



# **SIMULASI UNTUK PENINGKATAN KEAMANAN DATA PADA METAROUTER YANG SUDAH TEREKSPLOITASI**

Kristono

13917119

*Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer*

*Konsentrasi Digital Forensik*

*Program Studi Magister Teknik Informatika*

*Program Pascasarjana Fakultas Teknologi Industri*

*Universitas Islam Indonesia*

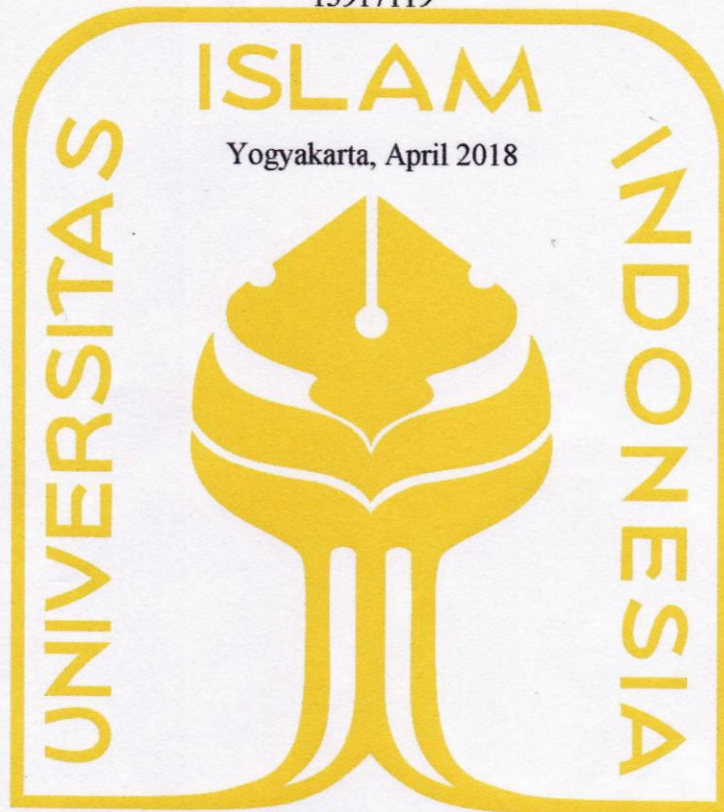
2018

**Lembar Pengesahan Pembimbing**

**Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter  
Yang Sudah Tereksplorasi**

Kristono

13917119



Pembimbing  
الإمامية الإسلامية  
التي تأسست في  
الهندو

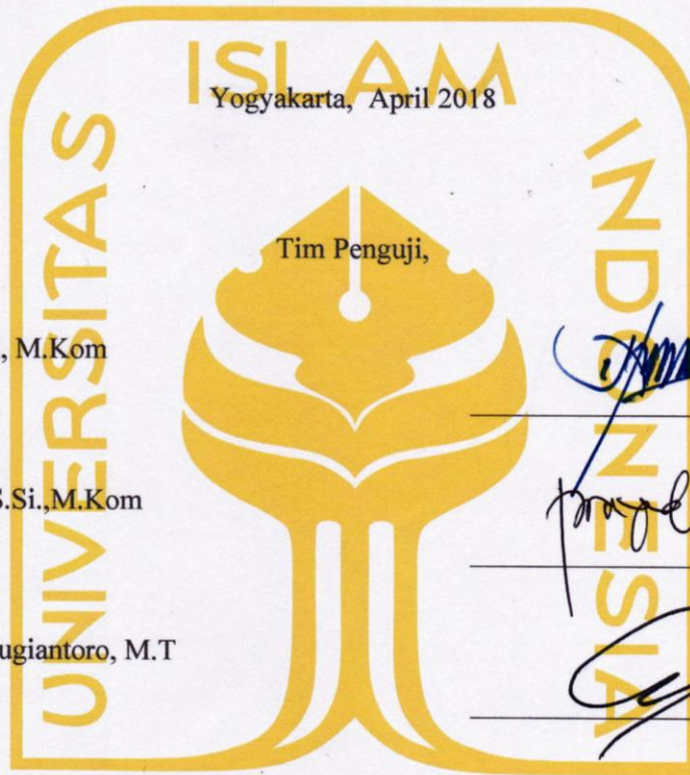
Dr. Imam Riadi, M.kom

**Lembar Pengesahan Penguji**

**Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter  
Yang Sudah Tereksplorasi**

Kristono

13917119



Yogyakarta, April 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom

Ketua

Yudi Prayudi, S.Si., M.Kom

Anggota I

Dr. Bambang Sugiantoro, M.T

Anggota II

*[Handwritten signatures of Dr. Imam Riadi, Yudi Prayudi, and Dr. Bambang Sugiantoro]*

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia



*[Handwritten signature of Dr. R. Veduh Dirgahayu]*  
Dr. R. Veduh Dirgahayu, ST., M.Sc

## **Abstrak**

### **Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter Yang Sudah Tereksplorasi**

MetaROUTER sebagai media dalam implementasi yang digunakan untuk keamanan data dengan metode simulasi. Dimana komputer yang terhubung dalam sebuah jaringan seakan memiliki router sendiri dalam manajemen jaringannya, dengan Metarouter yang telah dibuat akan mempermudah monitoring traffic aktifitas user tanpa mengganggu user lain walaupun dalam satu routerboard. Dalam perkembangan teknologi informasi sekarang ini sering kita mendengar istilah virtualisasi, teknik virtualisasi merupakan sebuah teknik versi virtual dari sistem komputer, sumber daya jaringan computer maupun sebuah perangkat penyimpanan.

Metarouter juga memungkinkan memonitoring beberapa aktifitas user secara bersamaan tanpa dengan hanya menggunakan satu routerboard. Untuk itu penulis mengharapkan dalam penelitian ini teknologi MetaROUTER selain dimanfaatkan untuk menghemat juga dikembangkan untuk manajemen dan keamanan data dalam sebuah jaringan komputer dengan metode simulasi monitoring trafic.

Dalam penelitian ini di simulasikan keamanan data dari serangan DoS ( Denial of Service) didalam MetaRouter yang tereksplorasi . Sehingga diharapkan akan mempermudah dalam monitoring data dan manajemen network dalam sebuah mikritik manajemen. Dengan menggunakan Metarouter maka sebuah RouterOS dapat menjalankan beberapa RouterOS lainnya dalam bentuk virtual.

#### **Kata kunci**

Metarouter, DoS ( Denial of Service), Keamanan Data , Mikrotik

## **Abstract**

### **Simulation For Increasing Of The Savety Of The Data Metarouter Which Is Explotased**

MetaROUTER as a medium in the implementation that is used for data security with the method of simulation. Where computers connected in a network as if the router had a huge jaringanya in the management of its own, with the works Metarouter has been monitoring traffic will make it easier for user activities without bothering other users even in a routerboard . In the development of information technology nowadays we often hear the term virtualisai, techniques of virtualization is a virtual version of the technique of computer systems, computer network resources as well as a storage device.

Metarouter also allows monitor several user activity simultaneously without using a routerboard. For that the author expects in this research are utilized in addition to MetaROUTER technology to save also developed for management and security of data in a computer network with monitoring traffic simulation method.

In this study on simulate security data from DoS attacks (Denial of Service) within the MetaRouter being exploited. So will hopefully memepermudah in monitoring data and management network in an mikritik management. Using Metarouter then a RouterOS RouterOS can run multiple virtual forms in the other.

#### **Keywords**

Metarouter, DoS (Denial of Service), Data Security, Mikrotik

## Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, April 2018

Kristono, S.Kom



## **Daftar Publikasi**

Tidak ada publikasi yang menjadi bagian dari tesis.

## **Halaman Kontribusi**

Tidak ada kontribusi dari pihak lain.



## Halaman Persembahan

Segala Puji Syukurku kepada Allah yang maha kuasa atas anugrah dan karunianya, serta cinta kasih dan perlindungannya yang telah memberikan kekuatan, kesehatan, kesabaran dan memberikan akal hikmat marifat dalam hidupku ini, sehingga oleh kasih-Nya aku bisa menyelesaikan Thesis ini dengan baik.

- Terimakasih kepada Bapak dan Ibuku tercinta yang selalu memberikan semangat, motivasi dan doanya, Doa-doamu slalu menemani dan menyertai sepanjang hidupku.
- Terimakasih kepada Bapak Yudi Prayudi dan bapak Imam Riadi selaku dosen pembimbing yang selalu sabar membimbingsaya dalam menyelesaikan Thesisku ini.
- Terimakasih kepada istriku tercinta Rina Ida Pratiwi yang slalu memberikan semangat, motivasi dan doanya.
- Terimakasih kepada teman-teman yang selalu support, berbagi ilmu dan saling membantu , semuanya luarbiasa, mantaf jiwa.
- Terimakasih buat keluarga besar STMIK AUB Surakarta yang sudah memberikan dukungan dan waktunya untuk saya menyelesaikan Thesis.

## Kata Pengantar

Segala puji syukur penulis panjatkan kepada Allah yang maha kuasa , atas segala anugrah dan karunia-Nya, sehingga tesis dengan judul “Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter Yang Sudah Tereksplotasi” ini dapat diselesaikan dengan baik.

Tesis ini disusun untuk memenuhi salah satu persyaratan memperoleh gelar Magister Komputer (M.Kom.) pada program studi Magister Teknik Informatika Universitas Islam Indonesia dengan sumber dana berasal dari dana mandiri.

Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa hormat dan menghaturkan terima kasih yang sebesar-besarnya, kepada :

1. Bapak Yudi Prayudi,S.Si.,M.Kom atas bimbingan, arahan dan waktu yang diluangkan kepada penulis untuk berdiskusi selama menjadi dosen pembimbing. Terima kasih juga karena selalu memberikan motivasi kepada saya sehingga saya mampu menyelesaikan tesis ini.
2. Bapak Dr. Imam Riadi,M.Kom, Bapak Dr. Bambang Sugiantoro yang telah memberikan masukan dan saran seminar proposal dan seminar hasil tesis.
3. Ketua Program Studi Pasca Sarjana Fakultas Teknik Industri Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc.
4. Seluruh dosen Pasca Sarjana Program Studi Magister Teknik Informatika khususnya jurusan Digital Forensik.
5. Ayahanda Sumarjo, Ibunda Kristuni, Istriku tercinta Rina Ida Pratiwi, anakku Shirlene dan Sharrone dan seluruh keluarga besar atas segala doa dan supportnya.
6. Bapak Agus Widiyanto,S.Kom.,M.Sc yang atas training dan sharing ilmunya di Solo.
7. Rekan rekan seperjuangan Grup “Wisuda Bersama”. Kalian memang luar biasa dan Mantaf Jiwa Kawan.
8. Kepada semua pihak yang sudah membantu yang tidak dapat saya sebutkan satu persatu.

Dengan keterbatasan pengalaman, ilmu maupun pustaka yang ditinjau, penulis menyadari bahwa tesis ini masih banyak kekurangan dan perlu pengembangan lanjutan agar benar benar bermanfaat. Oleh sebab itu, penulis sangat mengharapkan kritik dan saran agar tesis ini lebih sempurna serta sebagai masukan bagi penulis untuk penelitian dan penulisan karya ilmiah di masa yang akan datang.

Akhir kata, penulis berharap tesis ini memberikan manfaat bagi kita semua terutama untuk pengembangan ilmu pengetahuan dalam bidang digital forensik.

Yogyakarta, 02 April 2018

A handwritten signature in black ink, consisting of a stylized 'K' followed by a horizontal line and a small flourish.

Kristono, S.Kom

## Daftar Isi

Lembar Pengesahan Pembimbing.....	i
Lembar Pengesahan Penguji.....	<b>Error! Bookmark not defined.</b>
Abstrak .....	iii
Abstract .....	iv
Pernyataan Keaslian Tulisan .....	v
Daftar Publikasi .....	vi
Halaman Kontribusi .....	vii
Halaman Persembahan .....	viii
Kata Pengantar .....	ix
Daftar Isi.....	xi
Daftar Tabel.....	xiv
Daftar Gambar .....	xv
Glosarium .....	xvii
<b>BAB 1</b> Pendahuluan.....	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	4
1.3 Batasan Masalah .....	4
1.4 Tujuan Penelitian .....	4
1.5 Manfaat Penelitian .....	5
1.6 Metode Penelitian .....	5
1.7 Sistematika Penulisan .....	6
1.8 Literatur Review .....	7
<b>BAB 2</b> Tinjauan Pustaka.....	<b>13</b>
2.1 Landasan Teori .....	13
2.1.1 Manajemen Jaringan .....	13

2.1.2	Konsep Virtualisasi.....	15
2.1.3	Router.....	16
2.1.4	Mikrotik Router OS.....	17
2.1.5	MetaRouter.....	19
2.1.6	Keamanan Data.....	20
2.1.7	WINBOX 3.11.....	21
BAB 3 Metode Penelitian.....		23
3.1	Literature.....	23
3.1.1	Hardware.....	24
3.1.2	Software.....	24
3.2	Setting Jaringan.....	24
3.3	Pengambilan data metarouter.....	25
3.4	Eksploitasi Metarouter.....	27
3.4.1	Footprinting.....	27
3.4.2	Scanning.....	28
3.4.3	Enumeration.....	28
3.4.4	Gaining Access.....	28
3.4.5	Escalating Privilege.....	29
3.4.6	Pilfering.....	29
3.4.7	Covering Track.....	29
3.4.8	Creating Backdoors.....	30
3.4.9	Denial Of Service.....	30
3.5	Konfigurasi Keamanan Data.....	30
3.5.1	Services.....	31
3.5.2	Disable Service.....	33
3.5.3	Available From.....	33
3.5.4	Ubah Port.....	34

3.5.5	Management User .....	34
3.5.6	Group Policies .....	35
3.5.7	Allowed Address .....	36
3.5.8	MikroTik Neighbor Discovery Protocol (MNDP) .....	37
3.6	Simulasi dan Pengujian .....	38
3.6.1	Desain .....	38
3.6.2	Addressing.....	39
3.6.3	Access Control.....	40
3.6.4	Implementasi desain .....	40
3.6.5	Pengujian.....	40
3.7	Analisis.....	41
3.8	Kesimpulan.....	42
<b>BAB 4 HASIL DAN PEMBAHASAN.....</b>		<b>43</b>
4.1	Setting Metarouter .....	43
4.1.1	Melakukan pengaturan IP network.....	43
4.1.2	Melakukan Setting Metarouter.....	44
4.1.3	Pengambilan Data Metarouter.....	47
4.2	Skenario Pengujian Serangan DoS (Denial of Service).....	49
4.3	Keamanan Data.....	52
4.4	Hasil Pengujian.....	54
<b>BAB 5 KESIMPULAN DAN SARAN.....</b>		<b>58</b>
5.1	Kesimpulan.....	58
5.2	Saran .....	58

## Daftar Tabel

Tabel 1.1 Literatur Review.....	10
Lanjutan Tabel 1.2 Literatur Review .....	11
Lanjutan Tabel 1.3 Literatur Review .....	12
Tabel 3.1 IP Address.....	39
Tabel 3.2 Acces Control List.....	40
Tabel 3.3 Pengujian akses .....	40
Tabel 4.1 Hasil Pengujian Port 80 .....	54
Tabel 4.2 Hasil Pengujian Port 22 .....	56

## Daftar Gambar

Gambar 1.1 Topologi Metarouter .....	3
Gambar 2.1 Arsitektur Manajemen Jaringan .....	14
Gambar 2.2 Konsep Virtualisasi .....	15
Gambar 2.3 Contoh Sebuah Jaringan dengan Network .....	16
Gambar 2.4 Penggunaan Mikrotik RouterOS .....	18
Gambar 2.5 Pemanfaatan Metarouter .....	20
Gambar 3.1 Flowchart Penelitian Metarouter .....	23
Gambar 3.2 Topologi Jaringan .....	24
Gambar 3.3 Metarouter Setting New .....	25
Gambar 3.4 Virtual Ethernet Instalasi .....	26
Gambar 3.5 Instalasi OS dalam Metarouter .....	27
Gambar 3.6 Service list .....	31
Gambar 3.7 Disable list .....	33
Gambar 3.8 Available Form .....	34
Gambar 3.9 Ubah Port .....	34
Gambar 3.10 Group Police .....	35
Gambar 3.11 Allowed Address .....	37
Gambar 3.12 MikroTik Neighbor Discovery Protocol (MNDP) .....	38
Gambar 3.13 Topologi Jaringan yang dibangun .....	39
Gambar 4.1 Setting IP Networ di Virtual Box .....	43
Gambar 4.2 Pembuatan IP adres .....	44
Gambar 4.3 Membuat MetaRouter .....	45
Gambar 4.4 Console Meta router .....	46
Gambar 4.5 Setting Virtual Ethernet .....	46
Gambar 4.6 setting interface metarouter .....	46
Gambar 4.7 Create Client Metarouter .....	47
Gambar 4.8 Koneksi Metarouter Client .....	48
Gambar 4.9 Pengambilan Paket data Metarouter .....	48
Gambar 4.10 Konsep serangan DoS .....	49
Gambar 4.11 Simulasi Serangan DOS dengan Ping ICMP .....	50



Gambar 4.12 Simulasi traffic Sebelum terjadi serangan.....	51
Gambar 4.13 Hasil Serangan DoS .....	51
Gambar 4.14 Diagnosa Firewal .....	52
Gambar 4.15 Diagnosa interface network.....	52
Gambar 4.16 Diagnosa pada Kinerja CPU.....	52
Gambar 4.17 Melakukan Pembatasan IP Addres.....	53
Gambar 4.18 Pembatasan Paket pada Traficc.....	53
Gambar 4.19 Melakukan pemmfilteran SYN .....	53
Gambar 4.20 Ilustrasi Peningkatan Keamanan Port 80 .....	55
Gambar 4.21 Gambar Ilustrasi Pengamanan Port 22 .....	57

## Glosarium

Berikut ini merupakan istilah-istilah beserta definisinya atau singkatan beserta kepanjangan yang spesifik/khusus terkait “Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter Yang Sudah Tereksplorasi”

LAN	- Local Area Network
MAN	- Metropolitan Area Network
WAN	- Wide Area Network
ACLs	- Access Control Lists (ACLs)
NAT	- Network Address Translation
DNS	- Domain Name System
DHCP	- Dynamic Host Configuration Protocol
ISP	- Internet service provider
VPN	- Virtual Private Network
DOS	- Denial of Service
NMS	- Network Management Station
CMIP	- Common Management Information Protocol
GUI	- Graphical User Interface
CLI	- Command Line Interface
ADSL	- Asymmetric digital subscriber line
MIPS	- Microprocessor without Interlocked Pipeline Stages
API	- Application Programmable Interface
FTP	- File Transfer Protocol
SSH	- Secure Shell
MNDP	- MikroTik Neighbor Discovery Protocol

# **BAB 1**

## **Pendahuluan**

### **1.1 Latar Belakang**

Jaringan komputer merupakan kumpulan dari beberapa komputer yang saling terhubung melalui kabel maupun wireless dan dapat berkomunikasi satu dengan yang lainnya dengan menggunakan aturan (protocol) tertentu. Mengelola jaringan yang terdiri dari beberapa komputer merupakan pekerjaan yang masih dapat dilakukan dengan mudah. Namun bila jaringan tersebut berkembang, maka untuk mengelola jaringan akan menjadi sangat sulit bagi setiap pengelola jaringan (Administrator Jaringan).

