

**ANALISIS IMPLEMENTASI *PORT KNOCKING* DENGAN ROUTING
DINAMIS MENGGUNAKAN PROTOKOL TCP DAN ICMP
DI SMK PGRI 1 NGANJUK**

SKRIPSI

Diajukan Untuk Memenuhi sebagai Syarat guna
Memperoleh Gelar Sarjana Komputer (S.Kom)
Pada Program Studi Teknik Informatika



OLEH :

YANTO SETIAYOKO
NPM: 19.1.03.02.0001

FAKULTAS TEKNIK
UNIVERSITAS NUSANTARA PERSATUAN GURU REPUBLIK INDONESIA
UN PGRI KEDIRI
2023

Skripsi Oleh :

YANTO SETIAYOKO

NPM : 19.1.03.02.0001

Judul :

**ANALISIS IMPLEMENTASI *PORT KNOCKING* DENGAN ROUTING
DINAMIS MENGGUNAKAN PROTOKOL TCP DAN ICMP
DI SMK PGRI 1 NGANJUK**

Telah Disetujui Untuk Diajukan Kepada
Panitia Ujian/Sidang Skripsi Program Studi Teknik Informatika
Fakultas Teknik Universitas Nusantara PGRI Kediri

Tanggal : 12 Juli 2023

Pembimbing I



Daniel Swanjaya, M.Kom
NIDN. 0723098303

Pembimbing II



Intan Nur Farida, M.Kom
NIDN. 0704108701

Skripsi Oleh :

YANTO SETIAYOKO

NPM : 19.1.03.02.0001

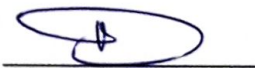


Judul :

**ANALISIS IMPLEMENTASI *PORT KNOCKING* DENGAN ROUTING
DINAMIS MENGGUNAKAN PROTOKOL TCP DAN ICMP
DI SMK PGRI 1 NGANJUK**

Telah dipertahankan di depan Panitia Ujian atau Sidang Skripsi Program Studi
Teknik Informatika Fakultas Teknik Universitas Nusantara PGRI Kediri
Pada tanggal : 18 Juli 2023

Dan Dinyatakan Telah Memenuhi Persyaratan

Panitia Penguji

- | | | |
|---------------|--------------------------------|---|
| 1. Ketua | : Daniel Swanjaya, M.Kom |  |
| 2. Penguji I | : Dinar Putra Pamungkas, M.Kom |  |
| 3. Penguji II | : Patmi Kasih, M .Kom |  |

Mengetahui,
Dekan Fakultas Teknik

Dr. Suryo Widodo, M.Pd
Nip. 196402021991031002

SURAT PERNYATAAN

Yang bertanda tangan di bawah ini saya,

Nama : YANTO SETIAYOKO
Jenis Kelamin : Laki-Laki
Tempat atau tgl.lahir : Nganjuk atau 18 Maret 1995
NPM : 19.1.03.02.0001
Fak atau Jur atau Prodi : Fakultas Teknik atau Teknik Informatika

Menyatakan dengan sebenarnya, bahwa dalam Skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi, dan sepanjang pengetahuan saya tidak terdapat karya tulis atau pendapat yang pernah diterbitkan oleh orang lain, kecuali yang secara sengaja dan tertulis diacu dalam naskah ini disebutkan dalam daftar pustaka.

Kediri, 18 Juli 2023
Yang Menyatakan

YANTO SETIAYOKO
19.1.03.02.0001

MOTTO PENULIS

Motto :

Tuhan Tidak Menuntut

Kita Untuk Sukses,

Tuhan Hanya Menyuruh

Kita Berjuang Tanpa Henti.

Kupersembahkan karya ini buat :
Seluruh keluargaku.

Abstrack

Yanto Setiyoko : ANALISIS IMPLEMENTASI *PORT KNOCKING* DENGAN ROUTING DINAMIS MENGGUNAKAN PROTOKOL TCP DAN ICMP STUDI SMK PGRI 1 NGANJUK, Skripsi, TI FT UN PGRI Kediri, 2022.

Kata kunci : Jaringan; DDOS; Alamat Ketukan; Keamanan; Pendidikan.

SMK PGRI 1 Nganjuk merupakan sekolah swasta yang menawarkan jaringan internet untuk mendukung pembelajaran. Server mikrotik sering diserang selama proses berlangsung. Serangan yang sering diterima yaitu probe, DDOS, kontrol port, dan sniffing. Metode yang digunakan dalam penelitian ini adalah port knocking untuk menutup akses port dan mengembangkan metode tersebut dengan menutup Mac interface winbox dan menambahkan fungsi anti DDOS. Penelitian ini bertujuan meningkatkan keamanan jaringan internet di SMK PGRI 1 Nganjuk. Dengan menambahkan metode pemblokiran DDOS, berdasarkan dapat memperkuat firewall server. Proses penelitian ini berdasarkan umpan NDLC, rencana keamanan jaringan dibuat dan berfungsi seperti yang diharapkan. Dengan menggunakan aplikasi keamanan jaringan, port knocking dan metode pencegahan DDOS dapat meminimalisir penyalahgunaan akses router oleh pihak yang tidak bertanggung jawab.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji Syukur Kami Panjatkan Kehadirat Allah Tuhan Yanh Maha Kuasa, Karena hanya atas perkenan-Nya tugas penyusunan skripsi ini dengan judul *“ANALISIS IMPLEMENTASI PORT KNOCKING DENGAN ROUTING DINAMIS MENGGUNAKAN PROTOKOL TCP DAN ICMP STUDI SMK PGRI 1 NGANJUK“* dapat diselesaikan.

Penyusunan skripsi ini merupakan bagian dari salah satu syarat untuk memperoleh gelar sarjana komputer pada program studi Teknik Informatika UN PGRI Kediri.

Pada kesempatan ini diucapkan terimakasih dan penghargaan yang setulus-tulusnya kepada :

1. Rektor UN PGRI Kediri Dr. Sulistiono, M.Si, yang selalu memberikan dorongan motivasi kepada mahasiswa.
2. Yang terhormat Drs. Suryo Widodo, M.Pd., Selaku Dekan FT Universitas Nusantara PGRI Kediri.
3. Ahmad Bagus Setiawan, S.T., M.M, M.Kom. Selaku Ketua Program Studi Teknik Informastika Universitas Nusantara PGRI Kediri.
4. Dan yang tak lupa Daniel Swanjaya, M.Kom, selaku Dosen Pembimbing I dan Intan Nur Farida, M.Kom, selaku Dosen Pembimbing II yang dengan penuh kesabaran telah memberikan bimbingan dan pengarahan kepada

penulis sehingga skripsi ini dapat terwujud.

5. Seluruh staf dan dosen Teknik Informatika yang telah memberikan ilmu yang sangat berarti untuk penulis.
6. Ibu dan ayah yang telah membantu serta mensupport penulis dalam mengembalikan semangat dalam menyelesaikan karya tulis ini.
7. Istri tercinta yang selalu memberikan semangat, motivasi, dan kasih sayang dan dukungan yang luar biasa.
8. Anakku tercinta dan tersayang yang menjadi motivasi dan semangat dalam menyelesaikan penulisan karya tulis ini.
9. Ucapan terimakasih juga disampaikan kepada pihak-pihak lain yang tidak dapat disebutkan satu persatu, yang telah banyak membantu menyelesaikan skripsi ini.

Disadari bahwa skripsi ini masih banyak kekurangan, maka diharapkan tegur sapa, kritik dan saran, dari berbagai pihak sangat diharapkan.

Wassalamu'alaikum Wr. Wb

Kediri, 18 Juli 2023

YANTO SETIAYOKO
NPM : 19.1.03.03.0001

DAFTAR ISI

Skripsi Oleh :	ii
Skripsi Oleh :	ii
SURAT PERNYATAAN	iv
MOTTO PENULIS	v
Abstrack	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
BAB I	1
PENDAHULUAN	1
A. Latar Belakang	1
B. Identifikasi Masalah	3
C. Rumusan Masalah	4
D. Batasan Masalah.....	4
E. Tujuan Penelitian	5
F. Manfaat Dan Kegunaan Penelitian	6
G. Metode Penelitian.....	7
H. Jadwal Penelitian.....	11
I. Sistematika Penulisan Laporan.....	11
BAB II	13
TINJAUAN PUSTAKA	13
A. Dasar Teori.....	13
1. Analisis	13
2. Lalu Lintas Komputer	14
3. Topologi Jaringan.....	19
4. Keamanan Jaringan	21
5. Metode Pengamanan Jaringan.....	21
6. Port Knocking.....	22
7. Bentuk serangan pada jaringan	23

8. Metode <i>Port Knocking</i>	24
9. <i>Firewall</i>	24
10. NAT	26
11. TCP/IP	27
12. Unit Dan Alat Jaringan.....	29
13. Mikrotik	36
14. <i>Ip Address</i>	37
B. Kajian Pustaka.....	41
C. Keunggulan Penelitian	43
D. <i>Flowchart</i> Alur Penelitian	44
E. Lokasi Penelitian	45
BAB III	50
ANALISIS DAN PERANCANGAN	50
A. Analisa	50
1. Analisa sistem yang berjalan	50
2. Analisa jaringan internet	51
3. Analisa permasalahan.....	52
4. Analisa metode serangan	53
5. Analisa Metode Pengamanan	57
6. Analisa Konfigurasi Perangkat Jaringan Saat Ini	57
7. Analisa NDLC.....	61
B. Desain Sistem (Perancangan)	64
1. Spesifikasi alat	65
2. Perangkat Lunak Yang Digunakan Saat Ini	66
3. Sistem Yang Direncanakan	67
4. Usulan Pengaturan Mikrotik.....	70
BAB IV	82
IMPLEMENTASI DAN PEMBAHASAN	82
A. Implementasi	82
1. Pengujian <i>port knocking</i>	83
2. Pengujian <i>scan port</i>	89
3. Pengujian <i>sniffing</i>	91
4. Pengujian DDOS	95

B. Monitoring	97
C. <i>Management</i>	98
D. Pembahasan.....	98
BAB V	100
PENUTUP	100
A. KESIMPULAN.....	100
B. SARAN.....	101
DAFTAR PUSTAKA	102
LAMPIRAN	104
1. Daftar Validasi Pertanyaan.....	105
2. Hasil Pertanyaan Guru	108
3. Hasil Pertanyaan Staff	108
4. Hasil Pertanyaan Siswa	109
5. Mikrotik Router SMK PGRI 1 Nganjuk.....	109
6. Melakukan Tinjauan Langsung Ruang Server.....	110
7. Melakukan Penerapan Hasil Penelitian	110
8. Hasil Penerapan Port Knocking dan Anti DDOS	111
9. Hasil Pertanyaan Setelah Implementasi Dari Guru.....	114
10. Hasil Pertanyaan Setelah Implementasi Dari Staff	115
11. Hasil Pertanyaan Setelah Implementasi Dari Siswa	116

