunakan pendekatan *port blocking*. Dalam studi ini, sistem proposal menggunakan protokol TCP untuk melakukan proses autentikasi. Meskipun pengamanan *port blocking* saat ini masih memanfaatkan protokol TCP untuk melindungi *router* MikroTik, pengamanan jenis ini memerlukan bahwa pengguna yang ingin mengakses *router* MikroTik harus memiliki akses langsung ke perangkat tersebut, Ketika *port* layanan *service* diblokir untuk mengakses *router* MikroTik, maka secara otomatis layanan tersebut tidak bisa lagi digunakan dalam mencapai *router* MikroTik, seperti yang ditunjukkan dalam Gambar 3.3.

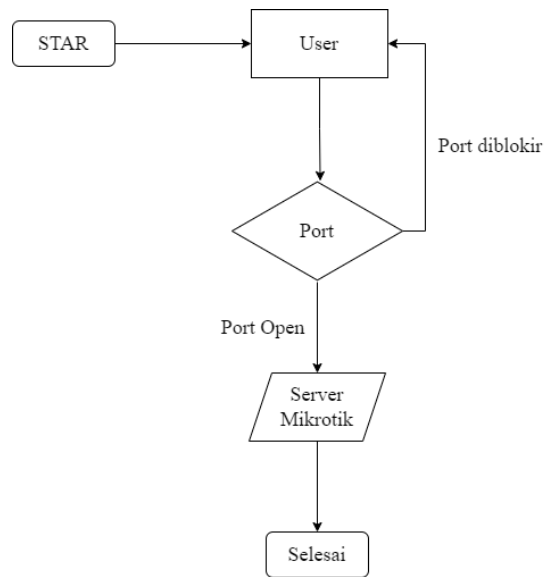


Gambar 3.2 Diagram block port blocking

Tabel 3.1 Software dan Hardware

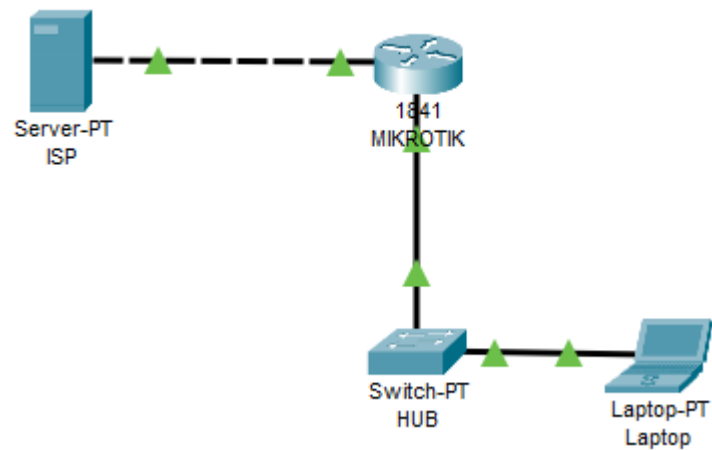
N	Jenis	Nama	Version
O	komponen	komponen	
1.	Hardware	Mikrotik Routerboard	RB-CC1036-8G- 2S+
2.	Software	Winbox Chrome	V3.35 -

		CMD	-
--	--	-----	---



Gambar 3.3 Port Blocking

Gambar 3.4 menjelaskan bahwa dalam konteks topologi sistem *port blocking* seperti yang terlihat pada ilustrasi tersebut, terdapat seorang pengguna yang menggunakan laptop sebagai klien untuk menguji *server* MikroTik yang telah diberikan perlindungan melalui *port blocking*.



Gambar 3.4 Topologi port blocking

1. ISP(*Internet Service Provider*)

Menyebarkan koneksi jaringan sehingga klien dan pengguna dapat mengakses seluruh informasi yang tersedia di internet.

2. Mikrotik

MikroTik dapat berperan sebagai gerbang internet lokal. Artinya, ini adalah perangkat yang memiliki kemampuan untuk mengatur akses internet dalam suatu jaringan.

3. *Firewall*

memantau aliran lalu lintas jaringan dan memberikan izin serta, dalam beberapa kasus, membantu menghentikan lalu lintas tertentu sesuai dengan peraturan yang ditetapkan.