Untuk mengelola jaringan dengan skala besar tersebut maka jaringan (network) itu harus dipisahkan menjadi beberapa jaringan kecil. Mengatur beberapa jaringan kecil yang berisi puluhan host, tentu akan lebih mudah daripada mengatur sebuah jaringan yang berisi ratusan bahkan ribuan host. Teknik memisahkan jaringan ini dapat diimplementasikan untuk jaringan (LAN), jaringan skala menengah (MAN) maupun jaringan besar (WAN/Internet).

Setelah jaringan tersebut dipisahkan menjadi beberapa jaringan kecil, maka pekerjaan selanjutnya adalah menghubungkan kembali jaringan-jaringan kecil tersebut. Dalam topologi jaringan di sebuah laboratorium memiliki ruangan untuk Praktikum, Server, Teknisi, dan Dosen. Setiap ruangan memiliki kebutuhan dan Access Control Lists (ACLs) berbeda. ACLs pada Laboratorium Komputer Jaringan Komputer terpusat pada router server, ACLs yang banyak dan terpusat dapat menyebabkan traffic padat. Pemisahan ACLs berdampak pada penggunaan router yang lebih banyak dan menyebabkan biaya berlebih untuk pembelian router, pemakaian listrik dan penggunaan ruang penyimpanan. Permasalahan tersebut dapat diatasi dengan virtualisasi. Router Mikrotik dapat menerapkan virtualisasi dengan MetaRouter yang berdampak pada penghematan biaya pembelian hardware router, penggunaan listrik, dan tempat penyimpanan. Virtualisasi router menggunakan MetaRouter dapat menghemat biaya pembuatan jaringan komputer, pemakaian energi listrik dan penggunaan tempat dibandingkan router non-virtualisasi (Galang dkk, 2017).

Router merupakan perangkat penting dalam sebuah jaringan, banyak bukti-bukti yang dapat diambil dari aktivitas jaringan, selain itu router juga secara cerdas mampu

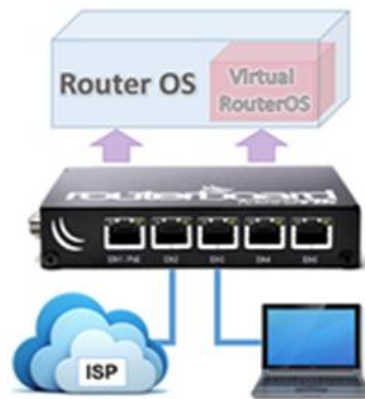
mengetahui kemana alur tujuan informasi (quota) yang akan dilaluinya. Bukti-bukti yang dapat diambil dari router antara lain konfigurasi firewall, mac address, daftar ip address client, aktivitas logging admin dan lain-lain. ( Liu Chen, Yu, & Fu, 2010 ).

Mikrotik routerOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk menjadikan komputer biasa menjadi router network yang handal, mencakup berbagai fitur yang dibuat untuk ip network dan jaringan wireless. Fitur-fitur tersebut diantaranya : Firewall & Nat, Routing, Hotspot, Point to Point Tunneling Protocol, DNS server, DHCP server, Hotspot, dan masih banyak lagi fitur lainnya.

Mikrotik dapat digunakan dalam 2 tipe, yaitu dalam bentuk perangkat keras dan perangkat lunak. Dalam bentuk perangkat keras, Mikrotik biasanya sudah diinstalasi pada suatu board tertentu, sedangkan dalam bentuk perangkat lunak, Mikrotik merupakan satu distro Linux yang memang dikhususkan untuk fungsi router. MikroTik RouterOS™, merupakan sistem operasi Linux base yang diperuntukkan sebagai network router. Didesain untuk memberikan kemudahan bagi penggunaannya. Administrasinya bisa dilakukan melalui Windows Application (WinBox). Selain itu instalasi dapat dilakukan pada Standard komputer PC (Personal Computer). PC yang akan dijadikan router mikrotik pun tidak memerlukan resource yang cukup besar untuk penggunaan standard, misalnya hanya sebagai gateway. Untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) disarankan untuk mempertimbangkan pemilihan resource PC yang memadai.

Metarouter merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru secara virtual baik untuk penerapan virtualisasi router maupun virtualisasi topologi jaringan. Hampir sama seperti aplikasi VMware atau VirtualPC. Dengan Metarouter sebuah routerboard mikrotik akan mampu menjalankan beberapa RouterOs dalam bentuk virtualisasi selain Router OS dengan Metarouter dapat juga dijalankan sebuah OS lain misalkan sistem operasi Linux Openwrt. Untuk itu dengan Metarouter memungkinkan dalam satu router bisa digunakan untuk berbagai hal misal membangun RouterOs Virtual, membangun Server Virtual, juga bisa membangun topologi jaringan. Selain itu bisa digunakan untuk menyederhanakan konfigurasi yang apabila disatukan akan sangat sulit atau bahkan membingungkan, contohnya untuk load balancing dua ISP sekaligus bandwidth manager sekaligus juga firewall ditambah pula VPN, akan sangat bijaksana bila dipisah-pisahkan dan dijalankan pada Metarouter dalam sebuah h/w Mikrotik. Dari kegunaan yang sangat banyak Metarouter memungkinkan lebih hemat dari

penggunaan daya dengan satu router seakan akan memiliki banyak router yang digunakan serta lebih praktis.



Gambar 1.1 Topologi Metarouter

Sistem Operasi MikroTik dirancang sebagai router jaringan. Dan yang dapat digunakan untuk membuat komputer menjadi router network yang handal. Fungsi dari MikroTik meliputi Firewall & Nat, Bandwidth Limiter, Routing, Hotspot, Point to Point Tunneling Protocol, DNS Server, DHCP Server, Hotspot dan masih banyak lagi fungsi dari MikroTik.

Karena terhubung dalam sebuah jaringan, maka sebuah komputer rawan terhadap penyusupan dari luar. Jika seseorang dapat menyusup ke sebuah komputer maka orang tersebut dapat mengambil data-data yang disimpan di komputer tersebut dan menggunakannya untuk keuntungan pribadi. Keamanan data menjadi hal penting dalam komunikasi data yang dilakukan. Bila data user ID dan password dari layanan yang gunakan jatuh ke tangan orang yang salah, bisa saja orang tersebut akan memanfaatkan untuk hal-hal yang tidak bertanggung jawab. Keamanan data Merupakan aktivitas untuk menjaga agar sumber daya informasi tetap aman. Hal ini dibutuhkan dalam sebuah aktifitas jaringan maka dibutuhkan monitoring alur akses yang dilakukan agar akses data yang mencurigakan dapat teratasi sebelum hal yang tidak diinginkan terjadi.

Berdasarkan latar belakang yang telah dipaparkan maka ranah dalam penelitian ini adalah melakukan eksploitasi dan monitoring digital yang terdapat pada mikrotik RouterOS dengan memanfaatkan Metarouter sebagai media dalam implementasi yang digunakan untuk keamanan data dengan metode simulasi. Dimana komputer yang terhubung dalam sebuah jaringan seakan memiliki router sendiri dalam manajemen jaringannya, dengan Metarouter yang telah di buat akan mempermudah monitoring traffic aktifitas user tanpa mengganggu user lain walaupun dalam satu routerboard. Metarouter juga memungkinkan

memonitoring beberapa aktifitas user secara bersamaan tanpa dengan hanya menggunakan satu routerboard. Untuk itu penulis mengharapkan dalam penelitian ini teknologi Metarouter selain dimanfaatkan untuk menghemat juga di kembangkan untuk manajemen dan keamanan data dalam sebuah jaringan komputer dengan metode simulasi monitoring trafic.

## **1.2 Rumusan Masalah**

Dari paparan latarbelakang yang sudah ada, maka dapat saya ambil rumusan masalah sebagai berikut :

- a. Bagaimana Karakteristik MetaRouter dalam sebuah manajemen network ?
- b. Bagaimana mengeksploitasi MetaRouter dalam keamanan data ?
- c. Bagaimana melakukan teknik konfigurasi untuk peningkatan keamanan data pada metarouter yang sudah tereksploitasi.
- d. Bagaimana kinerja sistem dengan konfigurasi yang baik dalam menjaga keamanan data dari metarouter yang tereksploitasi.

## **1.3 Batasan Masalah**

Dalam rangka mengarahkan penelitian berdasarkan rumusan masalah yang telah dipaparkan maka perlu adanya batasan masalah sebagai berikut :

- a. Peneliti menggunakan Lingkup penelitian dibatasi pada perangkat router yang digunakan adalah mikrotik RB 951Ui-2HND dengan routerOS versi6.
- b. Penelitian memanfaatkan Metarouter yang berjalan didalam RouterOS.
- c. Digunakan simulasi kasus dengan skenario pada proses Eksploitasi Metarouter terkait serangan DOS.
- d. Penulis menggunakan aplikasi GNS3 (Graphic Network Simulator)
- e. Penelitian hanya berlingkup pada raouter mikrotik yang berjalan dalam sebuah jaringan.

## **1.4 Tujuan Penelitian**

Tujuan yang hendak dicapai pada penelitian ini yaitu :

- a. Melakukan Eksploitasi MetaRouter dalam manajemen network .
- b. Melakukan Simulasi Keamanan Data dalam sebuah manajemen network dengan menggunakan Metarouter.

- c. Mengetahui setting, Kinerja dan manfaat dari Metarouter.
- d. Mendefinisikan dan melakukan pengujian atas metode yang digunakan untuk mendapatkan solusi dalam keamanan data.

### **1.5 Manfaat Penelitian**

Berdasarkan latar belakang, rumusan masalah batasan masalah, dan tujuan dari penelitian yang telah disampaikan pada bagian sebelumnya, adapun manfaat yang ingin dicapai dalam penelitian ini yaitu :

- a. Mengetahui bagaimana setting, kinerja dan manfaat Metarouter dalam manajemen networking.
- b. Mengetahui proses keamanan data dengan metode simulasi dalam Metarouter
- c. Mengetahui Karakteristik Metarouter.
- d. Memberikan panduan dalam manajemen network dan keamanan data dengan memanfaatkan Metarouter.

### **1.6 Metode Penelitian**

Adapun langkah-langkah yang akan ditempuh selama melakukan penelitian ini yaitu sebagai berikut :

- a. Studi Literatur

Penelitian ini dilakukan dengan melakukan studi kepustakaan yaitu dengan mengumpulkan bahan-bahan referensi yang terkait dengan penelitian , baik melalui buku, artikel, paper, jurnal, makalah, dan mengunjungi beberapa situs yang terdapat pada internet terkait dengan router forensik dan mikrotik serta beberapa referensi lain yang dapat menunjang kegiatan penelitian yang dilakukan.

- b. Setting Jaringan

Pada tahapan perancangan ini peneliti memberikan perancangan terkait dengan aplikasi yang akan dibangun untuk melakukan penarikan data dari perangkat mikrotik.

- c. Pengambilan data Metarouter

Pada tahap pengambilan data metarouter peneliti menggunakan aplikasi WinBox

- d. Eksploitasi Metarouter

Pada tahapan ini melakukan pengujian pada metarouter yang telah diakses oleh user tanpa sepengetahuan oleh user bahwa menggunakan metarouter.

#### e. Konfigurasi Keamanan Data

Konfigurasi metarouter akan dimulai dari pekerjaan membuat metarouter, kemudian dilanjutkan dengan konfigurasi interface bagi setiap metarouter.

#### f. Simulasi dan Pengujian

Tahapan implementasi yang dimaksud yaitu mengimplementasikan perancangan yang telah dibuat sebelumnya menjadi aplikasi yang berjalan pada komputer, dan tahapan ini bertujuan untuk mengetahui keberhasilan dalam penarikan data dan informasi dari mikrotik serta menguji informasi yang telah berhasil ditarik lalu kemudian dilakukan analisis forensik.

#### g. Analisis

Tahapan analisis ini dilakukan terhadap informasi yang terdapat dalam mikrotik yang dapat bernilai bukti digital serta analisa penggunaan metarouter yang dapat difungsikan untuk menarik data dari mikrotik melalui tools yang dikembangkan.

#### h. Kesimpulan dan Laporan

Tahapan laporan adalah tahapan akhir yaitu penyampaian kesimpulan atas hasil dari penelitian ini.

### **1.7 Sistematika Penulisan**

Tahapan ini adalah tahapan yang memberikan gambaran secara umum terkait dengan sistematika penulisan, dengan tujuan memberikan penjelasan secara ringkas terhadap kerangka dalam penulisan.

#### **BAB I: PENDAHULUAN**

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latarbelakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, serta sistematika penulisan.

#### **BAB II: LANDASAN TEORI**

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan network dan routing.



### BAB III: ANALISIS DAN PERANCANGAN

Bab ini membahas tentang kerangka konsep penelitian dan gambaran umum langkah penyelesaian yang akan dilakukan. Bagan proses investigasi dibuat berdasarkan referensi yang didapat, untuk menyelesaikan penelitian dilakukan pembuatan rancangan simulasi untuk membuktikan bagan proses investigasi yang dikembangkan.

### BAB IV: IMPLEMENTASI

Bab ini simulasi yang sudah dirancang pada bab sebelumnya di implementasikan pada sistem yang sebenarnya. Hasil yang didapat pada tahap simulasi dianalisa kembali dan dilakukan pembahasan terkait dengan penelitian yang dibuat.

### BAB V: KESIMPULAN DAN SARAN

Tahapan ini adalah tahapan terakhir yang dilakukan dalam penelitian ini dan memuat tentang kesimpulan dari keseluruhan uraian dari Bab-bab sebelumnya, serta memberikan saran terkait dengan kekurangan yang diperoleh dalam penelitian untuk pengembangan ilmu pengetahuan di kemudian hari.

#### **1.8 Literatur Review**

Penelitian terkait manajemen jaringan telah banyak dilakukan mengingat begitu luasnya cakupan dari manajemen jaringan tersebut akan tetapi penulis memfokuskan pada pemanfaatan manajemen jaringan dengan memanfaatkan Metarouter sebagai metode yang digunakan dalam penulisan ini. Traffic engineering digunakan untuk merekayasa trafik pada suatu jaringan, sehingga semua jalur pada jaringan tersebut dapat dioptimalkan. Sedangkan fast reroute adalah suatu metode yang dapat mempercepat proses perpindahan jalur, ketika jalur utama yang dilewatkan terputus oleh (Isnanto & Diponegoro, 2017). Jenis serangan terhadap suatu komputer atau server di dalam jaringan dengan cara menghabiskan sumber daya (resources) yang dimiliki oleh komputer sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar, sehingga secara tidak langsung mencegah pengguna lain untuk dapat memperoleh akses dari layanan jaringan yang diserang disebut dengan serangan Distributed Denial of Service (DDoS) oleh (Fahri, Fiade, & Suseno, 2017) Simulasi Jaringan Virtual Local Area Network (Vlan) Menggunakan Pox Controller.

Router Mikrotik dapat menerapkan virtualisasi dengan MetaRouter yang berdampak pada penghematan biaya pembelian hardware router, penggunaan listrik, dan tempat penyimpanan. Tujuan tugas akhir ini mengimplementasikan teknik virtualisasi

router menggunakan MetaRouter. Virtualisasi router ini dibangun menggunakan metode Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIOO) Network Lifecycle. Virtualisasi router menggunakan MetaRouter dapat menghemat biaya pembuatan jaringan komputer, pemakaian energi listrik dan penggunaan tempat dibandingkan router non-virtualisasi oleh (Galang, Eko, & Imam, 2017). Penggunaan komputer tidak dapat dipantau secara detail, bisa jadi komputer tersebut di gunakan untuk hal-hal yang tidak semestinya. Oleh karna itu harus ada sebuah upaya untuk mengelola pemakaian komputer pada laboratorium salah satunya dengan menerapkan konsep firewall. Permasalahan tersebut dapat diatasi menggunakan MikroTik sebagai pengatur lalu lintas data Internet serta melakukan pemfilteran beberapa aplikasi yang dapat mengganggu konektivitas jaringan komputer sesuai dengan aturan yang disepakati sebelumnya oleh (Isnanto & Diponegoro, 2017) selain itu juga untuk melakukan simulasi jaringan pada universitas diponegoro dengan multi protocol label switching menggunakan GNS3. Penelitian sejenis juga dilakukan oleh fahri dengan membangun simulasi jaringan virtual local area network menggunakan pox controller oleh (Fahri et al., 2017).

Penelitian yang dilakukan oleh galang dengan teknik virtualisasi router menggunakan metaroter mikrotik (Galang et al., 2017). Selain itu untuk peneliti dapat melakukan penelitian tentang pemakaian simulasi jaringan multi protocol label switching dan traffic engineering menggunakan router mikrotik. Akan tetapi penulis memfokuskan pada pemanfaatan manajemen jaringan dengan memanfaatkan Metarouter sebagai metode yang digunakan dalam penulisan ini oleh (Ghozali & Indriati, 2016). (Komang, Mardiyana, Komang, & Mardiyana, 2015). ) Implementing of Virtual Router Redundancy Protocol in a Private University . Analisa Sistem Pengaman Data Jaringan Berbasis VPN (Albert & Juni, 2015). Penelitian mengenai keamanan jaringan juga dilakukan oleh (Komang et al., 2015), dengan mengamankan jaringan dengan firewall filter berbasis mikrotik pada laboratorium komputer. (Fietyata & Prayudi, 2013) Teknik Eksplorasi Bukti Digital Pada File Sharing Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer.

Teknologi virtualisasi router memungkinkan beberapa contoh router berjalan pada fisik yang sama peron. Dan dua fitur performa tinggi dan penjadwalan sumber daya fleksibel adalah tantangan utama bagi desain virtual router oleh (Gao, Zhang, Lu, & Ma, 2013). Penelitian lain tentang implementing of virtual router redundancy protocol in a private university Oleh (Soon et al., 2013). Penelitian yang dilakukan menghasilkan karakteristik 2 bukti digital. Karakteristik tersebut terdapat pada barang bukti network

traffic dan log file . Paket data yang dikirim pada network traffic disertai dengan perintah pada protokol SMB. Log file yang terdapat pada server samba merupakan file kosong dibuktikan dengan pengujian yang dilakukan, baik pada sistem yang sedang hidup maupun sistem yang ada dalam kondisi off, oleh (Fietyata & Prayudi, 2013) tentang teknik eksplorasi bukti digital pada file sharing protocol SMB untuk mendukung forensika digital pada jaringan komputer. Aplikasi router menggunakan MikroTik yang dihasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna, sehingga aplikasi tersebut tidak dapat diakses oleh pengguna sesuai dengan ketentuan yang telah dirancang dan sepakati sebelumnya. Aplikasi router menggunakan MikroTik yang dihasilkan dapat memenuhi kebutuhan sistem khususnya dalam melakukan pemfilteran aplikasi sesuai dengan kebutuhan pengguna, sehingga aplikasi tersebut tidak dapat diakses oleh pengguna sesuai dengan ketentuan yang telah dirancang dan sepakati sebelumnya oleh (Riadi, 2011). Penelitian mengenai eksploitasi juga dilakukan oleh (Xianming Gao, Xiaozhe Zhang, Zexin Lu, 2009) dengan mengeksploitasi RPC pada sistem operasi windows. Rangkuman dari literature review terhadap penelitian – penelitian yang telah dipaparkan secara singkat dapat dilihat pada Tabel 1.1 dimana akan menunjukkan perbandingan dari beberapa penelitian sebelumnya.