DAFTAR TABEL

Tabel	Halaman
1.1 Rencana Penelitian	11
2.1 Alamat <i>Unicast</i> IP versi 4	39
2.1 Tabel Kepengurusan.....	46
3.2 Spesifikasi <i>Router</i> RB1100x4.....	66
3.3 Spesifikasi <i>Pc Client</i>	67
3.4 Operating Sistem <i>Router</i>	67
3.5 Operating Sistem <i>Pc Client</i>	67
4.1 Hasil Pengujian	100

DAFTAR GAMBAR

Gambar	Halaman
1.1 Proses tahapan penelitian NDLC	8
2.1 Jaringan LAN	15
2.2. Jaringan <i>Metropolitan Area Network</i>	16
2.3. Skema topologi <i>Wide Area Network</i>	18
2.4. Topologi <i>Star</i>	21
2.5. Skema <i>Firewall</i> Pada Jaringan.....	26
2.6. OSI Model (Kiri) dan TCP/IP Model (Kanan)	29
2.7. Modem <i>Internal</i> dan Modem <i>External</i>	30
2.8. LAN Card.....	31
2.9. <i>Switch</i>	32
2.10. Gambar <i>Router</i> dan Simulasinya	35
2.11. <i>Access Point</i>	36
2.12 Alur <i>Flowchart</i> Penelitian.....	45
2.13 Struktur Organisasi.....	48
3.1 Topologi Yang Berjalan.....	52
3.2 Grafik jumlah serangan terhadap mikrotik	53
3.3 Tindakan <i>Probing</i>	55
3.4 Tindakan DDOS.....	56
3.5 Sebelum terkena DDOS	57
3.6 DHCP <i>Client</i>	58
3.7 DHCP <i>Server</i>	59
3.8 NAT <i>Masquerade</i>	60
3.9 <i>Address List</i>	61

3.10 Pengaturan DNS.....	61
3.11 Topologi Yang diusulkan.....	63
3.12 Alur simulasi pengujian	65
3.13 Router RB1100x4.....	66
3.14 Gambar alur <i>flow chart port knocking</i>	69
3.15 Tampilan awal winbox.....	72
3.16 Tampilan <i>Rule Port knocking</i>	73
3.17 Tampilan <i>Action Rule Port knocking</i>	74
3.18 Tampilan <i>Action Rule Port knocking update</i>	75
3.19 Tampilan <i>Action</i>	76
3.20 Tampilan Blokir Winbox	77
3.21 Tampilan Advanced Blokir Winbox	77
3.22 Tampilan <i>Action</i> Blokir Winbox.....	78
3.23 Tampilan <i>Firewall Menampung Ip</i>	79
3.24 Tampilan <i>Advanced Menampung Ip</i>	80
3.25 Tampilan <i>Action Menampung Ip</i>	80
3.26 Tampilan <i>Drop IP DDOS</i>	81
3.27 Tampilan <i>Action Drop IP DDOS</i>	81
3.28 <i>Mac interface winbox</i>	82
4.1 skema penyerangan <i>hacker</i>	83
4.2 Hasil <i>login</i> winbox mode normal.....	84
4.3 <i>login</i> mikrotik via web	85
4.4 <i>Login</i> mikrotik jalur telnet	85
4.5 Gagal <i>Login</i> mikrotik via winbox	86
4.6 Gagal <i>login</i> mikrotik dari <i>webpage</i>	87
4.7 <i>login</i> mikrotik jalur <i>telnet</i>	87
4.8 Gagal <i>login</i> mikrotik jalur <i>telnet</i>	88
4.9 <i>Ping</i> terhadap <i>port service</i>	88

4.10 Aplikasi <i>Port knocking Client</i>	89
4.11 Berhasil <i>Login Mikrotik</i>	90
4.12 Hasil <i>Scan port Router</i>	91
4.13 Hasil <i>Scan port Router mode disable</i>	92
4.14 Hasil <i>Sniffing Router</i> jalur winbox	93
4.15 Hasil <i>sniffing Router</i> jalur <i>webpage</i>	94
4.16 Hasil <i>Sniffing Router</i> jalur <i>telnet</i>	94
4.17 Hasil <i>Sniffing Router</i> jalur winbox.....	95
4.18 Hasil <i>Sniffing Router</i> jalur <i>webpage</i>	95
4.19 Hasil <i>Sniffing Router</i> jalur <i>telnet</i>	96
4.20 Hasil <i>DDOS Router</i> mode normal	97
4.21 Implementasi anti <i>DDOS</i>	98

BAB I

PENDAHULUAN

A. Latar Belakang

SMK 1 Nganjuk merupakan salah satu lembaga pendidikan swasta terbaik di wilayah Nganjuk. Salah satu keunggulan sekolah ini adalah hasil ujian nasional yang setiap tahun mendapat peringkat bagus di daerah. Selain itu, SMK PGRI 1 Nganjuk juga sering meraih kemenangan dalam lomba-lomba tingkat regional, residensial, provinsi, dan nasional.

SMK PGRI 1 Nganjuk menyediakan berbagai program kejuruan bagi calon siswa yang ingin mendaftar di sana, seperti program Teknik Jaringan Komputer (TKJ) yang membahas tentang dunia jaringan komputer dan internet dan program Audio Video Technology (TAV) yang berhubungan dengan pemrosesan audio, video dan gambar. Banyak juga kesempatan pelatihan kejuruan lainnya di SMK PGRI 1 Nganjuk.

Di bidang pendidikan terdapat ruang-ruang yang mendukung proses belajar mengajar, yang membantu siswa mencari informasi dan menerapkan materi yang dipelajari di kelas. Salah satunya adalah akses *hotspot* yang memungkinkan siswa terhubung ke internet di area tertentu. SMK PGRI 1 Nganjuk menggunakan *router server* untuk mengelola jaringannya.

SMK PGRI 1 Nganjuk memilih *server router* karena selain fungsinya yang lengkap dan mudah digunakan, *router* juga sangat handal

untuk mengelola infrastruktur jaringan SMK PGRI 1 Nganjuk. *Router* ini memiliki beberapa fitur untuk membantu memenuhi kebutuhan jaringan SMK PGRI 1 Nganjuk. Selain itu, selain fungsionalitas dan kehandalan, infrastruktur ini juga memiliki harga beli yang cukup terjangkau.

Berdasarkan hasil wawancara pada tanggal 24 februari 2023 dengan bapak Sidik effendi selaku penanggung jawab jaringan internet SMK PGRI 1 Nganjuk, beberapa siswa atau pihak luar mencoba meretas manajemen *Router* mikrotik tersebut. Menurut narasumber, pelajar ataupun individu yang tidak bertanggung jawab tersebut mungkin hanya ingin mendapatkan kecepatan internet yang lebih tinggi atau akses internet gratis. Salah satu contoh kejadian yang terjadi adalah serangan DDOS pada *server*. Pada penelitian yang dilakukan oleh syahputra dalam penelitiannya yang berjudul “*Pemanfaatan Mikrotik Router Board Sebagai Pengaman Serangan Ddos Menggunakan Metode Ids tahun 2020*” dalam penelitian tersebut cara menanggulangi permasalahan serangan DDOS adalah dengan penambahan fitur *firewall filter* IDS.

Dari pembahasan sebelumnya, penulis memutuskan untuk melakukan penelitian proyek akhir di SMK PGRI 1 Nganjuk dengan judul "*Analisis Implementasi Port knocking Dengan Routing Dinamis Menggunakan Protokol Tcp Dan Icmp Studi SMK PGRI 1 Nganjuk*". Tujuan dari penelitian ini adalah untuk memberikan gambaran yang akurat tentang sistem jaringan dengan fokus pada keamanan. Metode *port knocking* akan digunakan dalam penelitian ini untuk meningkatkan proses analisis sistem

pada jaringan obyek penelitian. Kemudian lalu lintas jaringan akan dianalisa karena mengacu pada artikel yang dibuat oleh aldean tahun 2019 dalam penelitiannya yang menggunakan metode *port knocking* guna untuk memberikan pengamanan lalu lintas jaringan.

Pada penelitian ini langkah pertama yang akan dilakukan adalah pengumpulan informasi terkait permasalahan dan kondisi arsitektur jaringan di SMK PGRI Nganjuk. Dan langkah selanjutnya adalah menganalisa serta mencari jalan keluar dari permasalahan yang timbul. Setelah mendapatkan jalan keluar dari permasalahan yang timbul maka langkah selanjutnya dilakukan uji coba kelayakan. Uji coba ini diterapkan pada sebuah *prototype* guna untuk mengetahui apakah sudah efektif atau belum efektif sebelum diterapkan pada masalah yang sesungguhnya. Setelah proses implementasi pada masalah yang sesungguhnya langkah terakhir adalah memonitoring jalannya hasil implementasi dan terus di analisa guna untuk pengembangan dikemudian hari.

B. Identifikasi Masalah

Dari informasi di atas, fokus permasalahan ditujukan pada peningkatan keamanan jaringan di SMK PGRI 1 Nganjuk. Masalah yang teridentifikasi meliputi :

1. Kurangnya tindakan keamanan yang efektif terhadap serangan pada mikrotik *Router*, yang dapat terjadi baik *online* maupun *offline*. Dan masih rentannya mikrotik *Router* dari serangan dari dalam maupun luar.
2. Belum adanya penanganan yang tepat terhadap serangan DDOS.
3. .Rentannya sebuah *Router* terhadap serangan.

4. Masih banyak siswa atau orang lain yang mencoba merusak fasilitas umum

C. Rumusan Masalah

Berdasarkan latar belakang dan identifikasi masalah di atas, diperoleh rumusan masalah :

1. Bagaimana cara yang diambil guna untuk meningkatkan *Firewall* jaringan komputer pada lokasi penelitian supaya lebih kuat ?
2. Bagaimana membuat sebuah aturan mikrotik, agar tidak sembarangan orang bisa mengakses mikrtokit tersebut dan agar mirkrotik bisa tahan dari serangan DDOS ?
3. Cara menganalisa metode proteksi jaringan komputer pada aplikasi *Firewall* dengan menggunakan metode *port knocking*?
4. Bagaiman hasil sebelum dan sesudah setelah penerapan metode *port knocking* dan penerapan metode anti DDOS?
5. Apakah penerapan metode *port knocking* dan metode anti DDOS sudah efisien dalam penanganan permasalahan di SMK PGRI 1 Nganjuk ?