4. Laptop

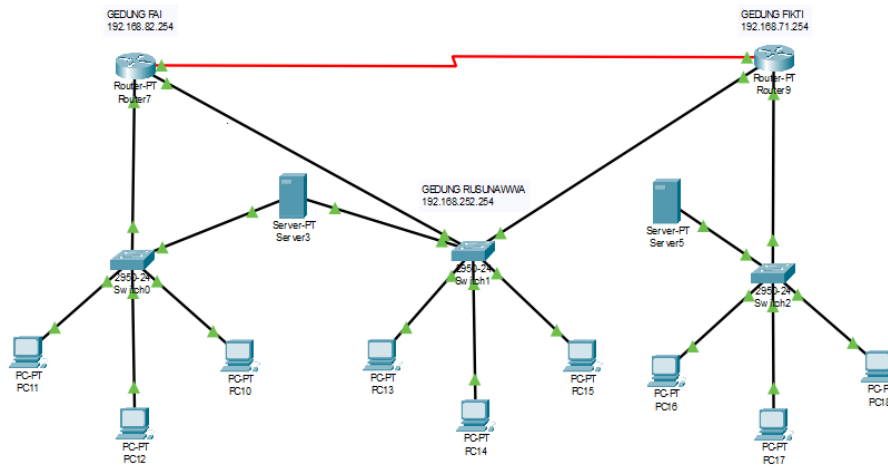
Sebagai media utama atau alat dalam proses setting port blocking

Pada awalnya, server telah dilindungi dengan mengaktifkan *firewall* di *routerboard Mikrotik* menggunakan *IP filter* untuk mengizinkan *IP* yang dikenali agar dapat mengakses layanan yang tersedia di *server*. Dengan metode port blocking, pengguna (klien) tidak bisa mengakses *server* MikroTik, bahkan jika mereka mengirimkan paket tertentu ke alamat IP MikroTik (Maulana, 2016).

3.7. Model Implementasi

Model Implementasi yang saya ambil ada tiga gedung yaitu sebagai berikut:

- Gedung FAI :
 - IP :192.168.82.254
- Gedung RUSUNAWA:
 - IP : 192.168.252.254
- Gedung FIKTI
 - IP: 192.168.71.254



Gambar 3. 5 Topologi Tiga Gedung

Dari Gedung Fai menghubungkan Gedung Rusunawa dan Gedung Rusunawa menghubungkan Gedung Fikti dari gedung 3 ini menggunakan topology Ring menghubungkan dari hub ke hub IP berubah karena menggunakan Vlan dari Router, dan Hub Cisco.

Permintaan dari pengguna terhadap kualitas jaringan semakin meningkat, baik itu di dalam LAN maupun di WAN, seperti yang terjadi di tiga gedung, yaitu FAI, Rusunawa, dan Fikti. Kualitas yang dimaksud merujuk pada kondisi jaringan komputer yang tidak mengalami kendala seperti pengiriman data yang terlambat, koneksi yang tidak stabil, dan lainnya, yang pada akhirnya dapat menghambat efisiensi kerja. Semakin luas jaringan dan semakin kompleks jaringan dan topologi multimedia yang ada dibangun, semakin sulit bagi administrator jaringan untuk memantau jaringan (Maulana & Al-Khowarizmi, 2021). Koneksi dalam jaringan komputer adalah aspek yang sangat penting, karena jika terjadi masalah pada koneksi tersebut, maka semua jenis aplikasi yang beroperasi melalui jaringan komputer tidak akan dapat berfungsi (Maulana et al., n.d.).

BAB IV

HASIL DAN PEMBAHASAN

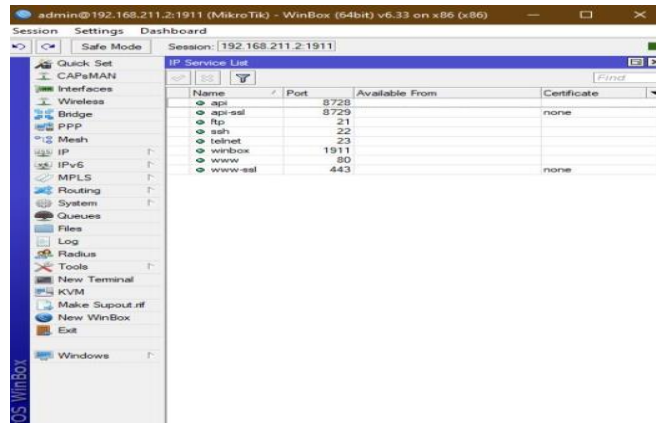
4.1 Deskripsi Data

Pada langkah ini, terjadi pengenalan terhadap keperluan reduksi data port yang dipakai dalam menerapkan sistem keamanan jaringan lokal menggunakan perangkat routerboard MikroTik. Kebutuhan akan data port yang diperlukan dalam metode *port blocking* dijelaskan secara rinci dalam Tabel 4.1. Dengan merujuk pada data dalam Tabel 4.1, strategi pengamanan dengan cara memblokir port pada *router* MikroTik melibatkan tindakan *port blocking www* serta *port winbox* secara permanen, menggunakan fitur yang tersedia pada *router* MikroTik.