Tabel 1.1 Literatur Review

<b>Paper Utama</b>	<b>Metode Simulasi</b>	<b>Keamanan Data</b>	<b>Metarouter</b>	<b>Eksplorasi Metarouter</b>
(Ghozali & Indriati, 2016)	Simulasi jaringan multi protocol label switching Dan traffic engineering Menggunakan router mikrotik	-	-	-
(Isnanto & Diponegoro, 2017)	-	Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan	-	-
(Fahri et al., 2017)	Simulasi Jaringan Virtual Local Area Network (Vlan) Menggunakan Pox Controller	-	-	-
(Galang, Eko, & Imam, 2017)	-	-	Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung)	-

Lanjutan Tabel 1.2 Literatur Review

(Komang, Mardiyana, Komang, & Mardiyana, 2015)	-	Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali	-	-
(Fietyata & Prayudi, 2013)	-	-	-	Teknik Eksplorasi Bukti Digital Pada File Sharing Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer
Xianming Gao, Xiaozhe Zhang, Zexin Lu, Shicong Ma, 2013	-	-	A General Model for the Virtual Router	-
Muhammad Itqan Mazdadi, Imam Riadi, Ahmad Luthfi, 2017	-	-	Live Forensics on RouterOS using API Services to Investigate Network Attacks	-
(Soon et al., 2013)	-	-	Implementing of Virtual Router Redundancy Protocol in a Private University	-

Lanjutan Tabel 1.3 Literatur Review

(Albert & Juni, 2015)	-	Analisa Sistem Pengaman Data Jaringan Berbasis VPN	-	-
Penelitian yang diusulkan	<b>Uraian singkat masalah penelitian</b>	<b>Solusi</b>	<b>Hasil yang diharapkan</b>	
	Melakukan explorasi terhadap keamanan data yang bisa didapatkan dari Sistem Operasi Router dengan MetaRouter yang memungkinkan berjalannya beberapa RouterOs dalam sebuah Mikrotik dengan Metode simulasi	Pemanfaatan <i>Mikrotik MetaRouter</i> untuk Mendukung Aktivitas Manajemen Jaringan dan keamanan data	<ul style="list-style-type: none"> <li>- Tools yang dapat membantu proses Manajemen jaringan dan Keamanan data</li> <li>- Memberikan gambaran tahapan proses Manajemen jaringan dan keamanan data</li> <li>- Pengurangan Biaya penggunaan Router dalam sebuah jaringan</li> <li>- Terpusatnya <i>controlling traffic network</i>.</li> </ul>	

## **BAB 2**

### **Tinjauan Pustaka**

#### **2.1 Landasan Teori**

##### **2.1.1 Manajemen Jaringan**

Manajemen jaringan merupakan kemampuan untuk mengontrol dan memonitor sebuah jaringan komputer dari sebuah lokasi. The International Organization for Standardization (ISO) mendefinisikan sebuah model konseptual untuk menjelaskan fungsi manajemen jaringan. Manajemen Kesalahan (Fault Management), menyediakan fasilitas yang memungkinkan administrator jaringan untuk mengetahui kesalahan (fault) pada perangkat yang dikelola, jaringan, dan operasi jaringan, agar dapat segera menentukan apa penyebabnya dan dapat segera mengambil tindakan (perbaikan). Untuk itu, manajemen kesalahan memiliki mekanisme untuk Melaporkan terjadinya kesalahan, Mencatat laporan kesalahan (logging), Melakukan diagnosis, Mengoreksi kesalahan (dimungkinkan secara otomatis), Manajemen Konfigurasi (Configuration Management), memonitor informasi konfigurasi jaringan sehingga dampak dari perangkat keras atau pun lunak tertentu dapat dikelola dengan baik. Hal tersebut dapat dilakukan dengan kemampuan untuk inisialisasi, konfigurasi ulang, pengoperasian, dan mematikan perangkat yang dikelola.

Manajemen Performa (Performance Management), mengukur berbagai aspek dari performa jaringan termasuk pengumpulan dan analisis dari data statistik sistem sehingga dapat dikelola dan dipertahankan pada level tertentu yang dapat diterima. Untuk itu, manajemen performa memiliki kemampuan untuk Memperoleh utilisasi dan tingkat kesalahan dari perangkat jaringan, Mempertahankan performa pada level tertentu dengan memastikan perangkat memiliki kapasitas yang mencukupi. Manajemen Keamanan (Security Management), mengatur akses ke sumber daya jaringan sehingga informasi tidak dapat diperoleh tanpa izin. Hal tersebut dilakukan dengan cara membatasi akses ke sumber daya jaringan, memberi pemberitahuan akan adanya usaha pelanggaran dan pelanggaran keamanan.



Gambar 2.1 Arsitektur Manajemen Jaringan

Network Management Station (NMS), menjalankan aplikasi manajemen jaringan yang mampu mengumpulkan informasi mengenai perangkat yang dikelola dari agen manajemen yang terletak dalam perangkat. Aplikasi manajemen jaringan harus memproses data dalam jumlah yang besar, bereaksi terhadap peristiwa tertentu (event), dan mempersiapkan informasi yang relevan untuk ditampilkan. NMS biasanya memiliki console kendali dengan sebuah antarmuka GUI yang memungkinkan pengguna untuk melihat representasi grafis dari jaringan, mengontrol perangkat dalam jaringan yang dikelola, dan memprogram aplikasi manajemen jaringan. Beberapa aplikasi manajemen jaringan dapat diprogram untuk bereaksi terhadap informasi yang didapat dari agen manajemen dan/atau mengeset nilai ambang(threshold) dengan cara Melakukan tes dan koreksi otomatis (konfigurasi ulang, mematikan perangkat yang dikelola), Mencatat yang terjadi pada jaringan (logging), Memberikan informasi status dan peringatan pada pengguna. Perangkat yang dikelola, berupa semua jenis perangkat yang berada dalam jaringan, seperti komputer, printer, atau pun router. Dalam perangkat, terdapat agen manajemen. Agen manajemen, memberikan informasi mengenai perangkat yang dikelola kepada NMS dan dapat juga menerima informasi kendali/kontrol. Protokol manajemen jaringan, digunakan oleh NMS dan agen manajemen untuk bertukar informasi. Informasi manajemen, merupakan informasi yang dipertukarkan antara NMS dan agen manajemen yang memungkinkan proses monitor dan kontrol dari perangkat.

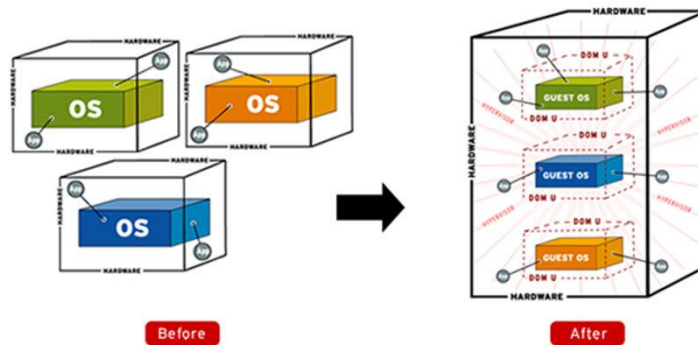
Perangkat lunak manajemen jaringan (aplikasi manajemen jaringan dan agen) biasanya berdasarkan pada protokol manajemen jaringan tertentu dan kemampuan manajemen jaringan yang diberikan oleh perangkat lunak biasanya berdasarkan pada fungsi yang didukung oleh protokol manajemen jaringan. Pemilihan perangkat lunak manajemen



jaringan ditentukan oleh Lingkungan jaringan (jangkauan dan sifat jaringan), Persyaratan manajemen jaringan, Biaya, Sistem operasi. Protokol manajemen jaringan yang paling umum digunakan adalah Simple Network Management Protocol (SNMP), Common Management Information Protocol (CMIP). SNMP merupakan protokol yang paling banyak digunakan pada lingkungan jaringan lokal (LAN). Sedangkan, CMIP digunakan pada lingkungan telekomunikasi, dimana jaringan lebih besar dan kompleks.)

### 2.1.2 Konsep Virtualisasi

Virtualisasi adalah sebuah teknik yang saat ini banyak diterapkan untuk memenuhi kebutuhan TI yang semakin tinggi namun diikuti dengan tuntutan untuk mengefisienkan biaya yang digunakan semaksimal mungkin. Virtualisasi adalah teknologi yang telah diterapkan secara luas saat ini dengan dampak peningkatan operasional dan finansial yang positif. Virtualisasi adalah konsep dimana akses ke sebuah hardware seperti server diatur sehingga beberapa operating system (guest operation system) dapat berbagi sebuah hardware. Tujuan dari virtualisasi adalah kinerja tingkat tinggi, ketersediaan, keandalan, ketangkasan, atau untuk membuat dasar keamanan dan manajemen yang terpadu. Berikut adalah gambar konsep virtualisasi:



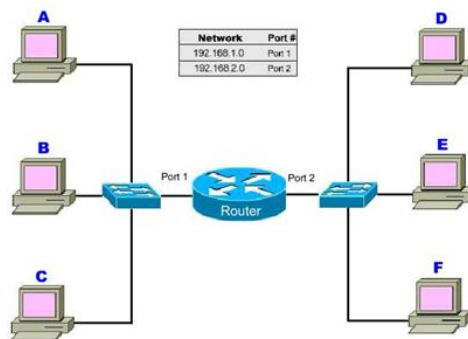
Gambar 2.2 Konsep Virtualisasi

Pada gambar 2.2 menjelaskan tentang konsep virtualisasasi pada metarouter , bahwa interface pada metarouter dapat digunakan untuk membangun hubungan dengan network yang sebenarnya. Selain itu, interface pada metarouter juga dapat digunakan untuk membangun hubungan dengan sesame metarouter lainnya.

### 2.1.3 Router

Teknologi dasar router merupakan sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang disebut routing. Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Baik network yang sama maupun berbeda dari segi teknologinya seperti menghubungkan network yang menggunakan topologi Bus, Star dan Ring. Seperti jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan internetwork, atau untuk membagi sebuah jaringan besar ke dalam beberapa subnetwork untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga merupakan sebuah perangkat jaringan yang bekerja pada OSI Layer 3, Network Layer atau perangkat komputer yang tugasnya menyampaikan paket data melewati jaringan internet hingga sampai ketujuannya. Pada layer ini juga sudah dikenal pengalamatan jaringan menggunakan IP Address, serta router ini juga berperan penting sebagai penghubung atau penerus paket data antara dua segmen jaringan/lebih.

Fungsi router yang paling utama adalah merutekan paket (informasi). Sebuah router memiliki kemampuan routing, artinya router secara cerdas dapat mengetahui kemana rute perjalanan informasi (paket) akan dilewatkan, apakah ditujukan untuk host lain yang satu network ataukah berada di network yang berbeda. Jika paket-paket ditujukan untuk host pada network lain maka router akan meneruskannya ke network tersebut. Sebaliknya, jika paket-paket ditujukan untuk host yang satu network maka router akan menghalangi paket-paket keluar. Gambar 2.1 menunjukkan contoh sebuah jaringan dengan network.



Gambar 2.3 Contoh Sebuah Jaringan dengan Network

Pada gambar 2.3 terdapat dua buah network yang terhubung dengan sebuah router. Network sebelah kiri yang terhubung ke port 1 router mempunyai alamat network 192.168.1.0 dan network sebelah kanan terhubung ke port 2 dari router dengan network address 192.155.2.0.

Komputer A mengirim data ke komputer B, maka router tidak akan meneruskan data tersebut ke network lain. 2. Begitu pula ketika komputer F mengirim data ke D, router tidak akan meneruskan paket data ke network lain. 3. Barulah ketika F mengirimkan data ke komputer B, maka router akan meneruskan paket data tersebut ke komputer B. Mikrotik adalah sistem operasi komputer dan perangkat lunak komputer yang digunakan untuk menjadikan komputer biasa menjadi router, mikrotik dibedakan menjadi dua yaitu operation sistem mikrotik bisa dikenakan mikrotik os dan mikrotik board, untuk mikrotik board tidak memerlukan komputer dalam menjalankannya cukup menggunakan board yang sudah include dengan mikrotik os. Mikrotik os mencakup fitur yang dibuat khusus untuk ip network dan jaringan wireless. Sistem operasi mikrotik, adalah sistem operasi Linux base yang digunakan sebagai network router. dibuat untuk memberikan kemudahan dan kebebasan bagi penggunaannya. Pengaturan Administrasinya dapat dilakukan menggunakan Windows Application (WinBox). Komputer yang akan dijadikan router mikrotik pun tidak memerlukan spesifikasi yang tinggi, misalnya hanya sebagai gateway. Kecuali mikrotik digunakan untuk keperluan beban yang besar (network yang kompleks, routing yang rumit) sebaiknya menggunakan spesifikasi yang cukup memadai.

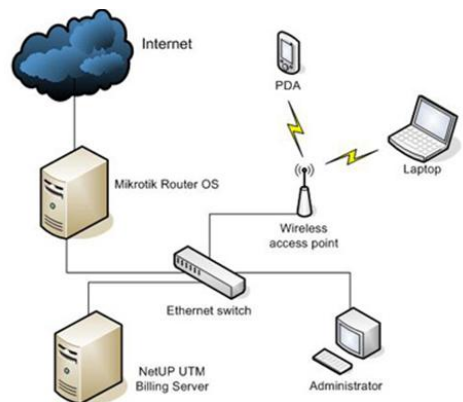
#### **2.1.4 Mikrotik Router OS**

Mikrotik adalah sebuah sistem operasi termasuk di dalamnya perangkat lunak yang dipasang pada suatu komputer sehingga komputer tersebut dapat berperan sebagai jantung network, pengendali atau pengatur lalu-lintas data antar jaringan, komputer jenis ini dikenal dengan nama router. Jadi intinya mikrotik adalah salah satu sistem operasi khusus untuk router. Mikrotik dikenal sebagai salah satu Router OS yang handal dan memiliki banyak sekali fitur untuk mendukung kelancaran network. Router Mikrotik bisa digunakan pada jaringan komputer berskala kecil atau besar, hal ini tentunya disesuaikan pada resource daripada komputer itu sendiri. Jika mikrotik digunakan untuk mengatur network kecil maka penggunaan perangkat komputernya bisa yang biasa-biasa saja, namun jika yang

ditanganinya adalah jaringan berskala besar seperti kelas ISP maka penggunaan perangkat komputernya pun harus yang benar-benar handal yang memiliki spesifikasi tinggi.

MikroTik RouterOS adalah sistem operasi perangkat keras MikroTik Routerboard. Hal ini juga dapat diinstal pada PC dan akan mengubahnya menjadi router dengan semua fitur yang diperlukan - routing, firewall, manajemen bandwidth, jalur akses nirkabel, link backhaul, gateway hotspot, server VPN dan banyak lagi. RouterOS mendukung berbagai metode konfigurasi - akses lokal dengan keyboard dan monitor, konsol serial dengan aplikasi terminal, akses Telnet dan SSH yang aman melalui jaringan, alat konfigurasi GUI kustom yang disebut Winbox, antarmuka konfigurasi berbasis Web sederhana dan antarmuka pemrograman API untuk bangunan aplikasi kontrol Anda sendiri. Jika tidak ada akses lokal, dan ada masalah dengan komunikasi tingkat IP, RouterOS juga mendukung koneksi berbasis tingkat MAC dengan alat Mac-Telnet dan Winbox yang dibuat khusus. RouterOS memiliki antarmuka konfigurasi command-line yang kuat namun mudah dipelajari dengan kemampuan scripting yang terintegrasi.

1. Winbox GUI over IP dan MAC
2. CLI dengan Telnet, SSH, konsol lokal dan konsol serial
3. API untuk memprogram alat Anda sendiri
4. Antarmuka web



Gambar 2.4 Penggunaan Mikrotik RouterOS

Pada gambar 2.4 menjelaskan bahwa Sebuah fasilitas untuk menghubungkan diri ke internet secara bersama-sama dan harus dapat memenuhi permintaan user untuk layanan Internet (http, FTP, Telnet) dan mengirimkannya sesuai dengan kebijakan. Bekerja sebagai gateway menuju layanan. Mewakili akses paket data dari dalam dan dari luar.

### 2.1.5 MetaRouter

Metarouter merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru secara virtual. Hampir sama seperti aplikasi VMware atau VirtualPC pada Windows. Metarouter bisa digunakan untuk menjalankan Operating System didalam OS MikroTik yang sedang berjalan. Dengan menggunakan Metarouter, client seolah-olah memiliki router sendiri. Dan sebagai admin, tetap bisa memmanagement router fisik. Sebelum membuat sebuah virtual machine, perlu tentukan terlebih dahulu besar RAM dan Hardisk yang akan dialokasikan untuk virtual router. Dengan Operating System Mikrotik, minimal RAM yang disarankan adalah 24MB. Untuk ukuran Hardisk bisa disesuaikan dengan kebutuhan. Jika parameter tadi sudah ditentukan maka saatnya jalankan virtualisasi di router MikroTik dengan fitur Metarouter. Metarouter adalah yang paling mudah digunakan, meskipun hanya bisa menjalankan virtualisasi topologi jaringan, RouterOS dan OpenWRT.

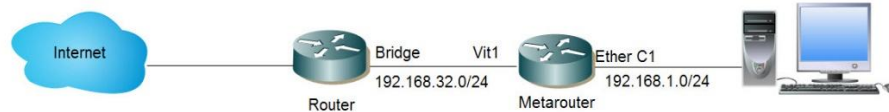
Metarouter memiliki beberapa keterbatasan seperti berikut :

1. Hanya bisa menjalankan sampai dengan 8 (delapan) mesin virtual untuk setiap Routerboard.
2. Tidak dapat menggunakan CF maupun MicroSD
3. Terkadang OpenWRT tidak ter-shutdown dengan sempurna pada saat
4. RouterOS mengalami Reboot.
5. RouterOS virtual tidak bisa menggunakan interface wireless yang dimiliki oleh RouterBoard.

Manfaat Virtualisasi Router Menggunakan Meta Router :

1. Virtualisasi dapat diterapkan untuk membangun beberapa RouterOS virtual.
2. Virtualisasi dapat diterapkan untuk membangun server virtual, seperti Web
3. Server, FTP Server, DNS Server, Database Server, VoIP Server, Proxy Server dan lain-lain.
4. Virtualisasi dapat diterapkan untuk membangun topologi jaringan.
5. Virtualisasi dengan Metarouter tidak akan membebani PC atau Laptop Anda, ini karena Metarouter dijalankan pada Routerboard.
6. Virtualisasi akan lebih ringkas dan kompak karena dapat dikemas dalam sebuah casing Routerboard. Ini membawa keuntungan karena jaringan

7. virtual Anda dapat dengan mudah dibawa maupun dipinjamkan keteman Anda. Sangat berguna bagi para trainer atau instruktur yang sering melakukan pelatihan maupun presentasi di tempat yang berbeda-beda.
8. Lebih hemat listrik, karena hanya membutuhkan catuan sebuah RouterBoard untuk mendapatkan 8 (delapan) unit RouterOS
9. Sistem operasi yang digunakan oleh RouterOS virtual adalah sistem operasi yang legal.