D. Batasan Masalah

Agar pembahasan tidak melenceng dari rencana semula, maka peneliti memfokuskan pada penerapan metode *port knocking* pada *Router* mikrotik sebagai berikut. :

1. Peneliti akan menerapkan *port knocking* pada *Router* board Mikrotik.

2. Hanya pengguna yang memenuhi aturan yang telah dibuat yang dapat mengakses port-port tertentu.
3. Metode *port knocking* yang dibuat khusus untuk SMK PGRI 1 Nganjuk.
4. Peneliti melakukan implementasi dengan menggunakan satu laptop.
5. Tahapan pengujian pengetukkan port, peneliti menggunakan sebuah aplikasi bawaan *windows* yaitu *Cmd* dan *port knocking client*.
6. Dalam tahap pengujian serangan DDOS dilakukan dengan menggunakan aplikasi LOIC (*Low Orbit Ion Cannon*). Router mikrotik yang digunakan dalam penelitian skripsi ini adalah Router RB951.
7. Tidak menampilkan konfigurasi dasar, penulisan skripsi ini berfokus pada *rules port knocking*.
8. Tidak menampilkan konfigurasi dasar, penulisan skripsi ini berfokus pada *rules* anti DDOS.
9. Penulis menggunakan metode NDLC dalam proses penelitian.

E. Tujuan Penelitian

Berdasarkan perumusan masalah yang telah disebutkan, tujuan dari penelitian ini adalah sebagai berikut:

1. Meningkatkan keamanan jaringan komputer yang ada dengan menggunakan metode *port knocking*.
2. Guna untuk mengurangi jumlah serangan komputer dengan

memperkenalkan metode *port knocking*.

3. Membuat aturan yang dapat diikuti oleh *administrator* jaringan untuk menentukan siapa saja yang berhak mengakses dan memasuki port tertentu.
4. Dengan metode penangkalan DDOS diharapkan bisa menangkal terjadinya penyerangan DDOS pada mikrotik pusat.
5. Menganalisis seberapa efisien penggunaan metode *port knocking* dalam penangamanan keamanan jaringan.
6. Menganalisis seberapa efisien penggunaan metode anti DDOS dalam penangamanan keamanan jaringan.
7. Dapat melindungi mikrotik dari serangan *hacker*.
8. Menguji kelamahan metode *port knocking* dalam keamanan jaringan.
9. Mengembangkan metode *port knocking*.

F. Manfaat Dan Kegunaan Penelitian

Untuk mencapai tujuan penelitian tersebut di atas, tugas akhir ini memiliki kelebihan dan tujuan sebagai berikut :

1. Memfasilitasi pertukaran informasi antar banyak organisasi tanpa mengkhawatirkan serangan hacker.
2. Memberikan solusi untuk mengamankan Mikrotik *Router OS* dan monitor jaringan komputer.
3. Informasi tentang sistem layanan yang optimal untuk diterapkan di lokasi penelitian ditambahkan.

4. Menggunakan ilmu yang diperoleh penulis dalam menyelesaikan tugas SMK PGRI 1 Nganjuk.
5. Izinkan pengguna mengotentikasi dirinya sendiri sebelum diberikan akses ke *server* pada perangkat jaringan.

G. Metode Penelitian

Teknik-teknik berikut digunakan untuk mencapai tujuan penelitian, terutama dalam mengumpulkan data dan informasi untuk mendukung proses penelitian :

1. Metode Teknik Kualitatif

Metode kualitatif deskriptif yaitu penelitian kualitatif yang menggambarkan fakta yang diperoleh dari sebuah data tanpa mengubah bentuk aslinya. Metode ini digunakan untuk mengumpulkan data dan menyusun laporan serta hasil akhir :

a. Metode Literatur

Metode ini digunakan dengan cara membaca buku, jurnal, referensi internet dan artikel terkait untuk menemukan temuan penelitian yang dapat mendukung dan referensi saat menulis penelitian ini.

b. Wawancara (*Interview*)

Wawancara adalah teknik pengumpulan data dengan mengajukan pertanyaan langsung untuk memperoleh informasi

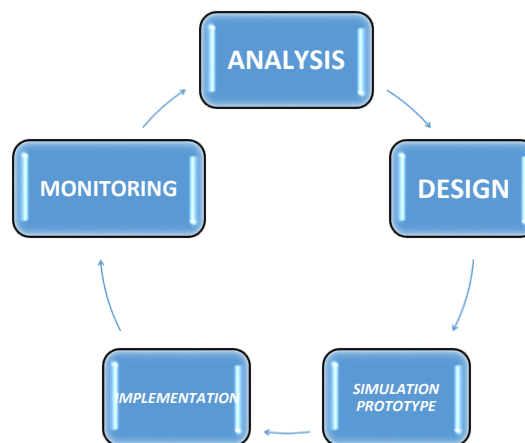
yang diperlukan. Informasi yang diperoleh dari hasil wawancara diolah kembali dalam penelitian.

c. Pengamatan (*Observasi*)

Merupakan teknik pengumpulan data secara langsung di SMK PGRI 1 Nganjuk. Hasil pengamatan membantu menentukan alat ukur yang tepat untuk digunakan.

2. Metode Pengimplementasian Sistem

Pengembangan sistem terkait pelaporan mengikuti metode NDLC (*Network Design Life Cycle*). Metode NDLC didasarkan pada fase pengembangan sebelumnya seperti perencanaan bisnis strategis, siklus hidup pengembangan aplikasi, dan analisis distribusi data. Dengan demikian, proses penelitian dapat dilakukan secara terstruktur dan terarah dan sistematis seperti terlihat pada gambar 1.1 :



Gambar 1.1 Proses tahapan penelitian NDLC

a. Analisis

Pada *fase* awal ini, kebutuhan dianalisis, masalah yang muncul dianalisis, keinginan pengguna dianalisis, dan *topologi* jaringan saat ini dianalisis. Beberapa metode yang biasa digunakan dalam langkah ini antara lain :

- 1) Wawancara dengan pihak-pihak terkait mulai dari manajemen puncak hingga level bawah atau operator untuk mendapatkan informasi yang spesifik dan komprehensif.
- 2) Survei atau observasi langsung di lapangan, tahap analisis ini seringkali mencakup pemetaan langsung di lapangan untuk mendapatkan hasil nyata dan gambaran umum sebelum tahap perencanaan.
- 3) Meneliti data yang diperoleh dari masing-masing data sebelumnya sehingga diperlukan analisis data untuk mencapai langkah selanjutnya. Beberapa pedoman yang dapat digunakan untuk mencari data dalam tahap analisis ini antara lain :

a) Pengguna

Jumlah *client*, Status pengguna jaringan yang ada pada tempat penelitian yaitu SMK PGRI 1 Nganjuk.

b) Perangkat

Perangkat yang digunakan di lokasi penelitian, kondisi perangkat jaringan, ketersediaan *database*

tentang laporan perbaikan alat, laporan upgrade dan laporan permasalahan yang sering timbul.

c) Jaringan

Penataan jaringan, jumlah lalu lintas jaringan, *standart* komunikasi, pemantauan jaringan yang sedang berjalan, harapan dan rencana pengembangan ke depan.

d) Perencanaan *Hardware*

Keterbatasan listrik, tata letak fisik, ruang khusus, sistem keamanan yang sedang berjalan dan kemungkinan pengembangan di masa depan.

b. Desain

Berdasarkan informasi yang telah dikumpulkan sebelumnya, langkah desain ini bertujuan untuk menyiapkan diagram proyek *topologi* jaringan koneksi yang akan dibangun. Semoga gambaran ini memberikan gambaran lengkap tentang kebutuhan SMK PGRI 1 Nganjuk.

c. Simulasi *Prototype*

Perancangan sistem pada SMK PGRI 1 Nganjuk dilakukan melalui tahap simulasi dengan memanfaatkan alat bantu paket tracer untuk merancang *topologi* yang diusulkan.

d. Implementasi

Proses implementasi menggunakan spesifikasi desain sebagai *input* untuk menghasilkan instruksi implementasi sistem

yang sebenarnya selama *fase prototype* simulasi. Tahapan ini terdiri dari dua bagian yaitu konfigurasi dan analisis yang meliputi perancangan *topologi* jaringan serta pemasangan dan konfigurasi komponen di SMK PGRI 1 Nganjuk.

e. Monitoring

Selain itu, memastikan kinerja sistem konsisten dengan keinginan dan tujuan awal, penulis melakukan monitoring atau pengawasan terhadap efektivitas jaringan komputer dan komunikasi pada tahap awal analisis.

H. Jadwal Penelitian

Tabel 1.1 Rencana Penelitian

No	Kegiatan	Bulan																							
		Bulan-1				Bulan-2				Bulan-3				Bulan-4				Bulan-5				Bulan-6			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	<i>Library Research</i>	■	■	■																					
2	<i>Observasi</i>		■	■	■																				
3	<i>Interview</i>		■	■	■	■																			
4	Perancangan sistem				■	■	■	■	■	■	■	■	■												
5	Implementasi sistem											■	■	■	■	■	■								
6	Uji coba													■	■	■	■	■	■	■	■	■	■	■	■
7	Laporan																				■	■	■	■	■

I. Sistematika Penulisan Laporan

Penulisan tugas akhir ini disajikan dengan sistem sebagai berikut :

1. BAB I : PENDAHULUAN

Menjelaskan kesenjangan antara teori dan praktik, atau kesenjangan antara harapan dan kenyataan, untuk memberi kesan bahwa ada masalah yang perlu ditangani. Meneliti hal-hal yang terbaik dalam konteks suatu masalah yang dapat meningkatkan pelayanan bagi mahasiswa.

2. BAB II : TINJAUAN PUSTAKA

Merupakan landasan teori atau dasar pemikiran penyusunan laporan akhir ini, termasuk proses analisis, perancangan dan implementasinya. Bab ini juga menjelaskan metode yang digunakan dalam penelitian.

3. BAB III : ANALISIS DAN PERANCANGAN

Deskripsi objek penelitian atau kegiatan yang akan dilakukan. Berisi tentang gambaran kondisi objek penelitian atau konfigurasi jaringan pada saat dilakukan survei sebelum dilakukan survei.

4. BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Penjelasan tentang objek investigasi atau kegiatan yang akan dilakukan, termasuk kondisi objek investigasi atau konfigurasi jaringan sebelum dilakukan investigasi. Penjelasan penanganan data dan analisa sistem *Firewall* menggunakan metode *port knocking* dan anti-DOOS pada Mikrotik *Router OS*.

5. BAB V : PENUTUP

Bab ini merupakan bab terakhir yang berisi keinginan dan harapan peneliti demi kelancaran pelaksanaan penelitian.

BAB II

TINJAUAN PUSTAKA

A. Dasar Teori

Isi ringkasan mengenai dasar teori dan *review* literatur yang mencakup prinsip-prinsip ilmiah yang mendukung pembahasan penelitian yang akan dilakukan.