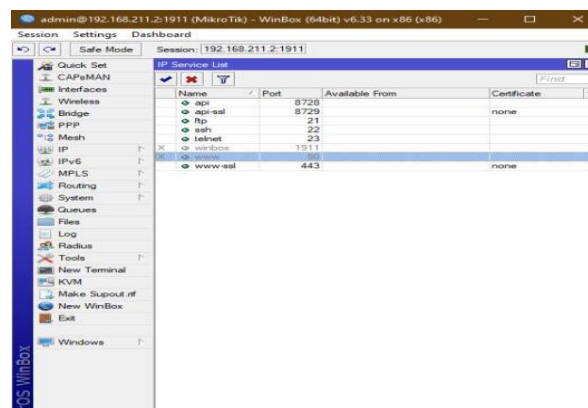
Tabel 4. 1 Kebutuhan Data Port Blocking

Port Block	Layanan	Waktu
80	WWW	-
1911	WINBOX	-

Berdasarkan Tabel 4.1 Pengaplikasian kebijakan keamanan dengan *port blocking* pada *router* MikroTik melibatkan pemblokiran permanen *port www* dan *port winbox* menggunakan fasilitas yang telah disediakan oleh *router* MikroTik. Untuk panduan konfigurasi lebih lanjut, dapat merujuk pada *ilustrasi* yang tercantum di Gambar 4.1 dan Gambar 4.2.



Gambar 4. 1 Konfigurasi Blocking Port



Gambar 4. 2 Pemilihan Port

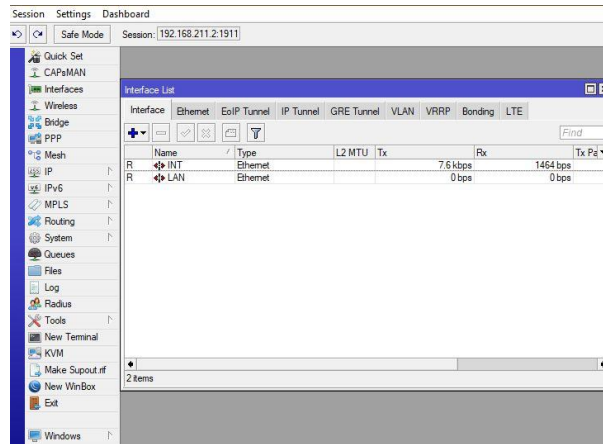
4.2 Analisis Data

4.2.1 Konfigurasi Mikrotik

Pada tahap ini melakukan beberapa bentuk konfigurasi jaringan seperti konfigurasi Ip Address, DNS, Interface, NAT, dan script yang telah didesain pada tahap design.

1. Konfigurasi Interface

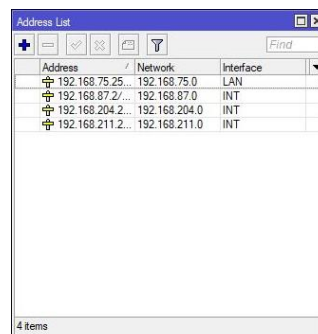
Konfigurasi interface terdapat pada menu interface, lalu aktifkan Wlan1. Kemudian hubungkan interface ether1 dengan nama INT, lalu ether 2 dengan nama LAN. Untuk memudahkan konfigurasi nama dari interface dapat diubah.



Gambar 4. 3 Konfigurasi Interface

2. Konfigurasi IP Address

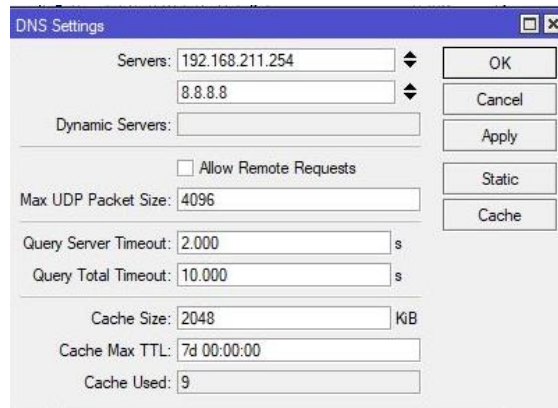
Konfigurasi IP address dilakukan dengan pemberian alamat IP address, untuk interface LAN adalah 192.168.75.25 sedangkan untuk interface INT adalah 192.168.87.2.