Gambar 2.5 Pemanfaatan Metarouter

Pada gambar 2.5 menjelaskan tentang pemanfaatan pada metarouter mengakses metarouter melalui console untuk melakukan konfigurasi dengan menggunakan bridge dan Ethernet.

### 2.1.6 Keamanan Data

Data-data yang dikirimkan melalui jaringan internet sebagian adalah data-data penting. Hal ini mengundang pihak lain untuk mencuri dan memanfaatkan data-data tersebut untuk kepentingan pribadinya. Tentu saja akan merugikan pemilik data. Pencurian dan pemanfaatan data-data oleh orang yang tidak berhak merupakan sebuah kejahatan. Internet sangat berperan penting dalam kehidupan manusia saat ini. Banyak aktivitas yang dilakukan dengan memanfaatkan internet. Data-data tersebut dikirim dari komputer user ke komputer server penyedia layanan yang digunakan. Sebelum sampai di komputer server penyedia jasa layanan, data-data yang dikirimkan akan melewati komputer-komputer yang ada di jaringan internet. Pada saat melewati jaringan internet, data-data yang dikirimkan rawan terhadap penyadapan. Selain penyadapan. Komputer yang digunakan bisa saja terjangkit oleh virus yang bekerja sebagai spyware. Dimana spyware dapat merekam semu aktivitas yang dilakukan. Jika seseorang dapat menyusup ke sebuah komputer maka orang tersebut dapat mengambil data-data yang disimpan di komputer tersebut dan menggunakannya untuk keuntungan pribadi. Keamanan data menjadi hal penting dalam komunikasi data yang dilakukan. Bila data user ID dan password dari layanan yang gunakan jatuh ke tangan orang yang salah, bisa saja orang tersebut akan memanfaatkan untuk hal-hal yang tidak bertanggung jawab.

Berdasarkan hasil penelitian, tidak ada jaringan komputer yang benar-benar aman dari serangan hacker, cracker, spam, e-mail bomb, virus komputer dsb. Yang dapat dilakukan adalah menjaga jangan sampai jaringan tersebut mudah ditembus, sambil terus berusaha meningkatkan sistem keamanan data dan jaringan. Pada era global sekarang ini, keamanan sistem informasi berbasis internet menjadi suatu keharusan untuk lebih diperhatikan, karena jaringan internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu komputer ke komputer lain di dalam internet, data itu akan melewati sejumlah komputer yang lain. Berarti akan memberi kesempatan pada user untuk mengambil alih suatu atau beberapa komputer. Kecuali suatu komputer terkunci dalam suatu ruangan yang mempunyai akses terbatas ke luar dari ruangan itu, maka komputer tersebut akan aman. Pembobolan sistem keamanan di Internet terjadi hampir setiap hari diseluruh dunia. Kejahatan Cyber atau lebih dikenal Cyber Crime adalah suatu bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung ke Internet dan mengeksploitasi komputer lain yang terhubung juga pada Internet. Adanya lubang-lubang pada system operasi menyebabkan kelemahan dan terbukanya lubang yang dapat digunakan para hacker, cracker dan Script kiddies untuk menyusup ke dalam komputer tersebut. Kejahatan yang terjadi dapat berupa Pencurian terhadap data, Akses terhadap jaringan internal, Perubahan terhadap data-data penting Pencurian informasi dan berujung pada penjualan informasi.

### **2.1.7 WINBOX 3.11**

Winbox adalah sebuah software atau utility yang di gunakan untuk meremote sebuah server mikrotik kedalam mode GUI (Graphical User Interface) melalui operating system windows. Orang-orang lebih banyak mengkonfigurasi mikrotik atau mikrotik routerboard menggunakan winbox di banding dengan yang mengkonfigurasi langsung lewat mode CLI (Command Line Interface). Itu di sebabkan, tidak lain karena pengerjaannya yang lebih simple & mudah dan dengan menggunakan software winbox ini penyettingan sebuah server dapat diselesaikan dengan cepat di banding dengan yang megunakan mode CLI yang harus menghafal dan mengetikan perintah printah console mikrotik.

Untuk konfigurasi penggunaan Winbox harian Router Mikrotik sebaiknya menggunakan IP-Address. Karena konfigurasi menggunakan IP-Address akan lebih stabil

dengan menggunakan protocol TCP. Untuk melakukan konfigurasi kadang sering tanpa sengaja atau karena mencoba suatu fitur sehingga dapat melakukan kesalahan setting yang mengakibatkan winbox putus dan Router tidak bisa diakses. Dengan kata lain konfigurasi yang tambahan mengganggu kinerja router yang sedang berjalan. Dalam hal ini dapat meminimalkan kesalahan konfigurasi, maka dapat menggunakan tombol "Safe Mode". Selain itu Dashboard winbox dapat digunakan untuk menampilkan beberapa informasi yaitu Time, Date, CPU load, memory, dan Uptime. Dengan adanya informasi yang tertampil langsung di dashboard akan lebih memudahkan dalam mengontrol atau monitoring Router saat melakukan remote winbox.

Fungsi utama winbox adalah untuk setting yang ada pada mikrotik, berarti tugas utama winbox adalah untuk menyetting atau mengatur mikrotik dengan GUI, atau tampilan desktop

fungsi winbox lebih rinci adalah :

1. Setting mikrotik router
2. Setting Limit Bandwidth jaringan
3. untuk setting blokir sebuah situs
4. Setting Login Hotspot
5. Setting pengamanan jaringan

Secara *default*, terdapat beberapa fitur yang dapat Anda temukan di Winbox, Antara lain:

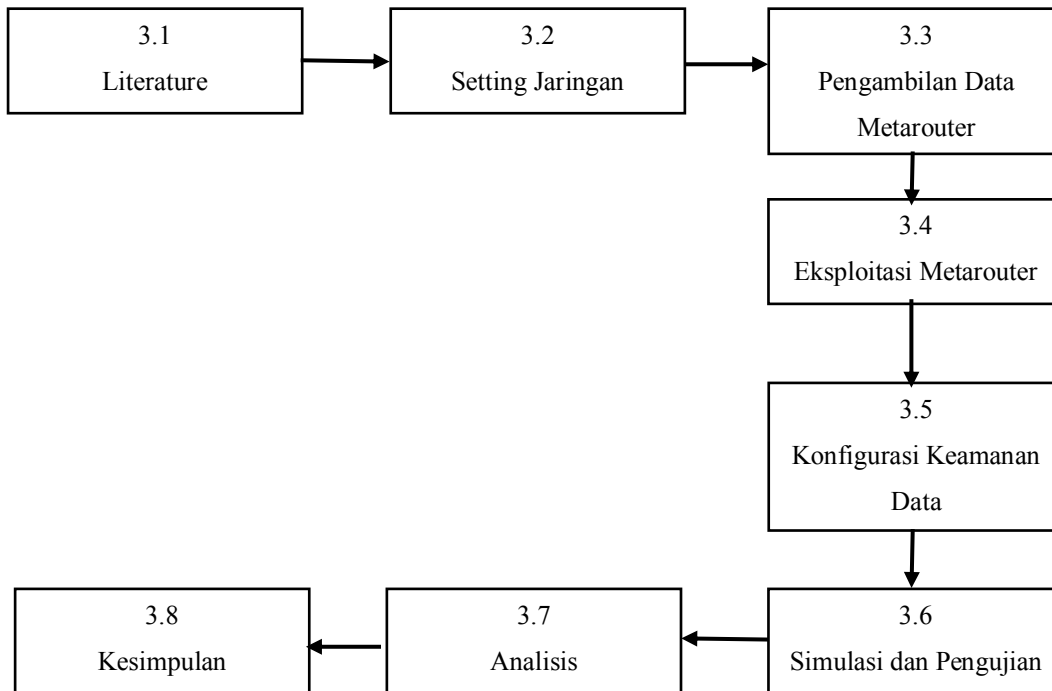
1. **Connect Button**, tombol *Connect* merupakan akses untuk *log on* ke router dengan menggunakan IP yang sudah ditentukan sebelumnya. Modifikasi *MAC address*, nama pengguna dan *password*.
2. **Save Button**, berfungsi sebagai perintah penyimpanan semua sesi ke dalam *list*, sehingga nantinya dapat dijalankan dengan mudah hanya dengan klik dua kali ke salah satu daftar.
3. **Remove**, untuk menghapus item yang sudah disimpan atau dipilih dari list.
4. **Tools**, terdapat beberapa pengaturan yang dapat dilakukan pada *menu* Tools antara lain; menghapus *cache*, *import* alamat dari *file*, ekspor file dan menghapus seluruh *item* yang ada pada daftar.
5. **Secure Mode**, secure mode merupakan jenis hubungan dengan tingkat keamanan yang relatif lebih ketat karena sistem akan menyediakan protokol yang bersifat *privacy* antar router.



## BAB 3

### Metode Penelitian

Studi pustaka merupakan kegiatan untuk mengkaji dan mempelajari berbagai sumber literatur dan teori-teori yang mendukung tentang penelitian yang dilakukan. Sumber pembelajaran pada studi pustaka dapat bersumber dari jurnal, paper, artikel, buku-buku, website, dan sumber pembelajaran lainnya yang membahas berkaitan tentang Network Forensik, Router Forensik, Mikrotik, RouterOS, dan MetaRouter. Pada tahap ini akan dilakukan pula pembuatan proposal penelitian. Berikut tahapan – tahapan yang akan dilakukan dalam penelitian ini:



Gambar 3.1 Flowchart Penelitian Metarouter

#### 3.1 Literature

Untuk mendukung impementasi dalam penelitian ini diperlukan adanya perangkat keras dan perangkat lunak sebagai alat dan bahan penelitian.

### 3.1.1 Hardware

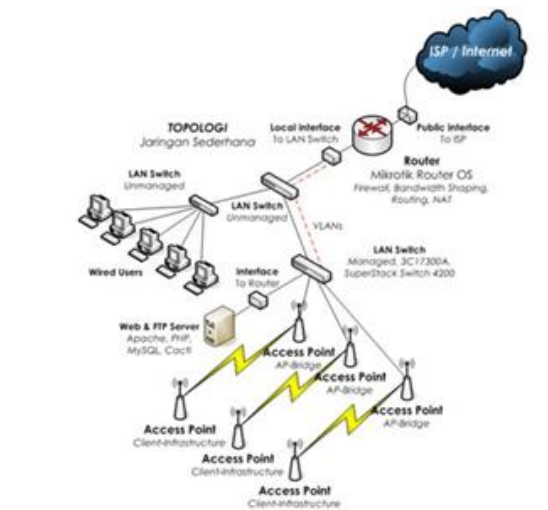
1. Mikrotik RB951Ui dengan RouterOS versi 6
2. Access Point TP-Link MR3020 atau Switch TP-Link
3. Modem ADSL sebagai sumber koneksi internet
4. Laptop Core i5, RAM 4GB sebagai Komputer untuk melakukan penarikan data dan analisa
5. Smartphone dan laptop sebagai client jaringan

### 3.1.2 Software

1. Mikrotik RouterOS versi 6
2. Winbox v3.11
3. Apache Server for Windows 2.4.9
4. Microsoft Windows 10

## 3.2 Setting Jaringan

Dalam penerapan simulasi kondisi jaringan untuk pada penelitian ini maka perlu dilakukan perancangan topologi jaringan, Adapun topologi yang diterapkan pada penelitian ini.



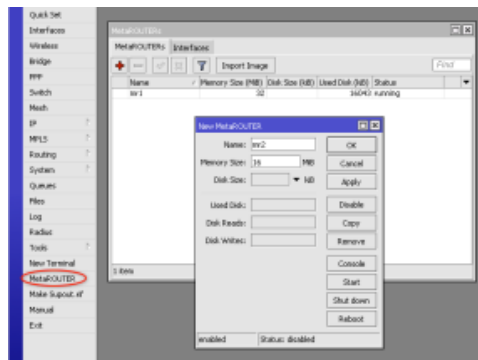
Gambar 3.2 Topologi Jaringan

Pada Gambar 3.2 menjelaskan tentang topologi jaringan, topologi ini adalah topologi umum yang biasa digunakan pada pengguna home maupun small office. Sumber internet yang digunakan adalah ISP yang menggunakan modem ADSL sebagai Public Interface. Komunikasi data dari Modem ADSL diteruskan ke router mikrotik yang bertugas untuk

mengatur lalu lintas jaringan serta pengaturan bandwidth. Agar pc client terhubung ke jaringan diperlukan sebuah switch yang bertugas menghubungkan PC client ke jaringan dan penghubung dari lalu lintas data yang dialirkan dari router. Adapun selain switch juga bisa digunakan Access Point yang berfungsi untuk menghubungkan jaringan tanpa kabel/nirkabel. Dengan penambahan AP (Access Point) atau yang biasa disebut WiFi memungkinkan smartphone dan laptop untuk juga terhubung pada jaringan sebagai client dalam simulasi ini

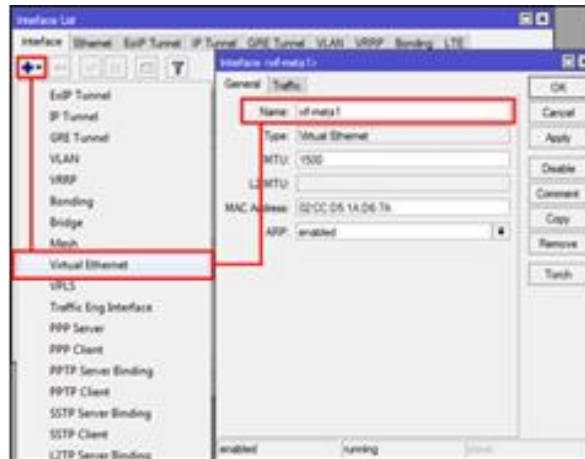
### 3.3 Pengambilan data metarouter

Tahapan ini merupakan perancangan sistem setting Meta Router yang digunakan sebagai pengambilan data. Pertama, masuk ke menu MetaROUTER. Klik tombol + untuk menambahkan virtual router. Disini ada 3 parameter yang perlu ditentukan, "Name" diisi dengan nama Virtual Router sesuai kebutuhan Anda. Kemudian Parameter RAM dan Hardisk juga diisi sesuai kebutuhan. Parameter lainnya bisa dibiarkan bernilai default.



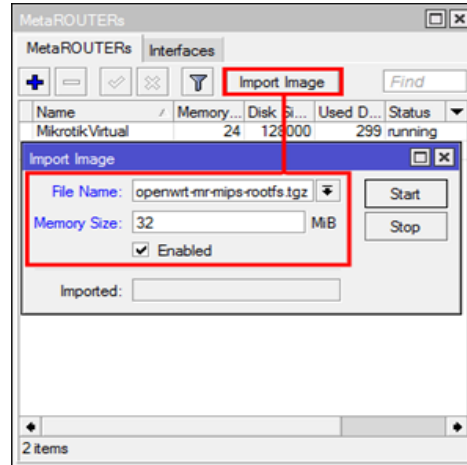
Gambar 3.3 Metarouter Setting New

Pada Gambar 3.3 Menjelaskan tentang Setting metarouter , operating System secara otomatis akan menggunakan RouterOS Mikrotik dan versi yang dijalankan sama dengan versi RouterOS Router Mikrotik. Virtual Router ini belum memiliki interface ethernet, dan belum bisa berkomunikasi secara network dengan perangkat lain, maka perlu diinstalasi virtual Ethernet yang akan digambarkan pada Gambar 3.3. Cara mudah untuk mengakses metarouter adalah melalui interface console. Cara mensetting seperti ini dapat dilakukan dengan membuka terlebih dahulu menu metarouter, kemudian baru menggunakan winbox dan menjalankan console. Maka setting metarouter melalui winbox bisa dilakukan dengan baik sesuai pada Gambar 3.3 diatas.



Gambar 3.4 Virtual Ethernet Instalasi

Pada Gambar 3.4 menjelaskan tentang virtual Ethernet instalasi, selain Menggunakan Virtual Ethernet yang instalasi sendiri disini peneliti juga kan menerapkan menjalankan OS lain secara virtual, misalnya OpenWRT. Namun tidak sembarang image bisa digunakan untuk Metarouter, Jika Anda familiar dengan compiling di linux, Anda bisa compile OS sesuai dengan platform mikrotik. Jika Anda belum familiar, Anda bisa menggunakan prebuilt OpenWRT image yang sudah disediakan oleh mikrotik berupa MIPS image untuk RouterBoard dengan platform Mipsbe, dan PPC image untuk RouterBoard dengan platform PowerPC. Sedikit berbeda dengan membuat virtual router dengan Mikrotik OS, untuk OpenWRT, harus upload terlebih dahulu image OpenWRT ke router, kemudian import di Metarouter. Seperti pada gambar 3.4. Pada tahapan virtualisasi yang kita lakukan, Disini kita akan membuat dua buah virtual ethernet. Satu virtual ether yang akan digunakan oleh virtual router untuk dapat berkomunikasi dengan Router Master, dan satu lagi virtual ethernet untuk komunikasi virtual router dengan host dalam sebuah jaringan komputer, misalnya laptop client. Jika sudah, kita mendefinisikan virtual ethernet ke dalam virtual router supaya dapat digunakan oleh virtual router. Masuk ke menu MetaROUTER, kemudian klik tab "Inteface". Klik Tombol + (add). Supaya dalam melakukan settingan metarouter kita tidak bingung membedakan mana yang router fisik dan mana yang virtual, kita bisa set *System Identity* masing - masing router. Karena virtual router belum memiliki interface, langkah selanjutnya yang perlu kita lakukan adalah membuat virtual ethernet.



Gambar 3.5 Instalasi OS dalam Metarouter

Pada Gambar 3.5 menjelaskan Instalasi OS dalam metarouter , Virtual ethernet ini yang nanti akan digunakan oleh virtual router untuk Import Image dapat berkomunikasi dengan router master atau bahkan device lain dalam jaringan.

### 3.4 Eksploitasi Metarouter

Keamanan jaringan menjadi semakin penting dengan semakin banyaknya waktu yang dihabiskan orang untuk berhubungan. Mengganggu keamanan jaringan sering lebih mudah daripada fisik atau lokal, dan lebih umum. Celah-celah keamanan jaringan sering digunakan untuk menjebol suatu sistem dibawah ini beberapa Eksploitasi yang dilakukan untuk masuk dalam keamanan suatu sistem.