1. Analisis

Pengertian analisa adalah serangkaian kegiatan seperti memecah sesuatu, memisahkannya, mengelompokkannya kembali menurut kriteria tertentu, dan kemudian mencari hubungan dan menafsirkan maknanya. Analisa juga dapat diartikan sebagai upaya untuk mengamati sesuatu secara cermat, memecahnya menjadi komponen-komponennya atau mengorganisasikan komponen-komponen tersebut untuk dipelajari lebih lanjut. (Menurut Wiradi (2006:103))

Sebagian orang menganggap analisa sebagai kemampuan untuk merangkum informasi menjadi bagian-bagian yang lebih kecil agar lebih mudah dipahami dan dijelaskan.

Menurut Harahap (Azwar, 2019), pengertian analisa adalah sebagai berikut:

Memecahkan atau menguraikan sesuatu unit menjadi unit terkecil. Dari pendapat diatas dapat ditarik kesimpulan bahwa analisis merupakan suatu kegiatan berfikir untuk menguraikan

atau memecahkan suatu permasalahan dari unit menjadi unit terkecil.

2. Lalu Lintas Komputer

Jaringan komputer adalah jaringan komunikasi yang memungkinkan komputer untuk berkomunikasi satu sama lain dengan bertukar data. Tujuan dari jaringan komputer adalah agar setiap bagian dari jaringan komputer dapat meminta dan menyediakan layanan dan dengan demikian mencapai tujuannya.(Wikipedia.org)

menurut Melwin Syafrizal, (Syafrizal, 2020) adalah sebagai berikut :

Jaringan komputer adalah (*interkoneksi*) antara 2 komputer *autonomous* atau lebih, yang terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). *Autonomous* adalah apabila sebuah komputer tidak melakukan control terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, restart, shutdowns, kehilangan file atau merusakkan sistem.

a. Jaringan Komputer Berdasarkan Kelompoknya

Jaringan komputer terdiri dari beberapa komputer yang terhubung ke komputer lain dengan kabel atau nirkabel (*wireless*). Jenis jaringan yang umum digunakan adalah (bhinneka.com) :

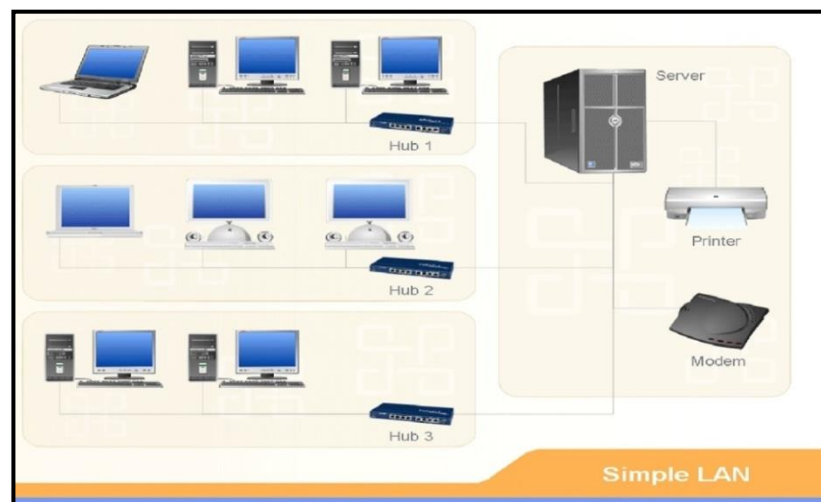
1) LAN (*Local Area Network*)

Jaringan area lokal (LAN) adalah lalu lintas yang dihasilkan di area tertentu, seperti gedung atau ruangan. Jaringan area lokal, terkadang disebut jaringan pribadi atau

pribadi, digunakan dalam jaringan kecil yang berbagi sumber daya seperti printer, media bersama, dan media bersama.

Menurut Kumala Dewi, Arman Syah (2021) definisi LAN adalah sebagai berikut :

LAN menggambarkan suatu jaringan yang menjangkau area yang terbatas, misalnya satu kantor satu gedung, di mana komputer yang mempunyai jaringan fisik berdekatan atau dengan lainnya. Biasanya antar *node* tidak jauh dari sekitar 200 meter, seperti pada gambar 2.1.



Gambar 2.1 Jaringan LAN
(Sumber : dokumen.tips)

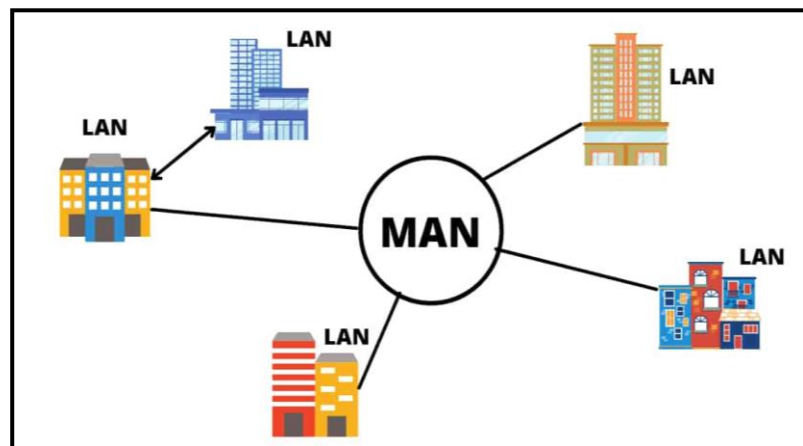
Dari gambar 2.1 menjelaskan sekumpulan komputer, dan laptop serta printer yang terhubung pada sebuah *switch* dengan menggunakan kabel *twisted pair* sebagai penghubung.

2) MAN (*Metropolitan Area Network*)

Metropolitan Area Network (MAN) menggunakan metode yang sama dengan LAN, tetapi memiliki jangkauan

yang lebih luas. MAN dapat mencakup satu RW, beberapa kantor dalam satu kompleks atau satu atau lebih desa. MAN adalah perpanjangan dari jaringan area lokal dengan kecepatan transmisi yang lebih tinggi dan jangkauan yang lebih luas, yang dapat terdiri dari dua atau lebih jaringan area lokal yang terhubung dalam batas kota besar atau kota kecil.

Jarak maksimum yang dapat dijangkau MAN adalah sekitar 80 kilometer, dan hanya satu atau dua kabel yang digunakan untuk menangani paket data pada kabel keluaran di dalamnya. Ada dua koneksi yang sering digunakan untuk menghubungkan MAN, yaitu wireless dan kabel fiber optic.



Gambar 2.2. Jaringan *Metropolitan Area Network*
(Sumber : morning.computer)

Gambar 2.2 menjelaskan gambaran sederhana dari sebuah topologi MAN yang dimana topologi MAN adalah sekumpulan dari topologi LAN yang saling terhubung menjadi

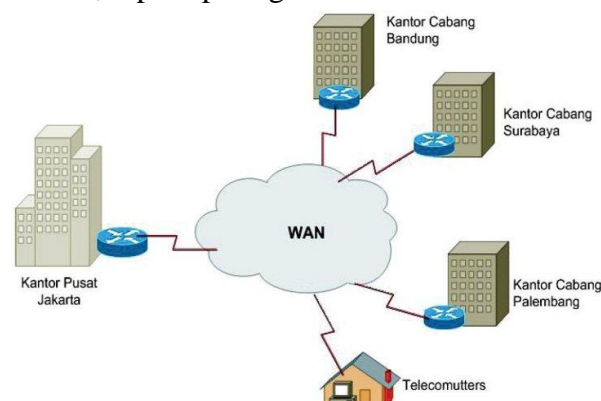
satu dan saling berhubungan.

3) WAN (*Wide Area Network*)

Wide area network (WAN) adalah jaringan yang lebih luas dari MAN, mencakup satu wilayah, satu negara, satu pulau, dan bahkan satu dunia. Metode yang digunakan WAN hampir sama dengan LAN dan MAN yang biasanya terhubung dengan jaringan telepon digital. Namun, pemancar lain juga bisa digunakan. WAN digunakan untuk menghubungkan satu jaringan area lokal ke jaringan area lokal lainnya sehingga pengguna atau komputer di satu lokasi dapat berkomunikasi dengan pengguna dan komputer di lokasi lain.

Mengutip dari Selmatpagi.id (2020:1) definisi WAN adalah sebagai berikut :

WAN adalah jaringan yang jangkauan area geografik paling luas, bisa antar pulau, negara, benua, bahkan bisa keluar angkasa. WAN biasanya sudah menggunakan media *wireless*, sarana satelit, ataupun kabel serat *optic*, karena jangkauannya yang lebih luas. Contoh terbaik dan sangat terkenal adalah Internet, seperti pada gambar 2.3.



Gambar 2.3. Skema *topologi Wide Area Network*
(Sumber: arduinoindonesia.id)

Gambar 2.3 menjelaskan skema dari topologi jaringan WAN. Yang dimana topologi WAN merupakan kumpulan dari topologi MAN yang terhubung dengan menggunakan perantara jaringan wireless dan serta kabel *twisted pair*. Topologi WAN juga bisa saling berbagi data serta saling terkoneksi satu sama lainnya dalam media internet.

b. Jaringan Komputer Berdasarkan Fungsi

Menurut bambang (2021) pada bukunya Pengenalan dasar dunia jaringan komputer, jenis jaringan komputer yaitu :

1) *Client Server*

Suatu sistem jaringan komputer dimana satu komputer bertindak sebagai *server* atau induk bagi komputer lain yang disebut *client*. *Server* menyediakan layanan seperti akses web, email, file atau lainnya. *Server client* sering digunakan di internet, tetapi jaringan lokal atau jaringan lain juga dapat mengimplementasikan *server client* sesuai dengan kebutuhan masing-masing pengguna.

2) *Peer To Peer*

Jaringan komputer juga dapat berupa jaringan *peer to peer*, dimana setiap komputer dapat menjadi *server* sekaligus *client*. *Peer to peer* banyak diimplementasikan di jaringan

lokal, meskipun bisa juga diimplementasikan di MAN, WAN atau Internet. Namun, hal ini kurang umum karena masalah administratif dan keamanan yang sulit dipertahankan dalam jaringan *peer to peer* dengan banyak pengguna.

Pengertian jaringan komputer adalah sekumpulan komputer yang saling terhubung satu sama lain melalui suatu protokol komunikasi melalui suatu media transmisi dalam suatu jaringan komunikasi untuk tujuan tertentu.

3. *Topologi Jaringan*

Menurut Melwin Syafrizal (2020:39) penjelasan tentang *topologi* jaringan adalah sebagai berikut :

Topologi jaringa atau arsitektur jaringan adalah gambaran perencanaan hubungan antar komputer dalam LAN yang umumnya menggunakan kabel (sebagai media transmisi), dengan konektor, ethernet card, dan perangkat pendukung lainnya.