Gambar 4. 4 Konfigurasi Ip Address

3. Konfigurasi DNS

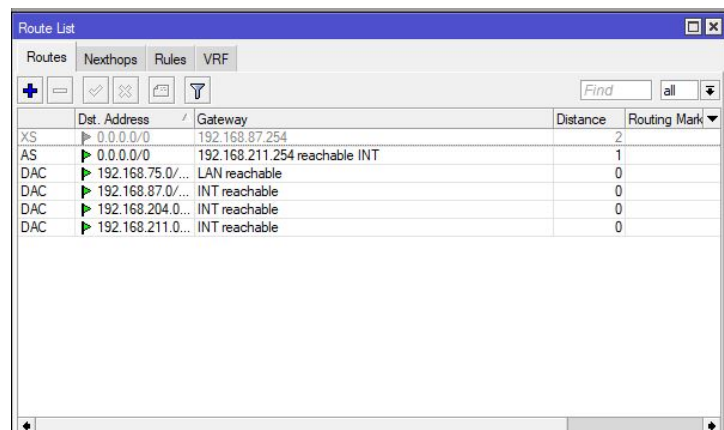
DNS dipakai demi mengartikan alamat IP menjadi domain address. Konfigurasi DNS terdapat dalam menu IP lalu pilih DNS. Untuk konfigurasi DNS dengan menggunakan DNS dari google dan IP gateway.



Gambar 4. 5 Konfigurasi DNS

4. Konfigurasi Route

Konfigurasi Routes ada pada menu Route List. Route List berfungsi untuk menampilkan daftar semua rute terdaftar untuk adress.



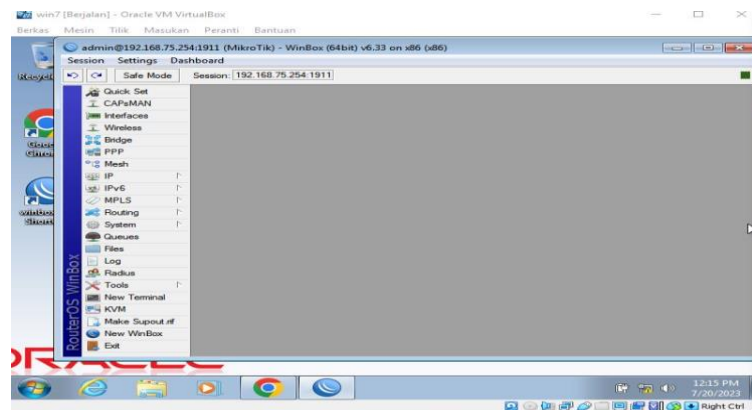
Gambar 4. 6 Konfigurasi Route

4.2.2 Pengujian Port Blocking

Pengujian *port blocking* dilaksanakan dengan mengimplementasikan pemblokiran permanen, kecuali untuk *port winbox* dan *port www*. Dengan pemblokiran permanen, pengguna tidak bisa mengakses sepenuhnya *router* MikroTik melalui layanan *winbox* dan *www*. Di sisi lain, dengan pemblokiran terkecuali, pengguna masih dapat meremote *router* MikroTik menggunakan layanan *winbox* dan *www* dengan menggunakan alamat IP yang telah diatur

sebelumnya. Proses pemeriksaan sebelum melakukan *port blocking* dapat ditemukan dalam Gambar 4.7 dan 4.8.

Selanjutnya, dilakukan penerapan *blocking port* pada perangkat MikroTik. *Port* yang diblokir termasuk *port www/80* dan *port winbox/1911*. Kemudian, pengujian langsung dilakukan setelah tindakan *blocking port*, sebagaimana terlihat di Gambar 4.9 dan 4.10.