Anatomi Suatu Serangan Hacking

#### 3.4.1 Footprinting

Mencari rincian informasi terhadap sistem-sistem untuk dijadikan sasaran, mencakup pencarian informasi dengan search engine, whois, dan DNS zone transfer.

hacker baru mencari-cari sistem mana yang dapat disusupi. Footprinting merupakan kegiatan pencarian data berupa:

- Menentukan ruang lingkup (scope) aktivitas atau serangan
- Network enumeration
- Interogasi DNS
- Mengintai jaringan

Semua kegiatan ini dapat dilakukan dengan tools dan informasi yang tersedia bebas di Internet. Kegiatan footprinting ini diibaratkan mencari informasi yang tersedia umum melalui buku telepon. Tools yang tersedia untuk ini di antaranya:

- Teleport Pro: Dalam menentukan ruang lingkup, hacker dapat men-download keseluruhan situs-situs web yang potensial dijadikan sasaran untuk dipelajari alamat, nomor telepon, contact person, dan lain sebagainya.
- Whois for 95/9/NT: Mencari informasi mengenai pendaftaran domain yang digunakan suatu organisasi. Di sini ada bahaya laten pencurian domain (domain hijack).
- NSLookup: Mencari hubungan antara domain name dengan IP address.
- Traceroute 0.2: Memetakan topologi jaringan, baik yang menuju sasaran maupun konfigurasi internet jaringan sasaran.

### **3.4.2 Scanning**

Terhadap sasaran tertentu dicari pintu masuk yang paling mungkin. Digunakan ping sweep dan portscan.

### **3.4.3 Enumeration**

Telaah intensif terhadap sasaran, yang mencari user account absah, network resource and share, dan aplikasi untuk mendapatkan mana yang proteksinya lemah.

enumerasi sudah bersifat sangat intrusif terhadap suatu sistem. Di sini penyusup mencari account name yang absah, password, serta share resources yang ada. Pada tahap ini, khusus untuk sistem-sistem Windows, terdapat port 139 (NetBIOS session service) yang terbuka untuk resource sharing antar-pemakai dalam jaringan. Anda mungkin berpikir bahwa hard disk yang di-share itu hanya dapat dilihat oleh pemakai dalam LAN saja. Kenyataannya tidak demikian. NetBIOS session service dapat dilihat oleh siapa pun yang terhubung ke Internet di seluruh dunia! Tools seperti Legion, SMBScanner, atau SharesFinder membuat akses ke komputer orang menjadi begitu mudah (karena pemiliknya lengah membuka resource share tanpa password).

### **3.4.4 Gaining Access**

Mendapatkan data lebih banyak lagi untuk mulai mencoba mengakses sasaran. Meliputi mengintip dan merampas password, menebak password, serta melakukan buffer overflow.

gaining access adalah mencoba mendapatkan akses ke dalam suatu sistem sebagai user biasa. Ini adalah kelanjutan dari kegiatan enumerasi, sehingga biasanya di sini penyerang sudah mempunyai paling tidak user account yang absah, dan tinggal mencari passwordnya saja. Bila resource share-nya diproteksi dengan password, maka password ini dapat saja ditebak (karena banyak yang menggunakan password sederhana dalam melindungi komputernya). Menebaknya dapat secara otomatis melalui dictionary attack (mencobakan kata-kata dari kamus sebagai password) atau brute-force attack (mencobakan kombinasi semua karakter sebagai password). Dari sini penyerang mungkin akan berhasil memperoleh logon sebagai user yang absah.

#### **3.4.5 Escalating Privilege**

Bila baru mendapatkan user password di tahap sebelumnya, di tahap ini diusahakan mendapat privilege admin jaringan dengan password cracking atau exploit sejenis getadmin, sechole, atau lc\_messages. Escalating Privilege mengasumsikan bahwa penyerang sudah mendapatkan logon access pada sistem sebagai user biasa. Penyerang kini berusaha naik kelas menjadi admin (pada sistem Windows) atau menjadi root (pada sistem Unix/Linux). Teknik yang digunakan sudah tidak lagi dictionary attack atau brute-force attack yang memakan waktu itu, melainkan mencuri password file yang tersimpan dalam sistem dan memanfaatkan kelemahan sistem. Pada sistem Windows 9x/ME password disimpan dalam file .PWL sedangkan pada Windows NT/2000 dalam file .SAM.

#### **3.4.6 Pilfering**

Proses pengumpulan informasi dimulai lagi untuk mengidentifikasi mekanisme untuk mendapatkan akses ke trusted system. Mencakup evaluasi trust dan pencarian *cleartext password* di *registry*, *config file*, dan *user data*.

#### **3.4.7 Covering Track**

Begitu kontrol penuh terhadap sistem diperoleh, maka menutup jejak menjadi prioritas. Meliputi membersihkan network log dan penggunaan hide tool seperti macam-macam rootkit dan file streaming.

penyerang sudah berada dan menguasai suatu sistem dan kini berusaha untuk mencari informasi lanjutan (*pilfering*), menutupi jejak penyusupannya (*covering tracks*), dan

menyiapkan pintu belakang (creating backdoor) agar lain kali dapat dengan mudah masuk lagi ke dalam sistem. Adanya Trojan pada suatu sistem berarti suatu sistem dapat dengan mudah dimasuki penyerang tanpa harus bersusah payah melalui tahapan-tahapan di atas, hanya karena kecerobohan pemakai komputer itu sendiri.

#### **3.4.8 Creating Backdoors**

Pintu belakang diciptakan pada berbagai bagian dari sistem untuk memudahkan masuk kembali ke sistem ini dengan cara membentuk user account palsu, menjadwalkan batch job, mengubah startup file, menanamkan servis pengendali jarak jauh serta monitoring tool, dan menggantikan aplikasi dengan trojan.

#### **3.4.9 Denial Of Service**

Bila semua usaha di atas gagal, penyerang dapat melumpuhkan sasaran sebagai usaha terakhir. Meliputi SYN flood, teknik-teknik ICMP, *Supernuke*, *land/latierra*, *teardrop*, *bonk*, *newtear*, *trincoo*, *smurf*, dan lain-lain.

kalau penyerang sudah frustrasi tidak dapat masuk ke dalam sistem yang kuat pertahanannya, maka yang dapat dilakukannya adalah melumpuhkan saja sistem itu dengan menyerangnya menggunakan paket-paket data yang bertubi-tubi sampai sistem itu *crash*. *Denial of service attack* sangat sulit dicegah, sebab memakan habis *bandwidth* yang digunakan untuk suatu situs. Pencegahannya harus melibatkan ISP yang bersangkutan. Para *script kiddies* yang pengetahuan hacking-nya terbatas justru paling gemar melakukan kegiatan yang sudah digolongkan tindakan kriminal di beberapa negara ini.

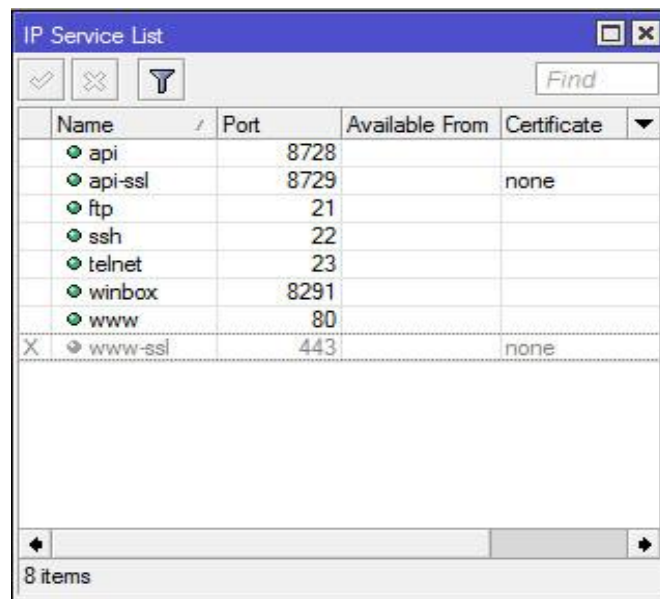
### **3.5 Konfigurasi Keamanan Data**

Setelah selesai dengan setting fitur yang dibutuhkan, terkadang admin jaringan mengabaikan sisi keamanan router. Hal ini akan sangat riskan akan terjadinya serangan terhadap router, terlebih ketika router langsung terkoneksi ke internet dan memiliki ip public. Namun jangan salah, serangan terhadap router tidak selalu berasal dari jaringan internet, bisa juga berasal dari jaringan lokal. akan coba bahas langkah pertama yang perlu dilakukan untuk menjaga router dari orang yang tidak bertanggung jawab.



### 3.5.1 Services

Router Mikrotik menjalankan beberapa service untuk memudahkan cara user dalam mengakses router, atau menggunakan fitur lainnya. *Service* ini *by-default* akan dijalankan oleh router terus menerus. bisa cek service yang dijalankan oleh mikrotik di menu IP --> *Services*. Setelah selesai dengan setting fitur yang dibutuhkan, terkadang admin jaringan mengabaikan sisi keamanan router. Dalam hal ini akan sangat riskan terjadinya serangan terhadap router, terlebih ketika router langsung terkoneksi ke internet dan memiliki ip public. Namun jangan salah, serangan terhadap router tidak selalu berasal dari jaringan internet, bisa juga berasal dari jaringan lokal. akan coba bahas *services* langkah pertama yang perlu dilakukan untuk menjaga router dari orang yang tidak bertanggung jawab.



Name	Port	Available From	Certificate
api	8728		
api-ssl	8729		none
ftp	21		
ssh	22		
telnet	23		
winbox	8291		
www	80		
X www-ssl	443		none

Gambar 3.6 Service list

Pada Gambar 3.6 menjelaskan kondisi IP Service pada settingan winbox. Ada beberapa service yang secara default dijalankan oleh router mikrotik. Berikut detail informasi service router MikroTik dan kegunaannya :

1. **API** : Application Programmable Interface, sebuah service yang memungkinkan user membuat custom software atau aplikasi yang berkomunikasi dengan router, misal

untuk mengambil informasi didalam router, atau bahkan melakukan konfigurasi terhadap router. Menggunakan port 8728.

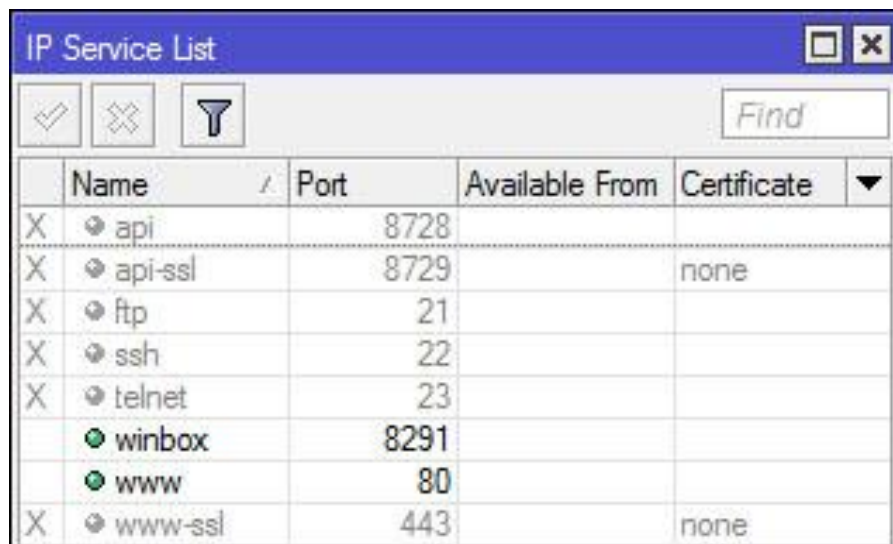
2. **API-SSL** : Memiliki fungsi yang sama sama seperti API, hanya saja untuk API SSL lebih secure karena dilengkapi dengan ssl certificate. API SSL ini berjalan dengan menggunakan port 8729.
3. **FTP** : Mikrotik menyediakan standart service FTP yang menggunakan port 20 dan 21. FTP biasa digunakan untuk upload atau download data router, misal file backup. Authorisasi FTP menggunakan user & password account router.
4. **SSH** : Merupakan salah satu cara remote router secara console dengan secure. Hampir sama seperti telnet, hanya saja bersifat lebih secure karena data yang ditransmisikan oleh SSH dienskripsi. SSH MikroTik by default menggunakan port 22.
5. **Telnet** : Memiliki fungsi yang hampir sama dengan ssh hanya saja memiliki beberapa keterbatasan dan tingkat keamanan yang rendah. Biasa digunakan untuk remote router secara console. Service telnet MikroTik menggunakan port 23.
6. **Winbox** : Service yang mengijinkan koneksi aplikasi winbox ke router. Tentu sudah tidak asing dengan aplikasi winbox yang biasa digunakan untuk meremote router secara grafik. Koneksi winbox menggunakan port 8291.
7. **WWW** : Selain remote console dan winbox, mikrotik juga menyediakan cara akses router via web-base dengan menggunakan browser. Port yang digunakan adalah standart port HTTP, yaitu port 80.
8. **WWW-SSL** : Sama seperti service WWW yang mengijinkan akses router menggunakan web-base, akan tetapi www-ssl ini lebih secure karena menggunakan certificaes ssl untuk membangun koneksi antara router dengan client yang akan melakukan remote. By default menggunakan port 443.

Selanjutnya adalah pertanyaan bagi administrator jaringan, apakah kemudian semua service tersebut akan digunakan ?. Terkadang admin jaringan tidak terlalu peduli, service tetap berjalan padahal tidak dibutuhkan, sehingga service ini bisa dimanfaatkan oleh orang yang tidak bertanggung jawab setiap saat. Pernahkah Anda membuka terminal router MikroTik kemudian muncul pemberitahuan "failure for user root from xx.xx.x.xxx via ssh" ? Error tersebut menginformasikan bahwa ada

user yang mencoba mengakses router dengan menebak username dan password router.

### 3.5.2 Disable Service

Untuk meminimalisasi user mencoba mengakses router menggunakan service tertentu, administrator jaringan bisa mematikan service yang dirasa tidak digunakan. Misal hanya butuh mengakses router via winbox dan web-base, maka bisa matikan service selain dua service tadi.



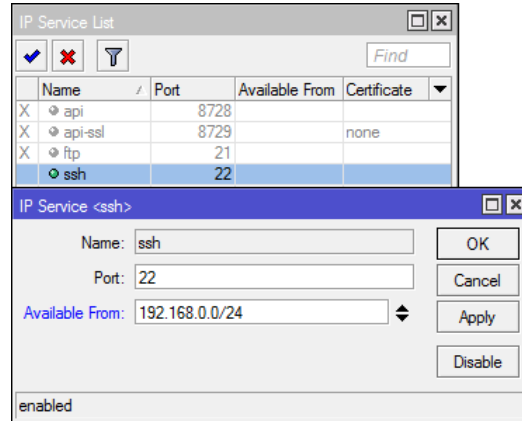
	Name	Port	Available From	Certificate
X	api	8728		
X	api-ssl	8729		none
X	ftp	21		
X	ssh	22		
X	telnet	23		
	winbox	8291		
	www	80		
X	www-ssl	443		none

Gambar 3.7 Disable list

Pada Gambar 3.7 Menjelaskan settingan winbox pada metarouter yaitu pada port winbox 8291 dan menjelaskan tentang port 80 pada settingan winbox.

### 3.5.3 Available From

Administrator jaringan bisa membatasi dari jaringan mana router bisa diakses pada service tertentu dengan menentukan parameter "Available From" pada setting service. dengan menentukan "Available From", maka service hanya bisa diakses dari jaringan yang sudah ditentukan. Ketika ada yang mencoba mengakses router dari jaringan diluar allowed-address, secara otomatis akan ditolak oleh router. Parameter "Available From" bisa diisi dengan IP address ataupun network address.

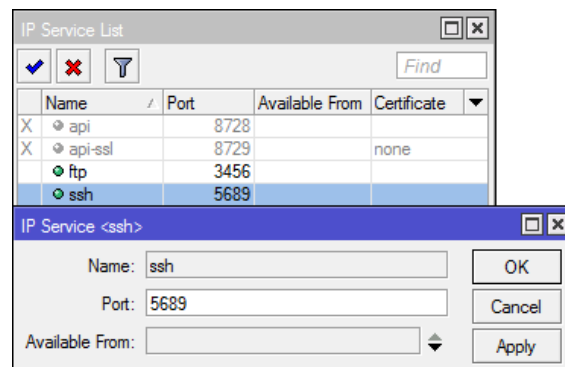


Gambar 3.8 Available Form

Pada Gambar 3.8 Menjelaskan settingan pada winbox IP Service List pada port 22 atau ssh, bahwa port 22 ini available fromnya 192.168.0.0/24.

### 3.5.4 Ubah Port

Selain menentukan *allowed address*, administrator jaringan juga bisa mengubah port yang digunakan oleh service tertentu. Seseorang yang berkecimpung di dunia jaringan bisa menebak dengan mudah port default yang biasa digunakan oleh *service - service* tertentu.



Gambar 3.9 Ubah Port

Pada Gambar 3.9 menjelaskan IP Service List bahwa ftp dengan port 3456, ssh dengan port 5689 dengan nama ssh dan port 5659.

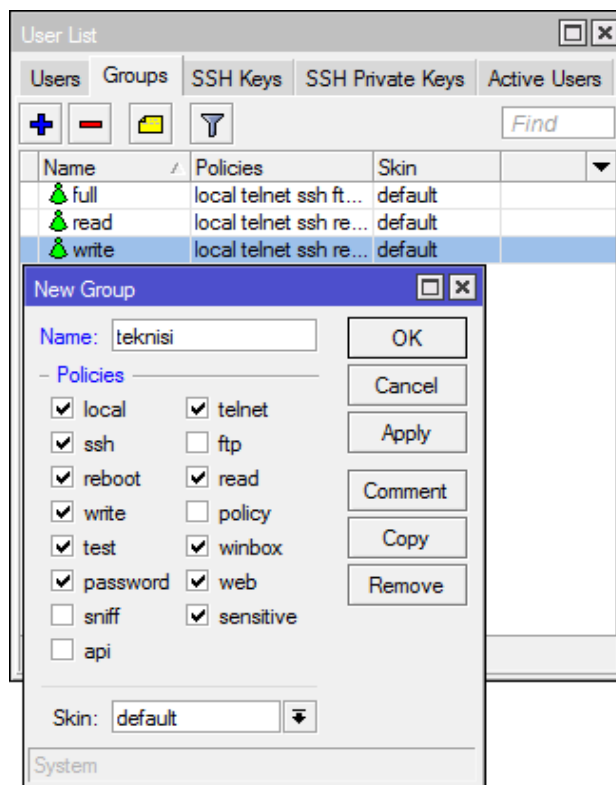
### 3.5.5 Management User

Beberapa administrator kadang berpikir bahwa dengan memberi password saja sudah cukup. Kemudian men-share username dan password ke beberapa rekan teknisi, bahkan untuk teknisi yang hanya memiliki akses monitoring router juga diberikan hak akses admin. Hal

ini tentu akan sangat riskan ketika router yang dihandle merupakan router penting. Berikut beberapa tips management user yang bijak.

### 3.5.6 Group Policies

Teknisi yang hanya memiliki tanggung jawab monitoring jaringan tidak membutuhkan hak akses full terhadap router. Biasanya hak akses full hanya dimiliki oleh orang yang paling tahu terhadap kondisi dan konfigurasi router. Admin jaringan bisa membuat user sesuai dengan tanggung jawab kerja masing - masing dengan menentukan group dan policies pada setting user. Jika menggunakan Winbox, masuk ke menu System --> User --> Tab Group.