Setelah mengetahui *topologi* jaringan, kita dapat melakukan *maintenance* jaringan dengan lebih mudah dan efisien. Beberapa *topologi* jaringan yang lebih umum digunakan adalah bus, ring, star dan mesh.

a. *Topologi Bintang*

Menurut pendapat Melwin Syafrizal (2020:41) *topologi*

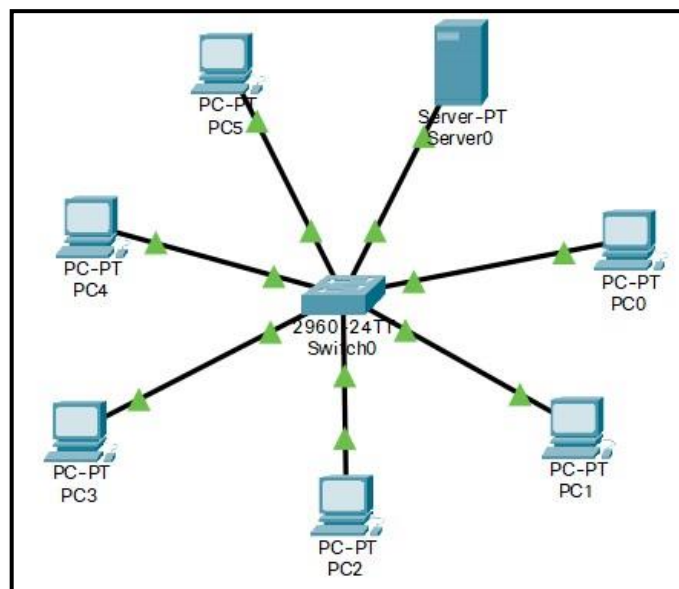
Ring adalah :

Topologi Star, masing-masing *Workstation* dihubungkan secara langsung ke *Server* atau *Hub* atau *Swich*. Hub atau *Swich* berfungsi menerima sinyal-sinyal dari komputer dan

meneruskannya ke semua komputer yang terhubung dengan *Hub* atau *Swich* tersebut. Jaringan dengan *Topologi* ini lebih mahal dan cukup sulit pemasangannya. Setiap komputer mempunyai kabel sendiri-sendiri sehingga lebih mudah dalam mencari kesalahan pada jaringan. Kabel yang digunakan biasanya menggunakan Kabel UTP CAT5, seperti pada gambar di bawah ini.

Topologi *star* merupakan salah satu jenis dari topologi jaringan komputer, yakni struktur geometri sebuah jaringan komputer. Topologi *star* memiliki kekurangan dan kelebihan. Kekurangan topologi *star* yang utama terletak pada penggunaan kabel dalam pembuatan jaringan.

Sementara itu, kelebihan topologi *star* yang utama adalah apabila salah satu komputer mengalami kerusakan, jaringan tidak bermasalah dan tetap berjalan. Topologi *star* menggunakan piranti sentral bernama *hub* yang menjadi peralatan pusat jaringannya.



Gambar 2.4. *Topologi Star*

Pada topologi 2.4, masing-masing komputer pada jaringan dihubungkan ke sebuah *hub* menggunakan kabel *twisted pair*, membentuk susunan yang serupa dengan sebuah bintang.

4. **Keamanan Jaringan**

Tujuan dari keamanan jaringan adalah untuk menyediakan jalur yang aman antara pihak yang bertukar informasi dan untuk melindungi informasi dari upaya orang yang tidak berwenang untuk mengumpulkan, mengubah, menggunakan, menonaktifkan, dan menghancurkan informasi. Ini penting untuk melindungi sumber daya dan data yang berharga dari potensi serangan dan ancaman.

5. **Metode Pengamanan Jaringan**

Menurut Wajong (2022) definisi pengamanan jaringan adalah sebagai berikut :

Mengamankan jaringan komputer membutuhkan tiga tingkatan proses utama, yaitu *prevention* (pencegahan), *observation* (observasi) dan *response* (respon).

a. **Pencegahan (*Prevention*)**

Sebagian besar ancaman mudah dihindari, meskipun keamanan lengkap tidak selalu memungkinkan. Akses yang tidak diinginkan ke jaringan komputer dapat dihindari dengan memilih dan mengonfigurasi layanan pekerjaan.

b. Observasi (*Observation*)

Jika jaringan komputer berfungsi dan akses yang tidak diinginkan dikecualikan, pemeliharaan jaringan harus mencakup pemeriksaan *log* yang tidak biasa yang mungkin mengindikasikan tidak adanya masalah keamanan.

c. Respon (*Response*)

Jika terjadi hal yang tidak diinginkan serta *Firewall* sistem ditembus, personel perawatan harus segera melakukan tindakan. Oleh karena itu, rencana perawatan harus dipertimbangkan dengan cermat. Ini menjadi sulit karena tidak ada yang tahu dengan pasti celah apa yang telah dimanfaatkan oleh pihak luar setelah sistem berhasil ditembus.

6. *Port Knocking*

Port knocking adalah sistem keamanan yang bertujuan untuk membuka atau menutup akses ke port tertentu menggunakan *Firewall* perangkat jaringan dengan mengirimkan paket atau koneksi tertentu. Koneksi dapat berupa protokol TCP, UDP atau ICMP. Untuk mendapatkan akses terhadap port terbatas tertentu, pengguna harus memasukkan aturan dengan mengetuk terlebih dahulu. Hanya penyedia layanan internet yang mengetahui aturan ini.

Menurut Amirudin (2018) definisi *port knocking* adalah sebagai berikut :

Port knocking merupakan suatu sistem keamanan yang bertujuan untuk membuka atau menutup akses *block* ke *port* tertentu dengan menggunakan *Firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protokol TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), maupun ICMP (*Internet Control Message Protocol*) sehingga untuk masuk dan menggunakan akses ke *port* tertentu yang telah dibatasi.

Maka *user* harus mengetuk terlebih dahulu dengan memasukkan *rule* yang harus dilakukan terlebih dahulu. *Rule* yang dimana hanya diketahui oleh pihak *administrator* jaringan. Sebuah sistem harus memiliki keseimbangan antara keamanan dan fleksibilitas. Salah satu cara untuk mencapai sistem seperti demikian yaitu dengan menggunakan akses *Firewall*. Dengan *Firewall* maka secara langsung kita dapat mendefinisikan *user* yang dapat dipercaya dan yang tidak dipercaya dengan menggunakan alamat IP sebagai kriteria.

7. Bentuk serangan pada jaringan

Menurut Kompirasi Media (2022) bentuk serangan pada jaringan adalah sebagai berikut :

Kegiatan dan hal-hal yang membahayakan keamanan jaringan antara lain adalah sebagai berikut :

a. Probe

Probing, atau sering disebut *security testing*, merupakan upaya untuk membobol suatu sistem atau memperoleh informasi tentang suatu sistem. Contoh sederhana pengujian keamanan adalah masuk ke akun yang tidak digunakan. *Probing* dapat disamakan dengan mencari kenop pintu yang tidak terkunci agar mudah masuk.

b. Scan

Pemindaian adalah sejumlah besar pengujian keamanan data dengan alat. Pemindaian biasanya merupakan pendahuluan untuk mengarahkan serangan terhadap sistem yang rentan terhadap penyerang.

c. Packet Sniffer

Packet Sniffer adalah program yang mengumpulkan data dari paket yang melewati jaringan. Informasi tersebut dapat mencakup nama pengguna, kata sandi, dan informasi sensitif lainnya yang dikirimkan melalui jaringan dalam teks yang jelas. Paket yang ditangkap tidak hanya satu, tetapi bisa ribuan, yang

berarti penyerang bisa mendapatkan ribuan nama pengguna dan kata sandi.

d. Denial of Service (DOS)

Denial of service adalah metode serangan yang bertujuan untuk menghabiskan sumber daya perangkat jaringan komputer sedemikian rupa sehingga layanan jaringan komputer terganggu. Salah satu bentuk serangan ini adalah serangan banjir *ping*, yang mengeksploitasi kelemahan dalam sistem *three way handshake*.

8. Metode *Port Knocking*

Port knocking digunakan untuk membuka akses ke port tertentu yang diblokir oleh *Firewall* perangkat jaringan dengan mengirimkan paket atau koneksi tertentu. Koneksi dapat berupa protokol TCP, UDP atau ICMP. Jika koneksi yang dikirim oleh *host* mengikuti aturan penyadapan yang telah ditentukan sebelumnya, *Firewall* secara dinamis memberikan akses ke port yang sebelumnya diblokir. Dengan menggunakan teknologi ini, perangkat jaringan seperti *Router* lebih aman.(Citraweb.com)

Ini karena *administrator* jaringan dapat memblokir port yang rentan terhadap serangan, seperti Winbox (tcp 8291), SSH (tcp 22), *Telnet* (tcp 23) atau webfig (tcp 80). Setelah pemindaian port selesai, port tampak tertutup.

9. *Firewall*

Firewall adalah mekanisme yang diimplementasikan dalam perangkat keras, perangkat lunak, atau sistem itu sendiri yang bertujuan untuk melindungi jaringan pribadi dari koneksi yang tidak diinginkan ke jaringan eksternal di luar jangkauannya. Segmen yang

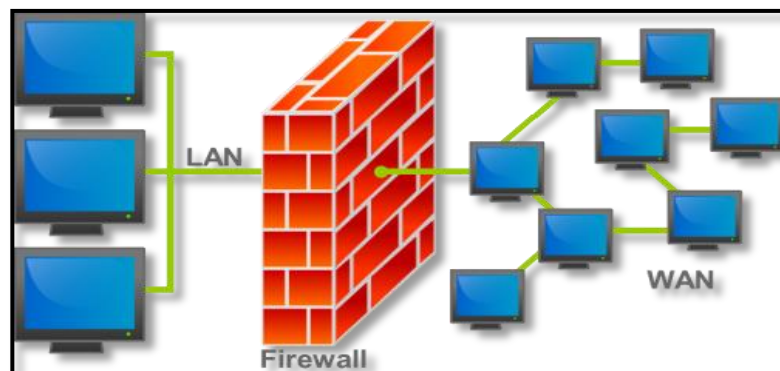
dilindungi dapat berupa *workstation*, *server*, *Router*, atau jaringan area lokal (LAN). *Firewall* dapat memfilter, membatasi, atau memblokir koneksi segmen di jaringan pribadi.(kominfo.go.id)

a. Fitur-fitur *Firewall* meliputi:

- 1) Filter paket statis.
- 2) Filter paket dinamis.
- 3) Filter paket berdasar keadaan *proxy*.

b. Karakteristik *Firewall*

- 1) Semua koneksi atau operasi dari dalam ke luar harus melalui *Firewall*. Ini dapat dicapai dengan memblokir atau membatasi akses ke jaringan lokal kecuali melalui *Firewall*. Jaringan yang berbeda mengizinkan pengaturan ini.
- 2) Hanya fungsi yang terdaftar atau dikenali yang dapat lewat atau terhubung. Ini dapat dilakukan dengan menetapkan kebijakan di pengaturan keamanan lokal. Ada berbagai jenis *Firewall* untuk dipilih dan juga aturan yang berbeda.
- 3) *Firewall* harus tahan lama atau cukup kuat untuk menyerang atau melemahkan. Artinya menggunakan sistem yang dapat



dipercaya dan relatif aman.