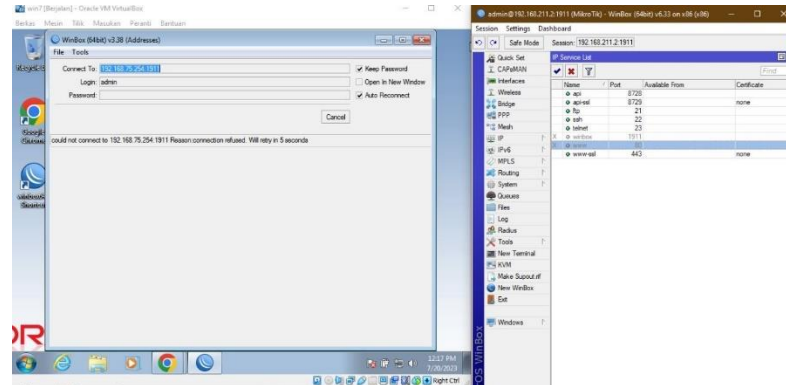


Gambar 4. 7 Koneksi Winbox Sebelum diblock

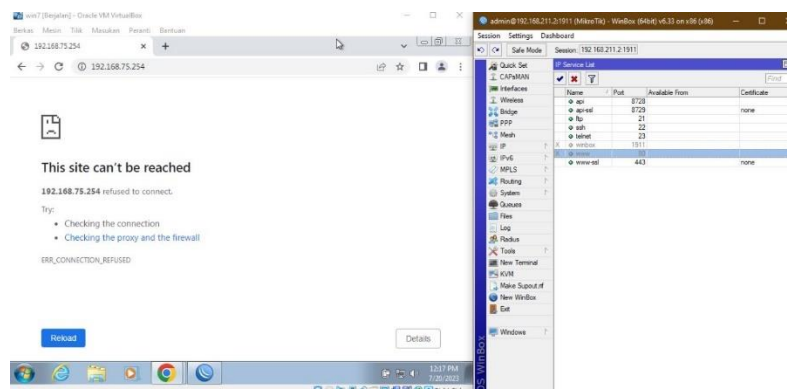


Gambar 4. 8 Koneksi WWW Sebelum diblock

Setelah semua langkah penerapan konfigurasi metode *port blocking* dilakukan, data dari pengujian pemblokiran port diuraikan dalam Tabel 4.2.



Gambar 4. 9 Koneksi Winbox Setelah di block



Gambar 4. 10 Koneksi WWW Setelah di block

Seperti pada gambar diatas pada gambar 4.9,dan 4.10 ketika kita matikan settingan port dan www kita tidak bisa melakukan remote sistem terhadap mikrotik melalui winbox dan situs.

Tabel 4. 2 Hasil Pengujian Port Blocking

No	Komponen Uji	Keterangan
1	Akses Winbox	<i>Gagal</i>
2	Akses WWW	<i>Gagal</i>

Penerapan perlindungan jaringan lokal telah dilakukan dengan menerapkan pendekatan *Port Blocking*. Hasil studi telah mengungkapkan keunggulan dan kekurangan dari teknik Pemblokiran *Port*. Keuntungan dari *Port Blocking* ialah

kemudahan dalam konfigurasi untuk memblokir akses *port*, serta bisa mengatasi kelemahan dalam mengamankan akses *port* layanan *server* MikroTik. *Port blocking* memiliki kekurangan hanya memungkinkan akses ke *server* MikroTik melalui alamat MAC, dan hanya memungkinkan akses ke server MikroTik melalui kabel UTP RJ45.

BAB V

PENUTUP

5.1 Kesimpulan

Sistem, prosedur, dan metode yang menjaga database, situs web, dan aplikasi dari tindakan yang disengaja maupun tidak disengaja. Sistem yang aman memastikan kebijakan privasi data yang terdapat di dalamnya.

Dari hasil pengujian keamanan menggunakan port winbox dan www pada Universitas Muhammadiyah Sumatera Utara masih kurang dari hasil pengujian dari dua komponen uji dengan sistem keamanan gagal.

Penerapan keamanan jaringan lokal telah dilakukan melalui penerapan metode pemblokiran port. Dari temuan analisis, ditemukan keunggulan dan kekurangan dari pendekatan *Port Blocking*. Keunggulan dari *Port Blocking* sendiri ialah kemudahan dalam mengkonfigurasi pemblokiran akses *port*, juga dapat secara efektif menutup potensi celah keamanan pada layanan *port* jaringan. *Port blocking* memiliki keterbatasan di mana akses ke *server* MikroTik hanya dapat dilakukan melalui pengenalan alamat MAC, dan akses ke server jaringan hanya mungkin melalui kabel UTP RJ45. Untuk studi selanjutnya, penting untuk mempertimbangkan implementasi pada *port* lainnya sehingga jumlah *port* yang terbuka untuk potensi serangan peretasan dapat diminimalkan. Selain itu, pengujian lebih lanjut seperti simulasi serangan pada port yang telah diterapkan metode keamanan *Port blocking* juga perlu dilakukan.