Gambar 3.10 Group Police

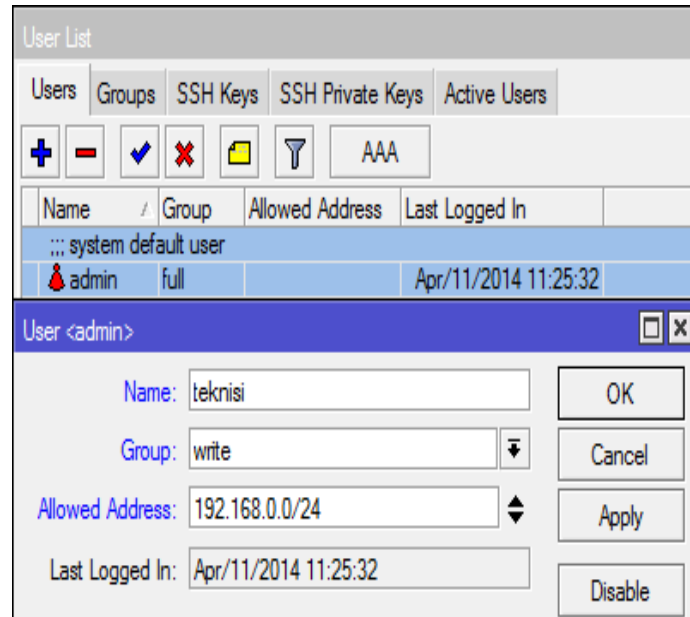
Pada Gambar 3.10 Menjelaskan tentang group police tentang user, ssh keys, active users dengan keterangan nama full, read, write.

Ada beberapa opsi kebijakan yang akan diberikan untuk menentukan priviledge user. berikut detail opsi policy dan hak yang dimiliki :

1. *local* : kebijakan yang mengizinkan user login via local console (keyboard, monitor)
2. *telnet* : kebijakan yang mengizinkan use login secara remote via telnet
3. *ssh* : kebijakan yang mengizinkan user login secara remote via secure shell protocol
4. *ftp* : Kebijakan yang mengizinkan hak penuh login via FTP, termasuk transfer file dar/menuju router. User dengan kebijakan ini memiliki hak read, write, dan menghapus files.
5. *reboot* : Kebijakan yang mengizinkan user me-restart router.
6. *read* : Kebijakan yang mengizinkan untuk melihat Konfigurasi router. Semua command console yang tidak bersifat konfigurasi bisa diakses.
7. *write* : Kebijakan yang mengizinkan untuk melakukan konfigurasi router, kecuali user management. Policy ini tidak mengizinkan user untuk membaca konfigurasi router, user yang diberikan policy wirte ini juga disarankan juga diberikan policy read.
8. *policy* : Kebijakan yang meemberikan hak untuk management user. Should be used together with write policy. Allows also to see global variables created by other users (requires also 'test' policy).
9. *test* : Kebijakan yang memberikan hak untuk menjalankan ping, traceroute, bandwidth-test, wireless scan, sniffer, snoopers dan test commands lainnya.
10. *web* : Kebijakan yang memberikan hak untuk remote router via WebBox
11. *winbox* : Kebijakan yang memberikan hak untuk remote router via WinBox
12. *password* : Kebijakan yang memberikan hak untuk mengubah password
13. *sensitive* : Kebijakan yang memberikan hak untuk melihat informasi sensitif router, misal secret radius, authentication-key, dll.
14. *api* : Kebijakan yang memberikan hak untuk remote router via API.
15. *sniff* : Kebijakan yang memberikan hak untuk menggunakan tool packet sniffer.

### **3.5.7 Allowed Address**

"Allowed Address" digunakan untuk menentukan dari jaringan mana user tersebut boleh akses ke router. Misalkan admin jaringan memiliki kebijakan bahwa teknisi hanya boleh mengakses router melalui jaringan lokal, tidak boleh melalui jaringan public. pada kasus seperti ini, bisa menggunakan opsi "Allowed Address".



Gambar 3.11 Allowed Address

Pada Gambar 3.11 Menjelaskan tentang Allowed Address dengan IP 192.168.0.0/24, group write. Allowed address bisa dengan ip address atau network address. Jika isi dengan ip address, maka user hanya bisa login ketika menggunakan ip address tertentu, jika isi network address, user bisa digunakan pada segmen Ip address tertentu.

### 3.5.8 Mikrotik Neighbor Discovery Protocol (MNDP)

Merupakan layer 2 broadcast domain yang memungkinkan perangkat yang support MNDP atau CDP untuk saling "menemukan". Contoh paling sederhana ketika scan winbox untuk meremote router. Dengan melakukan scan, akan muncul informasi mac address, identity, dan ip address router. Sehingga pada saat MNDP ini berjalan, user yang berada dalam jaringan router bisa dengan mudah menemukan router, dan mengetahui beberapa informasi router. Pada router Mikrotik, router yang menjalankan MNDP bisa dilihat di menu IP --> Neighbors. Akan terlihat router yang sedang terkoneksi dan menjalankan MNDP. Pada saat kita melakukan remote via winbox, lalu kita refresh akan muncul identitas, seperti versi mikrotik, mac address mikrotik, ip address mikrotik, dan beberapa lainnya, jika itu ditemukan attacker untuk memasuki system mikrotik dari identitas yang didapat, dan itu sangat membahayakan, jadi diperlukan pengamanan pada router mikrotik melalui mikrotik neighbor discovery protocol.

The screenshot shows a window titled "Neighbor List" with two tabs: "Neighbors" and "Discovery Interfaces". The "Neighbors" tab is active, displaying a table of discovered neighbors. The table has three columns: "Interface", "IP Address", and "MAC Address". There are 15 rows of data, each starting with a small red icon representing a neighbor. The status bar at the bottom indicates "23 items (1 selected)".

Interface	IP Address	MAC Address
ether1	192.168.128.11	00:0C:42:34:77:77
ether1	192.168.131.12	FC:5B:26:21:0B:90
ether1	192.168.131.105	FC:5B:26:21:0A:B0
ether1	192.168.131.106	FC:5B:26:21:0A:88
ether1	10.3.0.2	D4:CA:6D:41:1E:AC
ether1	192.168.128.13	00:0C:42:33:97:AC
ether1	192.168.128.2	D4:CA:6D:FA:11:44
ether1	192.168.131.14	FC:5B:26:21:0A:E0
ether1	192.168.131.13	FC:5B:26:21:09:20
ether1	192.168.131.15	FC:5B:26:21:0A:D0
ether1	192.168.131.101	FC:5B:26:21:0B:60
ether1	192.168.128.3	D4:CA:6D:FA:10:F9
ether1	192.168.131.16	FC:5B:26:21:0A:B8
ether1	192.168.128.1	FC:5B:26:11:14:C2
ether1	192.168.128.20	00:60:E0:06:02:49

Gambar 3.12 Mikrotik Neighbor Discovery Protocol (MNDP)

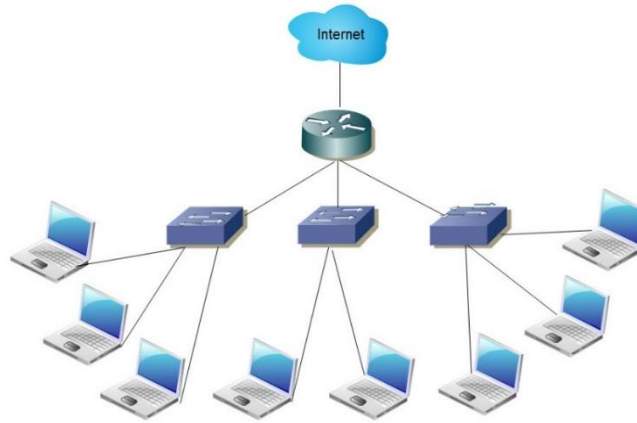
Pada Gambar 3.12 menjelaskan tentang mikrotik neighbour discovery protocol (MNDP), Agar router tidak menampilkan informasi ketika ada user yang melakukan scan discovery protokol, administrator jaringan disarankan untuk men-disable discovery interface. Jika menggunakan Winbox, masuk ke menu IP --> Neighbor --> Tab Discovery Interfaces. Misalnya disable ether2 pada setting discovery interfaces, maka router tidak dapat di scan atau "ditemukan" dari jaringan yang terkoneksi ke ether2.

### 3.6 Simulasi dan Pengujian

#### 3.6.1 Desain

Tahap design pertama membuat rancangan topologi yang terperinci. Terdapat pembagian vlan diantaranya: vlan 10, vlan 20, vlan, 30, dan vlan 40. Pembagian vlan tersebut berfungsi untuk membedakan ruangan yang akan digunakan.





Gambar 3.13 Topologi Jaringan yang dibangun

Pada Gambar 3.13 menjelaskan tentang topologi jaringan yang dibangun melalui metarouter. Topologi sebuah jaringan computer adalah sebuah desain jaringan komputer yang akan di bentuk dengan menggambarkan bagaimana komputer dalam jaringan tersebut dapat saling terhubung satu sama lainnya. Untuk membangun sebuah jaringan komputer baik yang berskala kecil atau besar, terlebih dahulu kita harus membuat rancangan topologinya. Dari topologi ini lah kita bisa menganalisa kebutuhan perangkat keras jaringan yang akan digunakan dan cara akses setiap computer yang tergabung dalam jaringan tersebut.

### 3.6.2 Addressing

Tahap design kedua pemberian IP address pada masing masing network.

Tabel 3.1 IP Address

No	Ru an gan	VI	Ne twork	Si z	B roadcas t
1	Prakt ikum	30	192.168.8.0/26	64	192.168.8.63
2	Server	40	192.168.8.64/28	14	192.168.8.79
3	Dosen	10	192.168.8.80/29	6	192.168.8.87
4	T eknisi	20	192.168.8.88/29	6	192.168.8.95
5	Net work1	-	192.168.8.96/30	2	192.168.8.99
6	Net work2	-	192.168.8.100/3	2	192.168.8.103
7	Net work3	-	192.168.8.104/3	2	192.168.8.107
8	Net work4	-	192.168.8.108/3	2	192.168.8.111

Pada Tabel 3.1 terlihat bahwa adanya pembagian IP Address untuk ruangan praktikum dikonfigurasi pada Vlan 30 dengan network 192.168.8.0/26, untuk ruangan server dikonfigurasi pada Vlan 40 dengan network 192.168.8.64/28, untuk ruangan dosen dikonfigurasi pada Vlan 10 dengan network 192.168.8.80/29, untuk ruangan network 1 dikonfigurasi pada Vlan kosong dengan network 192.168.8.96/30, untuk ruangan network 2 dikonfigurasi pada Vlan kosong dengan network 192.168.8.100/30, untuk ruangan network 3 dikonfigurasi pada Vlan kosong dengan network 192.168.8.104/30, dan untuk ruangan network 4 dikonfigurasi pada Vlan kosong dengan network 192.168.8.108/30.

### 3.6.3 Access Control

Tahapan berikutnya pemberian Access Control List (ACLs)

Tabel 3.2 Acces Control List

No	Vlan ID	IP Server	Website
1	10	159.148.147.196	mikrot ik.com
2	20	103.247.9.130	polinela.ac.id
3	30	202.65.113.16	mikrot ik.co.id
4	40	103.28.25.45	mikrot ik.polinela.ac.id

Pada Tabel 3.2 dilakukan proses Acces Control List berdasarkan ID Vlan , terlihat bahwa ID Vlan 10 diterapkan untuk IP Server 159.148.147.196 dengan domain mikrot ik.com, Vlan 20 diterapkan untuk IP Server 103.247.9.130 dengan domain polinela.ac.id, Vlan 30 diterapkan untuk IP Server 202.65.113.16 dengan domain mikrot ik.co.id, dan Vlan 40 diterapkan untuk IP Server 103.28.25.45 dengan domain mikrot ik.polinela.ac.id .

### 3.6.4 Implementasi desain

Tahap implement dilakukan instalasi peralatan router, switch, kabel UTP, dan Router Fisik konfigurasi. Konfigurasi yang diterapkan berupa: DHCP Server, Vlan, ACLs, Routing, dan IP Service.

### 3.6.5 Pengujian

Tahap operate pertama dilakukan pengujian pada konfigurasi yang telah diimplementasikan.

Tabel 3.3 Pengujian akses

<b>Router \Bandwidth</b>	<b>0 Mbps</b>	<b>30 Mbps</b>	<b>50 Mbps</b>	<b>80 Mbps</b>	<b>100 Mbps</b>
R-Dosen	7%	29%	54%	76%	88%
R-Teknisi	6%	18%	56%	86%	93%
R-Praktik	7%	18%	46%	73%	89%
R-Server	4%	24%	44%	73%	88%
RB 800	9%	23%	30%	41%	46%

Pada Tabel 3.3 untuk kecepatan 0 Mbps ruang dosen sebesar Load CPU nya 7%, untuk kecepatan 30 Mbps ruang teknisi Load CPU nya sebesar 6 %, untuk kecepatan 54 Mbps ruang Praktik Load CPU nya sebesar 7 %, untuk kecepatan 76 Mbps ruang server Load CPU nya sebesar 4 %, dan untuk kecepatan 88 Mbps Pada RB 800 Load CPU nya sebesar 9 % .

### **3.7 Analisis**

Pada tahapan ini dilakukan analisis Peneliti memberikan gambaran sekenario penggunaan Metarouter yang tujuan selain menghemat dengan penggunaan satu routerboard untuk beberapa router juga untuk melakukan monitoring traffic dalam masing masing router yang telah dibuat dalam virtual.

Hal utama yang diperlukan dalam analisa yang dibangun pada penelitian ini adalah pemanfaatan Router OS dan pada penelitian ini penulis menggunakan Winbox sebagai aplikasi Mikrotik RouterOs managemen .

Rancangan Sisitem yang akan dibangun peneliti adalah dengan cara membangun sebuah Metarouter dalam RouterBoard yang mana didalamnya dibentuk beberapa virtual sebagai Router maupun OS yang akan berjalarn dalam satu Router Board selain hai itu fungsi dari penelitian ini juga digunakan untuk memonitoring traffic dlam sebuah Router Board yang terdiri dari beberapa router sehingga akan lebih simple, hemat dan mudah dalam counter data khususnya dalam forensic digital.

Selain Itu penulis juga memanfaatkan metode lifeforensic guna memonitoring traffic yang terjadi dan mendapatkan bukti data yang valid. Akan tetapi dalam sebuah routerboard hanya terdapat satu consul yang digunakan untuk memonitoring maka penulis memberikan solusi dengan melakukan pemetaan user agar bukti digital yang didapat bisa valid.

### **3.8 Kesimpulan**

Berdasarkan data yang diperoleh selama penelitian dan pembahasan pada Simulasi peningkatan keamanan data pada metarouter yang sudah tereksplorasi, maka jika menggunakan teknologi metarouter dapat membangun insfrstruktur jaringan yang rumit dengan hanya menggunakan sebuah routerboard saja, walaupun topologi jaringan yang dibangun terlihat rumit, karena bagi yang menguasai dan mampu menerapkan virtualisasi metarouter akan dapat dengan mudah membangun jaringan dan mengembangkan jaringan pada umumnya. Jika membutuhkan jaringan yang komplek, dengan membeli berbagai macam hardware yang harganya sangat mahal bukanlah solusi satu-satunya yang peroleh. Fitur Metarouter mampu menjalankan routerOS secara virtual, sehingga bisa memiliki beberapa unit router hanya dengan modal sebuah routerboard. Selain itu Teknologi Metarouter juga dapat menjalankan Linux OpenWRT yang memungkinkan membangun web server dan server lainnya berbasis Linux. Dengan menggunakan virtualisasi metarouter maka tidak akan membuat beban atau hambatan pada sebuah laptop atau PC.

# BAB 4

## HASIL DAN PEMBAHASAN

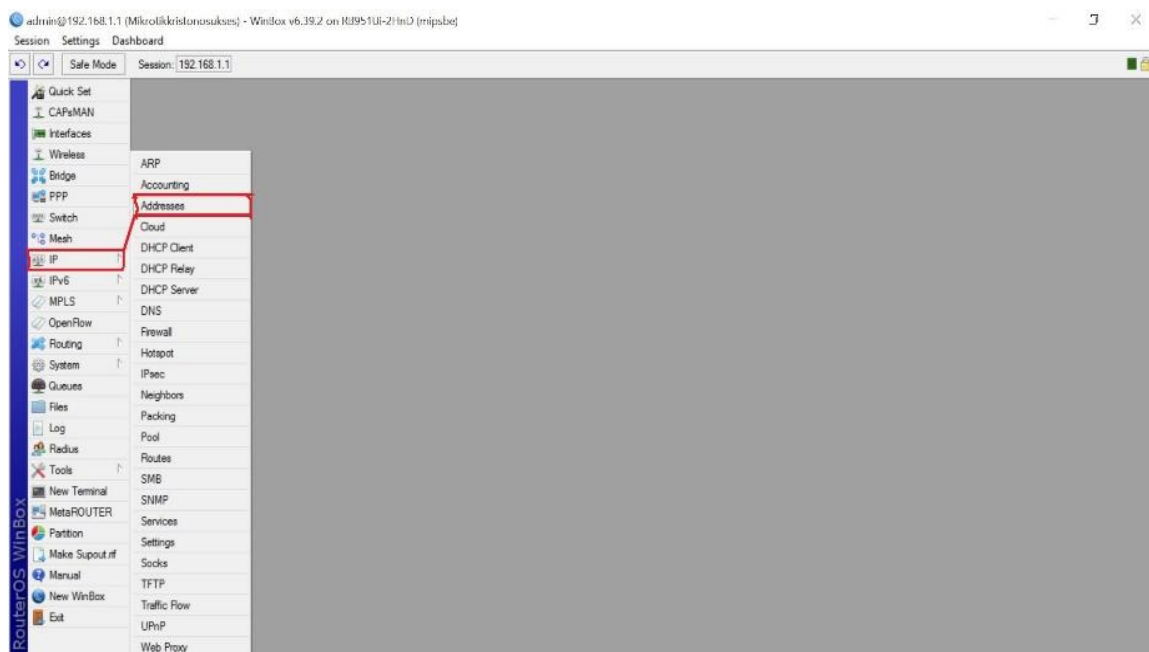
Pada bagian ini menjelaskan hasil yang didapatkan selama penelitian yang telah dilakukan berdasarkan perumusan dan tujuan penelitian, yaitu:

- 1) Melakukan setting metarouter dan keamanan data
- 2) melakukan simulasi eksplorasi meta router .