Gambar 2.5. Skema *Firewall* Pada Jaringan
(Sumber : yuliatwn.wordpress.com)

Pada Gambar 2.5 bisa terlihat sebuah skema *firewall* bahwa jaringan lokal harus melewati sebuah *firewall* guna guna untuk membatasi jaringan LAN atau jaringan lokal yang hendak mengakses jaringan yang lebih luas yaitu jaringan WAN dan internet.

10. NAT

NAT, kependekan dari *Network Address Translation*, yaitu menerjemahkan satu atau lebih alamat IP ke alamat IP lain, IP yang diterjemahkan adalah alamat IP yang ditetapkan untuk setiap mesin di jaringan internal, alamat IP yang diterjemahkan berada di luar jaringan internal dan ilegal.(Wikipedia.org)

Secara singkat *network address translation* ini memungkinkan perangkat mengakses internet melalui satu alamat publik melalui penerjemahan alamat IP pribadi ke IP publik.

Menurut Trivusi (2022), *Network Address Translation* (NAT) adalah :

NAT (*Network Address Translation*) adalah protokol yang digunakan untuk menghubungkan dua jaringan komputer dan memetakan *private address* (cakupan lokal) ke *public address* (cakupan global). Dengan kata lain, NAT adalah metode untuk mengubah alamat IP pribadi atau alamat lokal menjadi alamat IP publik. NAT berguna untuk menjaga agar alamat IP yang

tersedia tidak cepat habis dengan menerjemahkan IP lokal atau alamat IP pribadi menjadi alamat IP global atau publik.

11. TCP/IP

Transmission Control Protocol, atau *Internet Protocol*, lebih dikenal dengan TCP/IP, adalah standar komunikasi yang digunakan oleh komunitas Internet untuk bertukar informasi dari satu komputer ke komputer lain di Internet. (Wikipedia.org)

Menurut Trivusi (2022), dijelaskan bahwa TCP/IP (*Transmission control protocol* atau *Internet protocol*) adalah :

Merupakan *protocol* yang masing-masing bertanggung jawab atas bagian-bagian tertentu *protocol* yang satu tidak perlu mengetahui cara kerja *protocol* lainnya dalam proses pengiriman dan penerimaan data).

Arsitektur komputer model TCP/IP memiliki 4 layer kumpulan *protocol* yang bertingkat, yaitu :

a. Layer I Network Access

Lapisan pertama, yaitu koneksi jaringan, bertanggung jawab untuk mengirim dan menerima data melalui sarana fisik seperti kabel, serat optik, atau gelombang radio.

Beberapa contoh protokol pada lapisan ini adalah Ethernet, X25, dan SLIP (*Serial Line Internet Protocol*). Lapisan kedua, yaitu lapisan Internet, bertanggung jawab mengirimkan paket data ke alamat yang benar.

b. Layer 2 Internet

Protokol lapisan ini terdiri dari tiga jenis: IP (*Internet Protocol*), yang bertanggung jawab untuk meneruskan paket data ke alamat yang benar, ARP (*Address Resolution Protocol*), yang bertanggung jawab untuk menemukan alamat perangkat terminal dan hanya terletak di jaringan yang sama, dan ICMP (*Internet Control Message Protocol*), yang memantau pengiriman pesan dan melaporkan gangguan dalam pengiriman data.

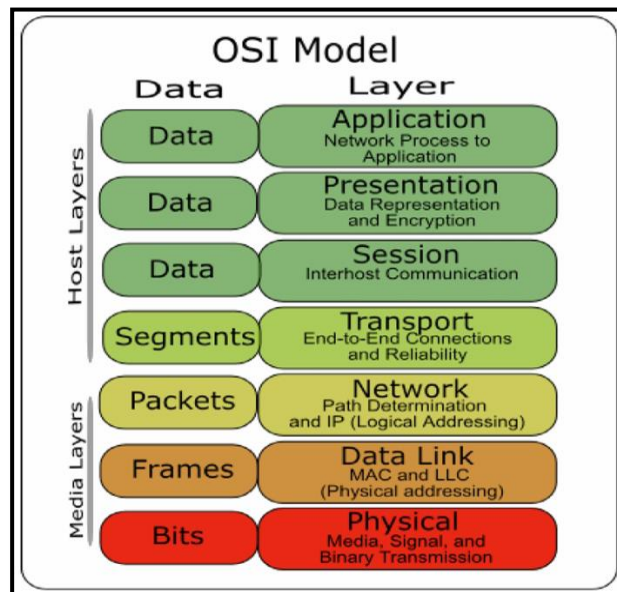
c. Layer 3 Transport

Lapisan transport berperan dalam memastikan transfer data antara dua perangkat akhir. Terdiri dari dua bagian yaitu :

- 1) TCP (*Transmission Control Protocol*)
- 2) UDP (*User Datagram Protocol*)

d. Layer 4 Application

Semua aplikasi seperti SMTP, FTP dan HTTP disimpan di dalam aplikasi dan langsung dapat diakses dari program aplikasi seperti yang ditunjukkan pada gambar 2.6 tentang model layer OSI.



Gambar 2.6. OSI Model (Kiri) dan *TCP/IP* Model (Kanan)
(Sumber : id.wikipedia.org)

Gambar 2.6 memperlihatkan susunan dari sebuah aturan baku dalam kerangka logika struktur komunikasi dan interaksi jaringan internet yaitu model layer OSI (*Open System Interconnection*).

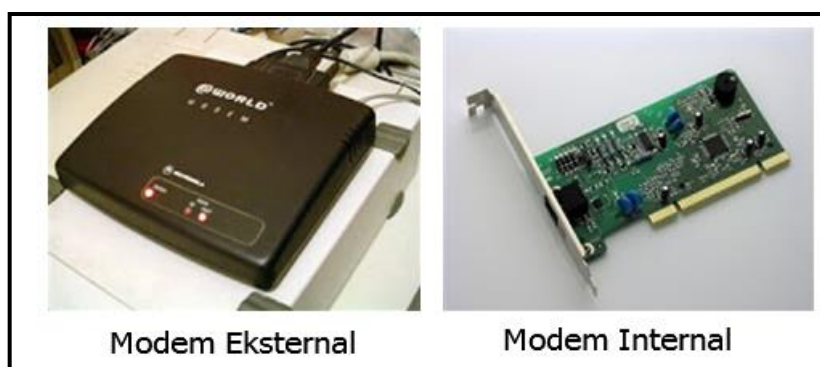
12. Unit Dan Alat Jaringan

Dari perspektif teknis, jaringan komputer menggunakan sejumlah alat. Alat-alat dalam jaringan komputer saling berhubungan dan tidak dapat dipisahkan satu sama lain, yaitu:

a. Modem

Modem berasal dari kata *Modulator Demodulator*. Modem berfungsi mengubah sinyal komputer digital (aliran data) menjadi sinyal analog (sinyal telepon) dan sebaliknya. Modem sering digunakan untuk menghubungkan komputer ke Internet.

Komputer yang terhubung ke Internet terhubung ke saluran telepon melalui modem. Ada modem yang terpasang di komputer (modem *internal*) dan juga tersedia terpisah dari komputer (modem *eksternal*), seperti terlihat pada gambar 2.7.



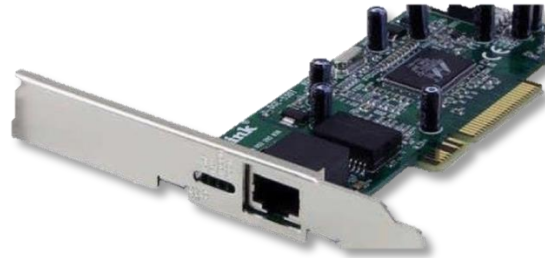
Gambar 2.7. Modem *Internal* dan Modem *External* (ADSL)
(Sumber : irmaningsihblog.wordpress.com)

Gambar 2.7 memperlihatkan bentuk dari *interface* sebuah modem. Dari gambar sebelah kiri melihatkan modem dalam bentuk *eksternal* yang penggunaanya sudah simple dan gambar sebelah kiri menunjukkan bentuk modem *internal* yang bisa terpasang langsung kedalam sebuah komputer melalui slot PCI *Express*.

b. NIC (*Network Interface Card*)

NIC atau kartu jaringan, juga dikenal sebagai kartu LAN atau kartu antarmuka jaringan, bertindak sebagai penghubung antara komputer dan jaringan komputer. NIC terdiri dari dua jenis yaitu *physical* dan *logical* NIC. Contoh NIC fisik adalah Ethernet

dan Token Ring, sedangkan NIC logis adalah adaptor loop dan NIC *dial-up*.



Gambar 2.8. *LAN Card*
(Sumber : www.eduprimer.com)

Gambar 2.8 memperlihatkan tampilan *interface* dari sebuah *LAN Card*. Dalam penggunaannya *LAN Card* terpasang dalam sebuah komputer melalui slot PCI akan tetapi beberapa komputer terkadang sudah terpasang *LAN Card* yang sudah ditanamkan pada mesin atau *mainboard* sebuah komputer.

c. **Switch**

Switch menghubungkan semua komputer di jaringan sebagai *hub*. Perbedaannya adalah *switch* dapat beroperasi dalam mode *dupleks* penuh dan merutekan data ke tujuan tertentu. *Switch* hanya dapat mengirim paket data ke port penerima yang dimaksud berdasarkan informasi di *header* paket. Sakelar membuat tautan sementara antara sumber dan tujuan untuk mengisolasi transmisi dari port lain.



Gambar 2.9. *Switch*
(Sumber : www.temukanpengertian.com)

Gambar 2.9 memperlihatkan tampilan *interface* dari sebuah *Switch*. Dalam *Hub* biasanya memiliki 4 hingga 12 jalur koneksi atau *port*. Sedangkan *Switch*, jumlah *port*-nya bisa lebih banyak, yaitu berkisar antara 24 hingga 48 port.

d. Router

1) Pengertian Router

adalah perangkat yang lebih pintar daripada *hub* dan *switch*. *Router* dapat menampilkan rute dan memfilter informasi pada jaringan yang berbeda. *Router* dapat mendeteksi masalah dan mengalihkan jalur data dari area masalah. *Router* menggunakan tabel *routing* untuk menentukan *Router* atau *workstation* mana yang akan menerima paket berdasarkan alamat lengkap paket tersebut.