5.2 Saran

Pada studi berikutnya, diperlukan penerapan teknik serupa pada *port* yang berbeda agar tidak terlalu banyak *port* yang terbuka untuk potensi serangan *hacking*. Selain itu, pengujian tambahan dapat mencakup simulasi serangan pada *port* yang telah diterapkan dengan metode keamanan *Port blocking*.

DAFTAR PUSTAKA

- Anggraeni, E. Y. (2017). *Pengantar Sistem Informasi* (E. Risanto (ed.)). CV. Andi Offset.
- Brades, T., & Irwansyah, I. (2022). Pemanfaatan Metode Port Knocking dan Blocking Untuk Kamanan Jaringan BPKAD Provinsi Sumsel. *Prosiding Semhavok*, 3(2), 99–107.
- Farunudin, R. (2013). *Membangun Firewall Dengan IPTables Di Linux*. PT Elex Media Komputindo.
- Hadi, A. (2016). *Administratif Jaringan Komputer* (Pertama). Kencana.
- Huthaeen, J. (2015). *Konsep Sistem Informasi*. Deepublish.
- Irawan, D. (2015). Keamanan jaringan komputer dengan metode blocking port pada laboratorium komputer program diploma-iii sistem informasi universitas muhammadiyah metro. *Manajemen Informatika Program Diploma III UM Metro*, 02(05), 1–9.
- Istiana, P. (2019). *Teknologi Informasi Dan Komunikasi*. Yudhistira Ghalia Indonesia.
- Juliandi, A., Irfan, & Manurung, S. (2014). *Metodologi Penelitian Bisnis Konsep Dan Aplikasi*. Umsu Press.
- Lukman, A. M., & Bachtia, Y. (2016). Analisis sistem keamanan jaringan dengan. *Computer Engineering, System And Science*, 1(1), 9–14.
- Maulana, H. (2016). Analisis Dan Perancangan Sistem Replikasi Database Mysql Dengan Menggunakan Vmware Pada Sistem Operasi Open Source. *InfoTekJar (Jurnal Nasional Informatika Dan Teknologi Jaringan)*, 1(1), 32–37. <https://doi.org/10.30743/infotekjar.v1i1.37>

- Maulana, H., & Al-Khowarizmi. (2021). Analyze and designing low-cost network monitoring system using Icinga and Raspberry Pi. *IOP Conference Series: Earth and Environmental Science*, 704(1). <https://doi.org/10.1088/1755-1315/704/1/012038>
- Maulana, H., Lubis, H., Teknik, J., Sekolah, I., Teknik, T., Sistem, J., Sekolah, I., Teknik, T., Management, I., Management, S., Cloud, U. E., & Computing, C. (n.d.). *Membangun Private Cloud Pada Vmware Dengan*.
- Nucahyo, A. C., Firgia, L., & Himanunanto, R. (2021). *Konfigurasi & Analisis Jaringan Berbasis Mikrotik* (D. R. Rizqian (ed.)). Amerta Media.
- Rizal, R., Ruuhwan, R., & Nugraha, K. A. (2020). Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941. *Jurnal ICT : Information Communication & Technology*, 19(1), 1–8. <https://doi.org/10.36054/jict-ikmi.v19i1.119>
- Sugiyono. (2018). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Alfabeta.
- Sumardi, R. A. T. (2013). Rancang Bangun Sistem Keamanan Jaringan Dengan Metode Blocking Port Pada Sekolah Menengah Kejuruan Karya Nugraha Boyolali. *Indonesia Jurnal on Networking and Security*, 2(Jaringan), 16–21.
- Sutabri, T. (2012). *Analisis Sistem Informasi* (C. Putri (ed.)). CV. Andi Offset.
- Suwarya, F. M. (2021). *Belajar Dengan Jaringan Komputer*. Guepedia.
- Syafrizal, M. (2020). *Pengantar Jaringan Komputer*. Andi.
- Tahir, M. (2023). *Pengantar Jaringan Komputer Dasar*. CV. Literasi Nusantara Abadi.
- Wahyono, T. (2017). *Building & Maintenance Pc Server*. Elex Media Komputindo.
- Wahyuddin S, S. N., Ariantoro, T. R., Yanto, G., Yuswardi, & Dewantara, R.

(2023). *Sistem Operasi Komputer* (Ariyanto (ed.)). Global Eksekutif Teknologi.