### 4.1 Setting Metarouter

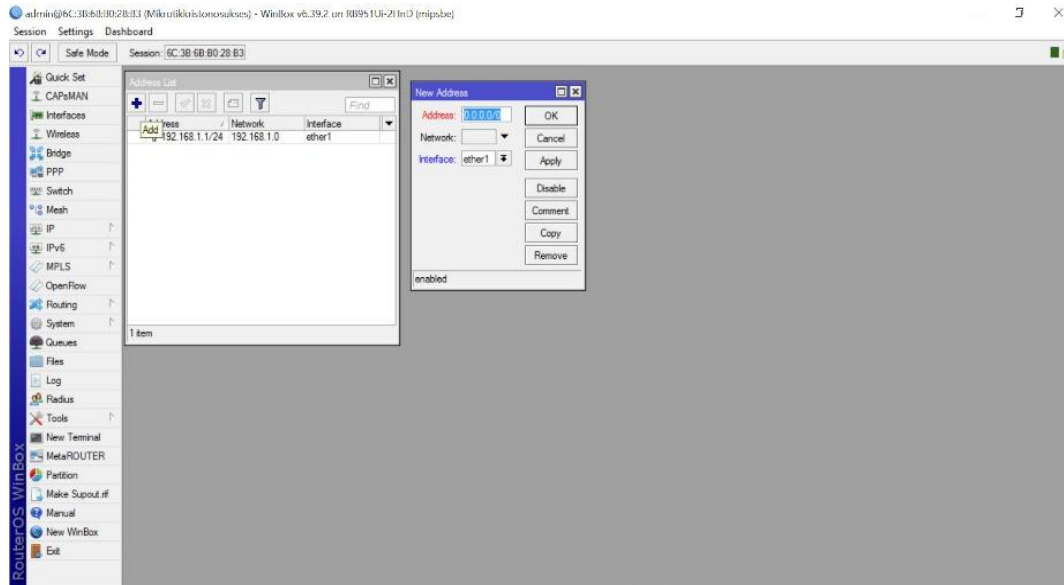
#### 4.1.1 Melakukan pengaturan IP network

Sebelum melakukan setting virtual router pada bagian ini terlebih dahulu melakukan setting IP yang akan gunakan untuk clien yang akan terkoneksi dengan mikrotik . menentukan IP yang akan jadikan sebagai IP public yang berikan kepada Clie. Berikut cara setting network IP pada mikrotik router board.



Gambar 4.1 Setting IP Networ di Virtual Box

Pada Gambar 4.1 Menjelaskan tentang bagaimana cara melakukan Settingan IP Network di Virtual Box. Kemudian di virtual box bisa melakukan setting IP , penentuan kelas dan penentuan klasifikasi IP.



Gambar 4.2 Pembuatan IP address

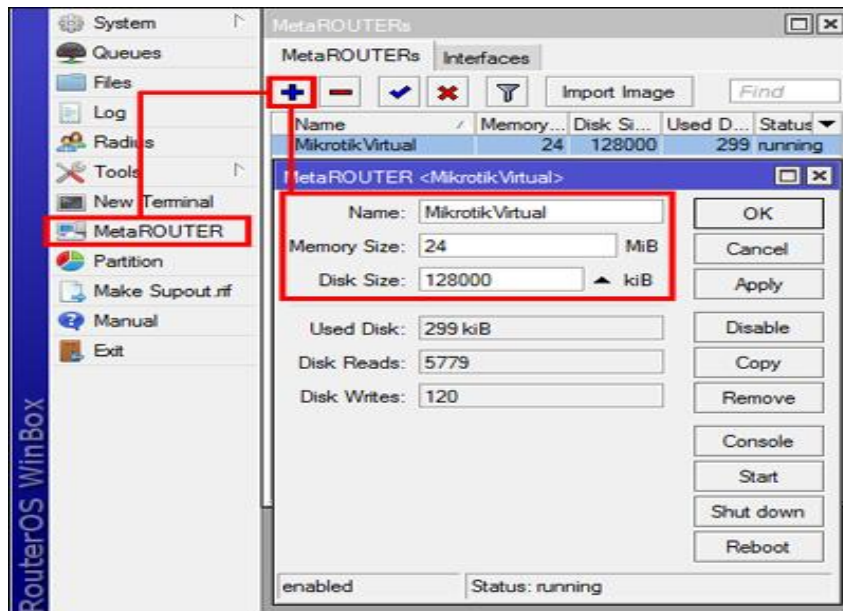
Pada Gambar 4.2 menjelaskan tentang pembuatan IP Address pada sebuah metarouter. Jika kita perhatikan pada router master terdapat ip address 10.10.10.1 di interface virtual, dan pada virtual router terdapat ip address 10.10.10.2 di interface ether1. Dengan ip address inilah nanti router master dan virtual router akan saling interkoneksi. Agar virtual router dapat terkoneksi ke internet, kita setting router master sebagai gateway. Cara setting juga sama persis ketika kita setting router fisik. Begitu juga dengan setting NAT, DNS nya.

#### 4.1.2 Melakukan Setting Metarouter

Pada saat berbisnis di dunia internet, tentu kita akan banyak menemui pelanggan yang bermacam kriteria. Beberapa user yang cukup mengenal MikroTik terkadang menginginkan akses full ke router kita, atau paling tidak mereka membutuhkan router lagi untuk bisa memmanagement jaringan secara full. Sebenarnya kita sebagai penyedia jasa bisa saja memberikan router lagi, namun tentu akan membutuhkan biaya yang lebih besar. Atau pada kasus lain misalnya kita hendak melakukan lab jaringan yang membutuhkan lebih dari satu router. Salah satu solusi hemat adalah dengan memanfaatkan fitur MetaROUTER.

MetaROUTER merupakan fitur MikroTik yang memungkinkan untuk menjalankan operating system baru secara virtual. Hampir sama seperti aplikasi VMware atau VirtualPC pada Windows. MetaROUTER bisa kita gunakan untuk menjalankan Operating System didalam OS MikroTik yang sedang berjalan.

Pada bagian ini menjelaskan bagaimana melakukan seting metarouter, berikut langkah yang bisa lakukan Pertama, masuk ke menu MetaROUTER. Klik tombol + untuk menambahkan virtual router. Disini ada 3 parameter yang perlu ditentukan, "Name" diisi dengan nama Virtual Router sesuai kebutuhan Anda. Kemudian Parameter RAM dan Hardisk juga diisi seuai kebutuhan. Parameter lainnya bisa dibiarkan bernilai default.



Gambar 4.3 Membuat MetaRouter

Pada Gambar 4.3 menjelaskan tentang bagaimana membuat metarouter. Virtual Router di Metarouter akan berjalan saat tombol *Apply* di eksekusi. Operating System secara otomatis akan menggunakan RouterOS MikroTik dan versi yang dijalankan sama dengan versi RouterOS Router MikroTik. Virtual Router ini hanya bisa diakses secara console dengan perintah : */metarouter console [nama-virtual-router]*.

```
[admin@RouterGW] > /metarouter console MikrotikVirtual

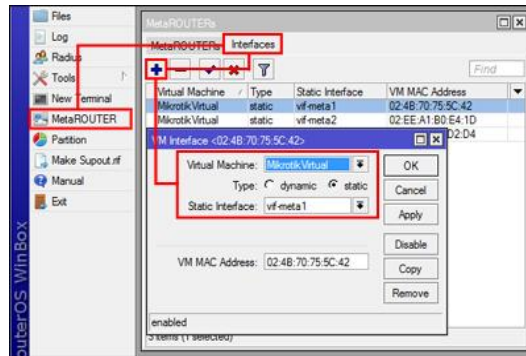
[Ctrl-A is the prefix key]

Starting...
Starting services...

MikroTik 6.15
MikroTik Login: admin
Password: █
```

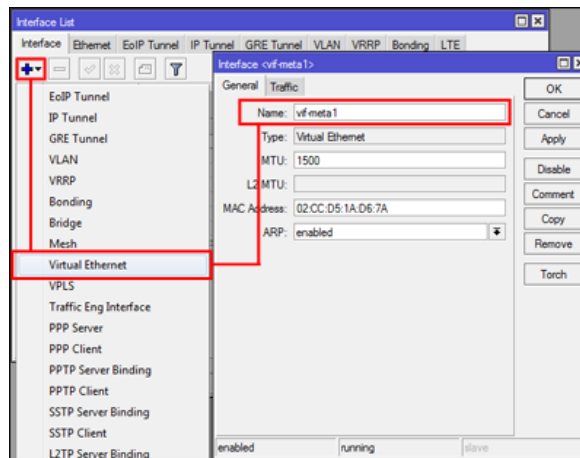
Gambar 4.4 Console Meta router

Pada Gambar 4.4 menjelaskan tentang console metarouter. Langkah selanjutnya adalah membuat virtual Ethernet yang nanti akan digunakan oleh virtual router untuk dapat berkomunikasi dengan router master atau bahkan device lain dalam jaringan.



Gambar 4.5 Setting Virtual Ethernet

Pada Gambar 4.5 Menjelaskan tentang setting virtual Ethernet. Satu virtual ether akan digunakan oleh virtual router untuk dapat berkomunikasi dengan Router Master client.



Gambar 4.6 setting interface metarouter



Pada Gambar 4.6 menjelaskan tentang bsetting interface metarouter. Langkah berikutnya adalah melakukan seting interface metarouter. Metarouter ini digunakan untuk membuat virtual interface router seperti pada Gambar 4.6. Setting berikutnya adalah pada opsi "Virtual Machine" pilih di virtual router mana virtual ethernet akan digunakan, pilih Type static Static Interface. Pada contoh diatas, akan mensetting virtual router dengan dua interface ethernet. Satu ethernet untuk komunikasi virtual router ke internet, satu lagi untuk komunikasi ke client. Untuk memastikannya, coba remote virtual router secara console kemudian tampilkan interface ethernet.

Interface ether1 di virtual router sudah bisa komunikasikan dengan interface pada router master, caranya cukup setting ip address satu segmen antara interface virtual di router master dengan interface ether1 di virtual router. Sedangkan ether2 virtual router, masih belum bisa berkomunikasi dengan perangkat lain atau client, supaya bisa berkomunikasi perlu bridging dengan interface yang terkoneksi secara fisik dengan jaringan client.

### 4.1.3 Pengambilan Data Metarouter

Pada bagian ini akan menjelaskan langkah-langkah Pengambilan data pada metarouter dengan melakukan interkoneksi antar ether yang sudah setting menjadi virtual router pada tahap setting diatas.

Langkah berikutnya adalah melakukan koneksi pengambilan data di metarouter. Pertama lakukan setting IP di computer client yang akan melakukan Pentest . langkah pertama membuat client meta router

```
[admin@RouterGW] /metarouter> add name=client1 memory-size=32
[admin@RouterGW] /metarouter> print
Flags: X - disabled
# NAME MEMORY-SIZE DISK-SIZE USED-DISK STATE
0 client1 32MiB 0kiB 189kiB running
[admin@RouterGW] /metarouter>
```

Gambar 4.7 Create Client Metarouter

Pada Gambar 4.7 menjelaskan tentang create client metarouter .Setelah membuat client meta router selanjutnya melakukan koneksi antar client meta router.

```

[admin@RouterGW] /ip address> add address=10.0.1.1/24 interface=vif1
[admin@RouterGW] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 D 10.5.8.68/24 10.5.8.0 10.5.8.255 ether1
1 10.0.1.1/24 10.0.1.0 10.0.1.255 vif1
[admin@RouterGW] /ip address>

```

Gambar 4.8 Koneksi Metarouter Client

Pada Gambar 4.8 menjelaskan tentang koneksi metarouter client. Setelah Client terinterkoneksi baru melakukan seting pengambilan paket data antar client dalam metarouter.

```

[admin@Client1] /interface ethernet> p
Flags: X - disabled, R - running, S - slave
# NAME MTU MAC-ADDRESS ARP
0 R ether1 1500 02:49:E8:55:8E:E8 enabled
1 R ether2 1500 02:16:16:90:EF:0E enabled
[admin@Client1] /interface ethernet> set 0 name=public
[admin@Client1] /interface ethernet> set 1 name=local
[admin@Client1] /interface ethernet> print
Flags: X - disabled, R - running, S - slave
# NAME MTU MAC-ADDRESS ARP
0 R public 1500 02:49:E8:55:8E:E8 enabled
1 R local 1500 02:16:16:90:EF:0E enabled
[admin@Client1] /interface ethernet>

[admin@Client1] /ip address> add address=10.0.1.2/24 interfae=public
[admin@Client1] /ip address> add address=10.0.2.1/24 interface=local
[admin@Client1] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
# ADDRESS NETWORK BROADCAST INTERFACE
0 10.0.1.2/24 10.0.1.0 10.0.1.255 public
1 10.0.2.1/24 10.0.2.0 10.0.2.255 local

[admin@Client1] /ip route> add gateway=10.0.1.1
[admin@Client1] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS PREP-SRC G GATEWAY DISTANCE INTERFACE
0 A S 0.0.0.0/0 r 10.0.1.1 1 public
1 ADC 10.0.1.0/24 10.0.1.2 0 public
2 ADC 10.0.2.0/24 10.0.2.1 0 local
[admin@Client1] /ip route>

[admin@Client1] /ip firewall nat> add action=masquerade out-interface=public chain=srcnat

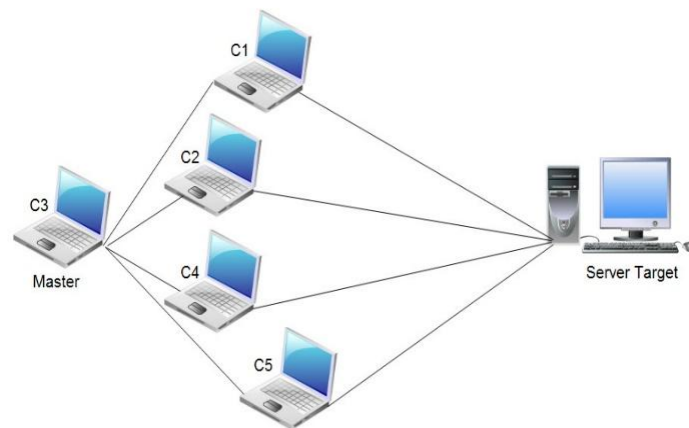
```

Gambar 4.9 Pengambilan Paket data Metarouter

Pada Gambar 4.9 menjelaskan tentang pengambilan paket data pada metarouter sehingga cara ini bisa digunakan pada saat kita melakukan praktek pengambilan data lewat metarouter.

## 4.2 Skenario Pengujian Serangan DoS (Denial of Service)

DoS (Denial of Service) adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

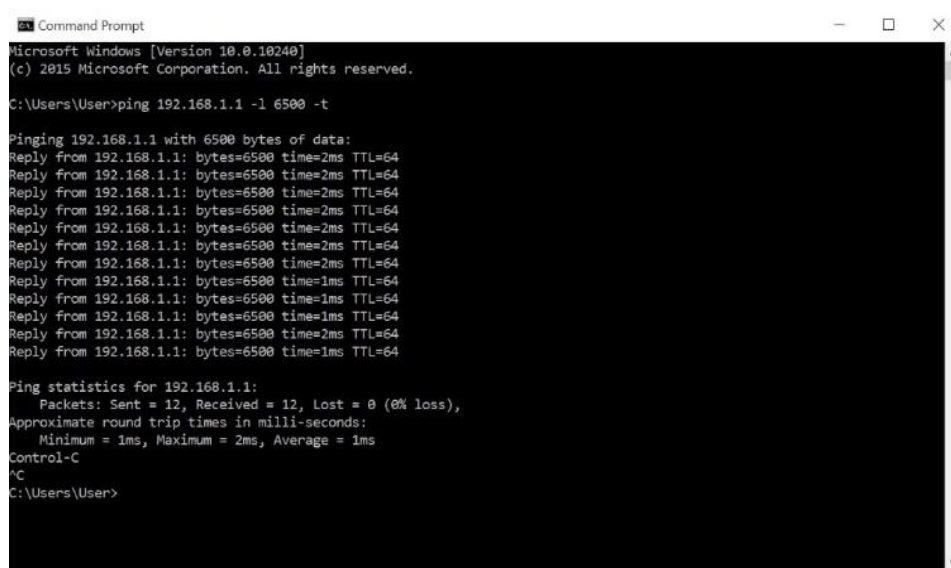


Gambar 4.10 Konsep serangan DoS

Pada Gambar 4.10 menjelaskan tentang konsep serangan Dos . Dalam sebuah serangan Denial of Service, penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:

1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai traffic flooding.
2. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disediakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai request flooding.
3. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan merusak fisik terhadap komponen dan server.

Bentuk serangan Denial of Service awal adalah serangan SYN Flooding Attack, yang pertama kali muncul pada tahun 1996 dan mengeksploitasi terhadap kelemahan yang terdapat di dalam protokol Transmission Control Protocol (TCP). Serangan-serangan lainnya akhirnya dikembangkan untuk mengeksploitasi kelemahan yang terdapat di dalam sistem operasi, layanan jaringan atau aplikasi untuk menjadikan sistem, layanan jaringan, atau aplikasi tersebut tidak dapat melayani pengguna, atau bahkan mengalami crash. Beberapa tool yang digunakan untuk melakukan serangan DoS pun banyak dikembangkan setelah itu (bahkan beberapa tool dapat diperoleh secara bebas), termasuk di antaranya Bonk, LAND, Smurf, Snork, WinNuke, dan Teardrop.



```
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\User>ping 192.168.1.1 -l 6500 -t

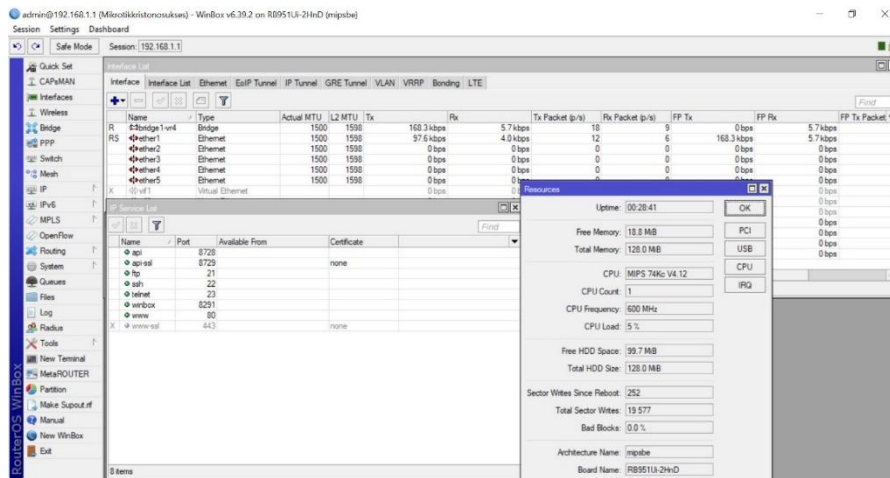
Pinging 192.168.1.1 with 6500 bytes of data:
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=1ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=1ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=1ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=2ms TTL=64
Reply from 192.168.1.1: bytes=6500 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 12, Received = 12, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
Control-C
^C
C:\Users\User>
```

Gambar 4.11 Simulasi Serangan DOS dengan Ping ICMP

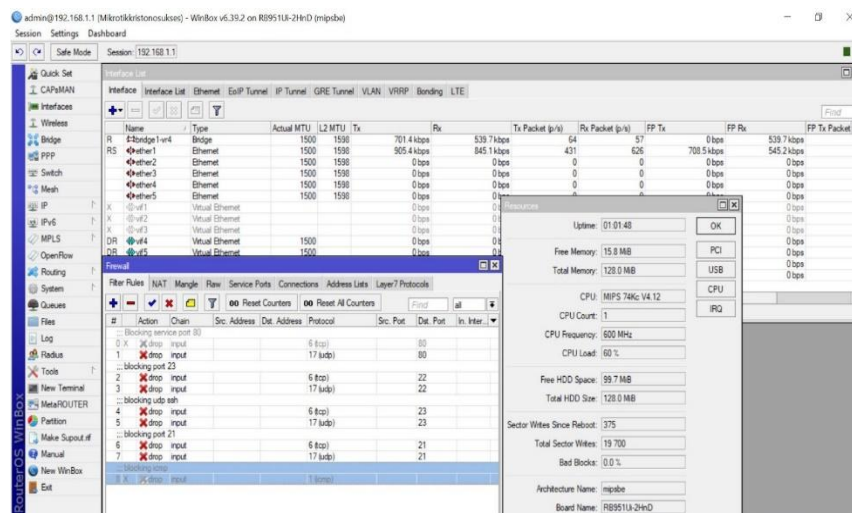
Pada Gambar 4.11 menjelaskan tentang simulasi serangan DoS dengan Ping ICMP. Meskipun demikian, serangan terhadap TCP merupakan serangan DoS yang sering dilakukan. Hal ini disebabkan karena jenis serangan lainnya (seperti halnya memenuhi ruangan hard disk dalam sistem, mengunci salah seorang akun pengguna yang valid, atau memodifikasi tabel routing dalam sebuah router) membutuhkan penetrasi jaringan terlebih dahulu, yang kemungkinan penetrasinya kecil, apalagi jika sistem jaringan tersebut telah diperkuat. Sebuah serangan Denial of Service adalah teknik hacking untuk membuat down atau lumpuh situs atau server dengan membanjiri situs atau server dengan banyak lalu lintas atau packet data sehingga server tidak dapat memproses semua permintaan dalam

real time atau bersamaan dan akhirnya down atau lumpuh. Berikut langkah langkah skenario penyerangan mikrotik .