Router memastikan bahwa paket mencapai tujuannya melalui rute yang paling efisien. Jika link antara dua *Router* gagal, pengirim dapat memilih rute alternatif. *Router* juga menyediakan tautan antar jaringan menggunakan protokol yang berbeda. Jenis-jenis *Router* :

a) Aplikasi

Jenis ini dapat diinstal sebagai aplikasi sistem operasi, dalam hal ini sistem operasi memiliki fitur seperti *Router*. Beberapa contoh aplikasi yang digunakan adalah *Win Route*, *Win Gate*, *Spy Gate* dan *Win Proxy5* dan masih banyak aplikasi lainnya.

b) Perangkat Keras

Beberapa contoh dari *Router* perangkat keras ini adalah Mikrotik *Router*, Cisco.

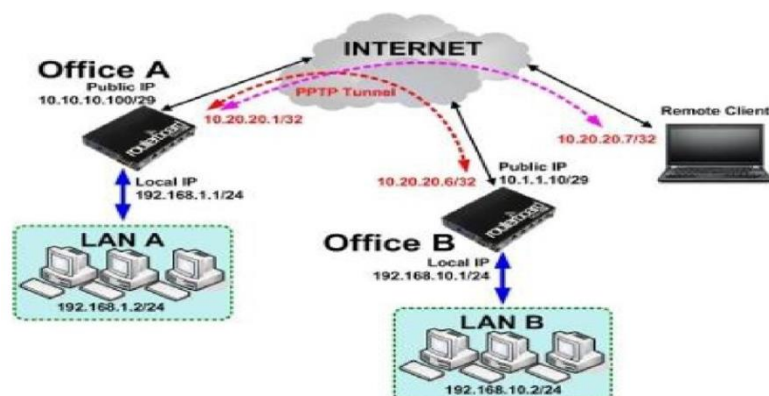
c) PC Router

Sistem operasi yang dilengkapi dengan kemampuan untuk menetapkan dan mengelola alamat IP memungkinkan perangkat jaringan seperti komputer atau komputer yang terhubung memperoleh alamat IP. Sistem operasi yang cocok untuk ini adalah berbasis *client-server*. Salah satu contoh *Router* jenis ini adalah Mikrotik *RouterOS*.

2) Cara Kerja Router

Perangkat router adalah perangkat yang meneruskan paket IP dari satu jaringan ke jaringan lain menggunakan metode dan protokol pengalamatan khusus untuk mengirim paket data. *Router* memiliki kemampuan untuk meneruskan paket IP dari satu jaringan ke jaringan lain, yang mungkin memiliki banyak jalur di antaranya.

Perangkat referensi yang terhubung ke internet bekerja sama dalam algoritma routing terdistribusi untuk menentukan rute terbaik bagi paket IP untuk melakukan perjalanan dari satu sistem ke sistem lainnya. Proses *forwarding* bersifat *hopping*, dimana IP tidak mengetahui jalur umum ke tujuan masing-masing paket.



Gambar 2.10. Gambar *Router dan Simulasinya*
(Sumber : citraweb.com)

Gambar 2.10 menjelaskan fungsi dan simulasi dari penggunaan router. Yang dimana dari kantor A yang memiliki jaringan lokal dibawahnya terhubung melalui

sebuah router ke kantor B yang juga memiliki jaringan lokal dibawahnya. Dan dari komunikasi itu router juga bisa di akses client dengan sistem *remote* yang telah diberikan akses.

e. Access Point

Access Point adalah perangkat yang menjadi pusat komunikasi dari pelanggan ke penyedia layanan jaringan, atau dari kantor cabang ke kantor pusat jika jaringan dimiliki oleh perusahaan. Tugasnya adalah mengubah sinyal frekuensi radio menjadi sinyal digital yang dikirim melalui kabel atau diarahkan ke perangkat WLAN lain, mengubahnya kembali menjadi sinyal frekuensi radio yang ditunjukkan seperti pada gambar 2.11.



Gambar 2.11. *Access Point*
(Sumber : www.ebay.com)

Gambar 2.11 memperlihatkan tampilan *interface* dari sebuah *Access Point*. Menurut fungsinya *Access Point* digunakan untuk menyebarkan sebuah signal dengan frekuensi tertentu serta cakupan area tertentu tergantung dari jenis *Access Point* yang

digunakan. Dan dalam berkembangnya jaman saat ini signal *Access Point* sudah mencapai kecepatan 5G.

13. Mikrotik

MikroTik adalah sebuah *operating system* yang dalam penggunaannya digunakan untuk mengubah personal komputer menjadi sebuah *Router* jaringan.

Menurut Amarudin & Atri (2018) dijelaskan dalam jurnal ilmiah mereka definisi mikrotik adalah :

Perangkat jaringan komputer yang berupa *hardware* dan *software* yang dapat difungsikan sebagai . Dan *software* yang difungsikan sebagai , sebagai alat *filtering*, *switching* maupun yang lainnya. Adapun *hardware* Mikrotik biasa berupa *PC* yang di *install* pada *PC* maupun berupa *Board* (sudah dibangun langsung dari perusahaan Mikrotik). Sedangkan *software* Mikrotik atau yang dikenal dengan nama *OS* ada beberapa versinya.

Perusahaan Mikrotik memiliki beberapa jenis produk yang di tawarkan diantaranya, yaitu :

a. Mikrotik Router OS

Mikrotik *Router OS* adalah platform UNIX yang dapat mengubah komputer biasa menjadi *Router*, *Firewall*, *bridge*, *hotspot* atau *server proxy* dan banyak lagi. Karena kemudahan penggunaannya, banyak orang memilih OS ini untuk membangun *Router* mereka.

b. Router Board

Namun, *Router Board* adalah perangkat keras jaringan yang diproduksi oleh Mikrotik. Sistem operasi Mikrotik *RouterOS* diinstal pada *Router Board*. Terlepas dari perangkat kerasnya, *Router Board* sangat kecil dan mudah digunakan.

14. Ip Address

Alamat IP adalah bagian dari Internet yang bertanggung jawab untuk mengirimkan informasi melalui jaringan. Setiap komputer *host* di Internet memiliki alamat identifikasi yang terdiri dari urutan angka biner 32-128-bit. Angka-angka ini menunjukkan alamat komputer di Internet berdasarkan protokol TCP/IP. IPv4 panjangnya 32 bit, sedangkan IPv6 panjangnya 128 bit.

a. Alamat IPv4

Dalam lingkungan jaringan, alamat IPv4 terdiri dari beberapa alamat *unicast*, antara lain :

1) Alamat Unicast

Alamat *broadcast* mengacu pada alamat IPv4 yang ditujukan untuk semua *node* IP pada segmen jaringan yang sama. Alamat pengiriman digunakan untuk komunikasi *one-to-one*.

2) Alamat Broadcast

Pada saat yang sama, alamat *multicast* dimaksudkan untuk diproses oleh satu atau lebih *node* pada segmen

jaringan yang sama atau berbeda. Alamat *multicast* digunakan dalam komunikasi *one-to-many*.

3) Alamat *Multicast*

Alamat IPv4 dibuat untuk mengatasi satu atau lebih *node* pada segmen jaringan yang sama atau berbeda. Alamat *multicast* digunakan untuk komunikasi *one-to-many*.

b. Kelas-Kelas IP Address

Alamat IP dibagi menjadi beberapa kategori berdasarkan kapasitas. Kelas A berkapasitas lebih dari 16 juta komputer, Kelas B berkapasitas lebih dari 65 ribu komputer, dan Kelas C berkapasitas 254 komputer. Ukuran *grid* ditentukan berdasarkan tabel berikut :

Tabel 2.1 Alamat *Unicast* IP versi 4

Kelas Alamat Ip	Oktet Pertama (Desimal)	Oktet Pertama (Biner)	Digunakan Oleh
Kelas A	1–126	0xxx xxxx	tujuan <i>unicast</i> untuk jaringan ruang lingkup besar.
Kelas B	128–191	1xxx xxxx	Alamat <i>unicast</i> untuk jaringan ruang lingkup menengah sampai ruang lingkup besar.
Kelas C	192–223	110x xxxx	Tujuan <i>unicast</i> untuk jaringan ruang lingkup kecil.
Kelas D	224–239	1110 xxxx	Alamat <i>multicast</i> (bukan

			alamat <i>unicast</i>).
Kelas E	240–255	1111 xxxx	Direservasikan, umumnya digunakan sebagai alamat percobaan (eksperimen) (bukan alamat <i>unicast</i>).

Tabel 2.1 memperlihatkan kelas IP dari kelas A,B,C,D, dan E beserta jumlah *client* yang bisa terhubung dalam masing-masing kelas. Dan pengalamatan tersebut sudah dijadikan aturan baku dalam pengalamatan sebuah IP *address* dalam sebuah jaringan internet.

1) Kelas A

Alamat *unicast* Kelas A ditugaskan ke jaringan besar. Nilai bit paling signifikan dari alamat IP Kelas A selalu 0. Tujuh bit berikutnya membentuk pengidentifikasi jaringan, yang melengkapi oktet pertama. 24 bit sisanya (atau tiga oktet terakhir) mewakili pengidentifikasi *host*.

Dengan ini, kelas A dapat menampung hingga 126 jaringan dan 16,777,214 *host* per jaringannya. Alamat dengan oktet awal 127 tidak diizinkan karena digunakan untuk mekanisme *Interprocess Communication* (IPC) di dalam mesin yang sama.

2) Kelas B

Alamat-alamat *unicast* kelas B diperuntukkan untuk jaringan yang berukuran menengah hingga besar. Dua bit pertama di dalam oktet pertama alamat IP kelas B selalu diatur sebagai bilangan biner 10. 14 bit berikutnya (untuk melengkapi dua oktet pertama) akan membentuk pengenal jaringan. 16 bit yang tersisa (dua oktet terakhir) akan mewakili pengenal *host*. Kelas B dapat menampung hingga 16,384 jaringan dan 65,534 *host* untuk setiap jaringannya.

3) Kelas C

Alamat IP *unicast* kelas C digunakan untuk jaringan yang kecil. Tiga bit pertama di dalam oktet pertama alamat kelas C selalu diatur sebagai 110. 21 bit berikutnya (untuk melengkapi tiga oktet pertama) akan membentuk pengenal jaringan. 8 bit yang tersisa (sebagai oktet terakhir) akan mewakili pengenal *host*. Dengan ini, total 2,097,152 jaringan dapat dibuat dan 254 *host* dapat ditampung untuk setiap jaringannya.