Gambar 4.12 Simulasi traffic Sebelum terjadi serangan

Pada Gambar 4.12 menjelaskan tentang simulasi traffic sebelum terjadi serangan DoS. Keadaan traffic sebelum terjadi serangan menunjukkan memori data dan cpu yang bergerak belum signifikan terjadinya transaksi DoS akan Mempengaruhi kinerja dari mikrotik dimana dengan adanya serangan Dos CPU akan mengalami kenaikan akses yang signifikan hal ini akan menyebabkan kinerja dari paket data akan down.



Gambar 4.13 Hasil Serangan DoS

Pada gambar 4.13 menjelaskan tentang hasil serangan DoS. Setelah terjadi serangan resource pad traffic paket datanya amenjadi naik baik dari space memorinya hingga CPU load akan naik secara signifikan hal ini yang menyebabkan kan down dalam network traffic maupun down computer yang diserang.

### 4.3 Keamanan Data

Serangan DoS (Denial of Service) dapat menyebabkan overloading router. Yang berarti bahwa penggunaan CPU mencapai 100% dan router bisa menjadi tidak terjangkau dengan timeout. Semua operasi pada paket yang dapat menggunakan daya CPU yang signifikan seperti firewall (filter, NAT, mangle), logging, antrian dapat menyebabkan overloading jika terlalu banyak paket per detik tiba di router.

Umumnya tidak ada solusi sempurna untuk melindungi terhadap serangan DoS. Setiap layanan bisa menjadi kelebihan beban karena terlalu banyak permintaan. Tapi ada beberapa metode untuk meminimalkan dampak serangan.

Langkah Pertama yang dilakukan Adalah Melakukan Diagnosa serangan pada traffic jaringan .

1. Melakukan koneksi diagnose Firewal

```
/ip firewall connection print
```

Gambar 4.14 Diagnosa Firewal

2. Melakukan Diagnosa koneksi pada interface network

```
/interface monitor-traffic ether3
```

Gambar 4.15 Diagnosa interface network

3. Melakukan diagnose pada kinerja CPU

```
/system resource monitor
```

Gambar 4.16 Diagnosa pada Kinerja CPU

Setelah melakukan diagnose pada traffic jaringan maka akan diketahui traffic aman atau terdapat gejala gejala serangan atau traffic yang mencurigakan, untuk menanggulangi terjadinya keusakan data dan serangan yang tidak diinginkan maka melakukan proteksi terhadap serangan atau alur data yang tidak wajar salah satunya dengan melakukan pembatasan akses.

### 1. Melakukan Pembatasan pengalamatan IP adres

```
/ip firewall filter add chain=input protocol=tcp connection-limit=LIMIT,32 \  
action=add-src-to-address-list address-list=blocked-addr address-list-timeout=1d
```

Gambar 4.17 Melakukan Pembatasan IP Adres

### 2. Melakukan pembatasan paket data pada traffic

Bukan hanya dengan menjatuhkan paket penyerang (dengan 'action = drop') router dapat menangkap dan menahan koneksi dan dengan router yang cukup kuat, ia dapat memperlambat penyerang ke bawah.

```
/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr \  
connection-limit=3,32 action=tarpit
```

Gambar 4.18 Pembatasan Paket pada Traffic

### 3. Melakukan pemfilteran SYN

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-state=new \  
action=jump jump-target=SYN-Protect comment="SYN Flood protect" disabled=yes \  
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=400,5 connection-state=new \  
action=accept comment="" disabled=no \  
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-state=new \  
action=drop comment="" disabled=no
```

Gambar 4.19 Melakukan pemfilteran SYN

Pada Gambar 4.19 menjelaskan tentang melakukan pemfilteran pada metarouter. Dengan Melakukan pembatasan dan proteksi diharapkan bisa mempermudah dalam monitoring dan mempersempit kinerja dari para attacker yang ingin masuk kedalam server tanpa ijin.

#### 4.4 Hasil Pengujian

Hasil pada tahap pengujian mengenai keamanan port 80 dapat dilihat pada Tabel 4.1, dimana kondisi pada saat sebelum diserang ,sesudah diserang tanpa dilakukan pengamanan, dan sesudah diserang dengan melakukan peningkatan keamanan.

Tabel 4.1 Hasil Pengujian Port 80

Eksploitasi Port 80	Sebelum Diserang	Sesudah diserang tanpa pengamanan	Sesudah diserang ditingkatkan keamanannya
CPU	5 %	60 %	5 %
Memory	18,8 MiB	15,8 MiB	15,5 MiB
Kecepatan	5.7 kbps	539.7 kbps	5.3 kbps
Paket	9 Packet	57 Packet	8 Packet
Status Router	Normal	down	Normal

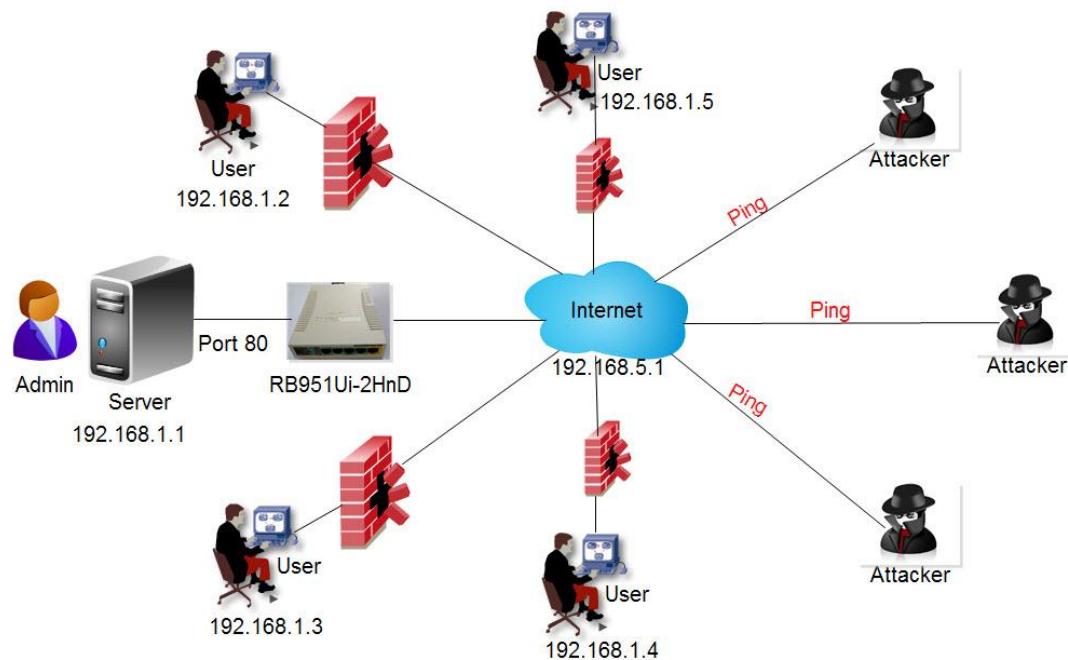
Berdasarkan hasil pengujian yang telah dilakukan maka dapat disimpulkan bahwa kondisi CPU sebelum diserang berada pada posisi 5%, Memory 18,8 MiB, kecepatan 5,7 kbps, paket 9, status router normal, setelah dilakukan penyerangan tanpa adanya pengamanan terjadi perubahan pada setiap komponennya, yaitu CPU meningkat menjadi 60%, Memory 15,8 MiB, Kecepatan 539.7 kbps, paket 57, dan status router menjadi down. Untuk menanggulangi permasalahan yang ada maka perlu ditingkatkan keamanannya. Setelah ditingkatkan keamanannya maka kondisi CPU menjadi 5%, Memory 15,5 MiB, Kecepatan 5.3 kbps, Paket 8 dan Status Router menjadi Normal.

Cara Meningkatkan keamanan data:

1. Modifikasi Header Paket berfungsi untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing.
2. Translasi Alamat Jaringan berfungsi untuk metranslasikan alamat IP privat ke IP publik.
3. Filter Paket berfungsi untuk menentukan nasib paket apakah dapat diteruskan atau tidak.



4. Harus tahu serangan berasal, jika yang diserang lewat port 80 langkah yang harus dilakukan adalah mengganti port yang masih digunakan, atau mendisable port lewat firewall nya.
5. Filterisasi terhadap port dan service, itu jika masih menggunakan layanan webservice pada mikrotik metarouter.
6. Membatasi penggunaan port , misal jika yang gunakan port 80 , maka bisa ganti port 8888 atau yang lainnya, dengan catatan port yang gunakan tidak sama dengan service yang lain harus ingat port nya , begitupula jika port yang lain diserang hal yang lakukan adalah sama ,yaitu dengan melakukan tindakan sesuai penjelasan meningkatkan keamanan data pada langkah-langkah 1 dan 2.



Gambar 4.20 Ilustrasi Peningkatan Keamanan Port 80

Hasil pada tahap pengujian mengenai keamanan port 22 dapat dilihat pada tabel 4.2, dimana kondisi pada saat sebelum diserang ,sesudah diserang tanpa dilakukan pengamanan, dan sesudah diserang dengan upaya melakukan peningkatan keamanan.

Tabel 4.2 Hasil Pengujian Port 22

Eksplorasi Port 22	Sebelum Diserang	Sesudah diserang tanpa pengamanan	Sesudah diserang ditingkatkan keamanannya
CPU	5 %	35 %	4 %
Memory	15,9 MiB	15,5 MiB	15,3 MiB
Kecepatan	6.8 kbps	514.3 kbps	6.8 kbps
Paket	10 Packet	46 Packet	11 Packet
Status Router	Normal	down	Normal

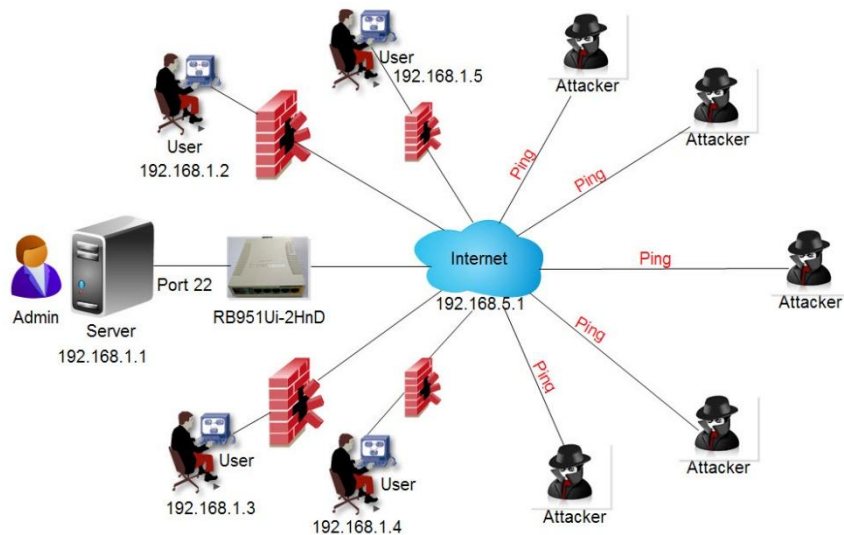
Berdasarkan hasil pengujian yang telah dilakukan maka dapat disimpulkan bahwa kondisi CPU sebelum diserang berada pada posisi 5%, Memory 15,9 MiB, kecepatan 6.8 kbps, paket 10, status router normal, setelah dilakukan penyerangan tanpa adanya pengamanan terjadi perubahan pada setiap komponennya, yaitu CPU meningkat menjadi 35%, Memory Menurun 15,5 MiB, Kecepatan 514.3kbps, paket 46 , dan status router menjadi down. Untuk menanggulangi permasalahan yang ada maka perlu ditingkatkan keamanannya. Setelah ditingkatkan keamanannya maka kondisi CPU menjadi 4%, Memory 15,3 MiB, Kecepatan 6.8 kbps, Paket 11 dan Status Router menjadi Normal.

Berikut bagan keamanan jaringan sesudah diserang dengan melakukan peningkatan keamanan:

Cara Meningkatkan keamanan data:

1. Modifikasi Header Paket berfungsi untuk memodifikasi kualitas layanan bit paket TCP sebelum mengalami proses routing.
2. Translasi Alamat Jaringan berfungsi untuk metranslasikan alamat IP privat ke IP publik.
3. Filter Paket berfungsi untuk menentukan nasib paket apakah dapat diteruskan atau tidak.
4. Harus tahu serangan berasal, jika yang diserang lewat port 22 langkah yang harus dilakukan adalah mengganti port masih digunakan, atau mendisable port lewat firewallnya .
5. Filterisasi terhadap port dan service, itu jika masih menggunakan layanan webservice pada mikrotik metarouter.

6. Membatasi penggunaan port , misal jika yang gunakan port 22 , maka bisa ganti port 99 atau yang lainnya, dengan catatan port yang gunakan tidak sama dengan service yang lain dan harus ingat port nya, begitupula jika port yang lain diserang hal yang lakukan adalah sama ,yaitu dengan melakukan tindakan sesuai penjelasan meningkatkan keamanan data pada langkah-langkah 1 dan 2.



Gambar 4.21 Gambar Ilustrasi Pengamanan Port 22

Berdasarkan gambar 4.21 diketahui bahwa pada port 22 dengan IP Server 192.168.1.1 setelah terjadi penyerangan dan dilakukan peningkatan keamanannya maka kondisi port 22 keamanannya meningkat. Ini dapat dilihat dari hasil pengujian dengan ditingkatkan keamanannya maka kondisi CPU menjadi 4%, Memory 15,3 MiB, Kecepatan 6.8 kbps, Paket 11 dan Status Router menjadi Normal. Dari hasil analisis antara port 80 dan port 22 terjadi perbedaan pada kecepatan CPU, Memory, dan Paket.

# **BAB 5**

## **KESIMPULAN DAN SARAN**

### **5.1 Kesimpulan**

Kesimpulan yang telah didapatkan selama proses penelitian dalam Simulasi Untuk Peningkatan Keamanan Data Pada Metarouter Yang Sudah Tereksplorasi menyimpulkan bahwa:

1. Dari hasil simulasi dapat diketahui karakteristik dari Metarouter dapat mencari rute atau jalur yang terbaik antara dua segmen jaringan, dapat mengelola dan menangani banyak tugas antar segmen, dan dapat membantu mengelola lalu lintas jaringan.
2. Metarouter selain lebih hemat dari segi finansial, juga mudah dalam melakukan manajemen network dan proteksi keamanan. Dimana hanya dengan satu setingan pengamanan akan berdampak kepada semua klien yang dibuat dalam metarouter, selain itu juga mempermudah dalam monitoring network.
3. Metarouter Memungkinkan terjadinya keamanan data dan pengambilan log data yang dilakukan dalam satu panel Routerboard walaupun terdapat beberapa client.
4. Untuk menanggulangi terjadinya kerusakan data dan serangan yang tidak diinginkan maka melakukan proteksi terhadap serangan atau alur data yang tidak wajar salah satunya dengan melakukan pembatasan akses.

### **5.2 Saran**

1. Metarouter hanya terdapat dalam satu Routerboard yang belum bisa terupdate secara otomatis . Hal ini untuk menanggulangi ketika terjadi kerusakan pada RouterBoard secara fisik.
2. Melakukan perbandingan terhadap beberapa penelitian pada metarouter yang lainnya untuk bisa membangun keamanan data pada jaringan yang lebih baik kedepannya.

## Daftar Pustaka

- Albert, S., & Juni, E. (2015). Analisa Sistem Pengaman Data Jaringan Berbasis VPN. *Stmik Ikmi*, 10(18), 220. Retrieved from [www.ikmi.ac.id](http://www.ikmi.ac.id)
- Fahri, M., Fiade, A., & Suseno, H. B. (2017). Simulasi Jaringan Virtual Local Area Network (VLAN) Menggunakan Pox Controller. *Jurnal Teknik Informatika*, 10(1), 85–90.
- Fietyata, Y., & Prayudi, Y. (2013). Teknik Eksplorasi Bukti Digital Pada File Sharing Protokol SMB Untuk Mendukung Forensika Digital Pada Jaringan Komputer. *Konferensi Nasional Informatika*, (October).
- Galang, C. M., Eko, S., & Imam, A. (2017). Teknik Virtualisasi Router Menggunakan Metarouter Mikrotik (Studi Kasus: Laboratorium Jaringan Komputer Politeknik Negeri Lampung), 2641–2644. <https://doi.org/10.1111/ijlh.12426>
- Ghozali, T., & Indriati, K. (2016). Simulasi Jaringan Multi Protocol Label Switching Dan Traffic Engineering. *JURNAL ELEKTRO*, 9(1), 23–34.
- Isnanto, R., & Diponegoro, U. (2017). Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan. *Jurnal Ilmu Teknik Elektro Komputer Dan Informatika*, 3, 12–19.
- Komang, I. G., Mardiyana, O., Komang, I. G., & Mardiyana, O. (2015). Keamanan Jaringan Dengan Firewall Filter Berbasis Mikrotik Pada Laboratorium Komputer STIKOM Bali. *Stmik Stikom*, 1(86), 9–10.
- Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik Pendahuluan Landasan Teori. *JUSI, Universitas Ahmad Dahlan Yogyakarta*, 1(1), 71–80.
- Soon, J. N. P., Abdulla, S. H. R., Yin, C. P., Wan, W. S., Yuen, P. K., & Heng, L. E. (2013). Implementing of Virtual Router Redundancy Protocol in a Private University. *Journal of Industrial and Intelligent Information*, 1(4), 255–259. <https://doi.org/10.12720/jiii.1.4.255-259>

Xianming Gao, Xiaozhe Zhang, Zexin Lu, S. M. (2009). A General Model for the Virtual Router. *ICCT2013, I(1)*, 6–13. Retrieved from binabar@yahoo.co.id