4) Kelas D

Alamat IP kelas D hanya digunakan untuk alamat-alamat IP *multicast*, sehingga berbeda dengan tiga kelas di atasnya. Empat bit pertama pada IP kelas D selalu diset ke nilai biner 1110. 28 bit lainnya digunakan sebagai alamat yang dapat digunakan untuk mengidentifikasi *host*. Untuk

lebih memahami tentang alamat ini, lihat pada bagian alamat *Multicast IPv4*.

5) Kelas E

Alamat IP kelas E disediakan sebagai alamat yang bersifat "eksperimental" atau percobaan dan ditetapkan untuk digunakan pada masa depan. Empat bit pertama selalu diset ke nilai biner 1111. 28 bit lainnya digunakan sebagai alamat yang dapat digunakan untuk mengidentifikasi *host*.

B. Kajian Pustaka

Tinjauan literatur didasarkan pada publikasi penelitian sebelumnya tentang topik atau masalah yang sama atau serupa dengan penelitian yang sedang dilakukan. Berikut beberapa hasil penelitian sebelumnya. :

1. Penelitian sebelumnya dilakukan oleh Desmira dan Romi Wiryadinata dari Fakultas Keguruan dan Ilmu Pendidikan dan Fakultas Teknik Elektro UNTIRTA Banten dengan judul "*Rancang Bangun Keamanan Port Secure Shell (SSH) Menggunakan Metode Port knocking tahun 2022*". Studi ini membahas tentang keamanan Mikrotik OS menggunakan metode *port knocking* dengan jalur port SSH. Fitur SSH ini digunakan untuk memonitoring server masing-masing agen tiket. Dalam kasus yang dipelajari oleh Desmira dan Romi, Romi mengusulkan untuk mengamankan jaringan dengan metode port-knocking, karena tidak ada pengamanan khusus dalam pengelolaan jaringan yang ada.

2. Penelitian selanjutnya di lakukan oleh tiga orang bersahabat yaitu Yudi Mulyanto, M.Julkarnain, Aldela JabiAfahar dari jurusan Teknik Informatika, Universitas Teknologi Sumbawa tahun 2021, dengan judul “*Implementasi Port knocking Untuk Keamanan Jaringan smkn1 Sumbawa besar*”. Penelitian ini menjelaskan tentang desain dan rangkaian percobaan rangkaian keamanan jaringan dengan *port knocking*. Dalam studi yang dilakukan oleh ketiga sahabat ini, mereka mensimulasikan pentingnya keamanan jaringan utama dengan memastikan *port knocking*.
3. Penelitian yang lain yaitu dari Januar Al Amien dari Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau dengan judul “*Implementasi Keamanan Jaringan Dengan IpTabels Sebagai Firewall Menggunakan Metode Port knocking*”. Studi ini membahas analisis dan implementasi *port knocking Firewall* di Mikrotik OS. Untuk penelitian yang berfokus pada keamanan dilakukan pada penyortiran alamat IP yang diangkat oleh mikrotik untuk mencegah akses lebih lanjut oleh perangkat manajemen jaringan yang ada.
4. Penelitian selanjutnya dari Teddy, dengan judul “*Analisis Keamanan Jaringan Wireless Fidelity Sekolah Menengah Atas Negeri 10 Luwu tahun 2020*”. Dari Program Studi Informatika Fakultas Teknik Komputer Universitas Cokroaminoto Palopo. Penelitian ini menjelaskan tentang sistem keamanan jaringan wireless yang menggunakan *Who is On my Wifi*, karena serangan sering terjadi melalui packet *sniffing*.

5. Penelitian berikutnya dari Agung dan Alvian dengan judul “*implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X* “ tahun 2020 dari Fakultas Ilmu Komputer, Program Studi Teknik Komputer, Universitas Amikom Yogyakarta. Masalah muncul dari penelitian, yaitu. tidak ada batasan akses untuk penggunaan internet di dalam perusahaan. Yang menyebabkan ketidak seimbangan akses jaringan di semua perangkat di perusahaan, ia kemudian mengusulkan metode *Access Control List* (ACL) VLAN (*Virtual Local Area Network*) yang diterapkan di Perusahaan X.

C. Keunggulan Penelitian

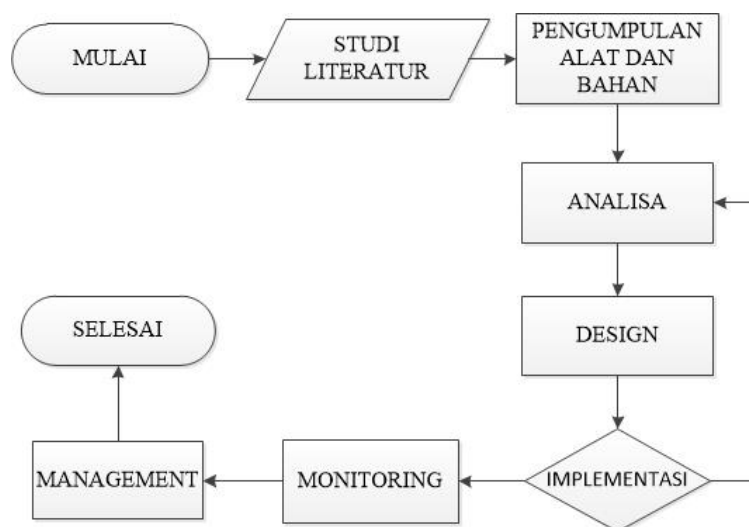
Dalam penelitian ini, penulis menerapkan teknik *port knocking* yang berguna menganalisis keamanan sistem jaringan yang kurang baik. Teknik ini dijalankan guna menganalisa jalur lalu lintas sebuah port yang sedang berjalan ditempat penelitian. Berikut ini adalah beberapa keunggulan dari proyek yang dilakukan oleh penulis :

1. Menggunakan teknik *port knocking* yang efisien serta lebih fleksibel dibandingkan penelitian sebelumnya dan berguna untuk memecahkan masalah yang timbul pada SMK PGRI 1 Nganjuk.
2. Dilakukannya pengembangan dari metode *port knocking* hasil penelitian sebelumnya, yang menjadikan metode *port knocking* yang diterapkan oleh penulis lebih kuat dan lebih kompleks. Pengembangan dari *port knocking* disini adalah dengan mengunci semua jalur menuju pintu

server yang dimana salah satunya adalah menutup jalur akses masuk lewat jalur *mac address*.

3. Dilakukan proses analisis sistem pada jaringan untuk menganalisis lalu lintas port pada lokasi penelitian.
4. Menambahkan fitur aturan untuk memblokir sebuah serangan DDOS pada *Router* di SMK PGRI 1 Nganjuk.
5. Pengoperasian yang sangat mudah dan lebih praktis.
6. Jalannya penelitian yang terstruktur dengan baik, berdasarkan penerapan kaidah NDLC.
7. Kaidah NDLC membuahkan data yang terperinci dan membantu dalam pelaporan.

D. Flowchart Alur Penelitian



Gambar 2.12 Alur *Flowchart* Penelitian

Pada skema yang ditunjukkan gambar 2.12, menunjukkan proses alur penelitian dalam pengumpulan data serta penerapan dari sebuah metode

yang diusulkan. Terlihat pada gambar diatas setelah melakukan proses pencarian data serta analisa permasalahan prosedur selanjutnya adalah tahap implementasi.

Pada tahap implementasi terjadi sebuah alur penentuan dimana apabila hasil dari sistem usulan masih belum dapat di implementasikan maka mengulangi proses analisa, guna untuk mencari jalan keluar yang lebih efisien dari permasalahan yang timbul. Proses selanjutnya adalah monitoring hasil dari tahap implementasi dan sampai akhirnya di terapkan.

E. Lokasi Penelitian

Dalam penulisan Tugas Akhir skripsi ini yang menjadi objek penelitian adalah kewanar jaringan pada SMK PGRI 1 Nganjuk.

1. Sejarah singkat SMK PGRI 1 Nganjuk

SMK PGRI Nganjuk berdiri mulai tahun pelajaran 1901-902, tepatnya tercantum di dalam Surat Keputusan Dewan Pengurus Yayasan persekolahan PGRI Daerah V Jawa Timur, tentang Pengesahan SMK PGRI Nganjuk yaitu tanggal 01-01-1901, dengan No.SK: 105/I04.5.1/E-80. Adapun kepengurusan saat ini sebagai berikut :

Tabel 3.1 Tabel Kepengurusan

NAMA	JABATAN
Drs. LUKMAN, M.Mpd	Kepala Sekolah (Ks)
Erin Agus Tiyono	Ktu
Sunarso, S.Pd	Bendahara Sekolah
Guru Dan Staff	

SMK PGRI 1 Nganjuk Memiliki 8 jurusan yang bisa dipilih oleh calon siswa yang hendak bergabung sebagai keluarga besar SMK PGRI 1 Nganjuk.

2. Visi dan Misi SMK PGRI 1 Nganjuk

Berikut ini Visi dan Misi yang dimiliki dan dijunjung tinggi oleh SMK PGRI 1 Nganjuk :

a. VISI SMK PGRI 1 Nganjuk

Mewujudkan Sekolah Menengah Unggulan berstandart Nasional dan Internasional.

b. MISI SMK PGRI 1 Nganjuk

- 1) Meningkatkan kualitas pembelajaran terhadap peserta didik perkembangan IPTEK dan berwawasan IMTAQ.
- 2) Menyelenggarakan kegiatan DIKLAT yang relevan dengan kebutuhan kehidupan masyarakat, berorientasi pada “ *Key Competencies* “.
- 3) Mengembangkan jalinan sama dengan mitra kerja didalam dan di luar negeri.
- 4) Menumbuhkan kembangkan budaya kedisiplinan
- 5) Menyiapkan tenaga kerja tingkat menengah yang kompeten bidang pengetahuan dan teknologi mekanik otomotif sehingga siap bekerja sesuai dengan kompetensinya.
- 6) Menyiapkan tenaga kerja tingkat menengah yang bertaqwa kepada Tuhan Yang Maha Esa, berbudi pekerti luhur,

berkepribadian dan berkebangsaan Indonesia, jujur dan bertanggung jawab.

- 7) Menyiapkan tenaga kerja tingkat menengah yang memiliki kecakapan hidup, memiliki pengetahuan dan keterampilan berwirausaha sehingga mampu mengatasi masalah kehidupan diri sendiri, keluarga dan bermanfaat bagi masyarakat sekitarnya.
- 8) Membekali siswa dengan Ilmu pengetahuan dan keterampilan berkomunikasi bahasa internasional kejuruan serta penguasaan teknologi Informasi dan komunikasi global sehingga mampu beradaptasi serta berkompetisi di dunia kerja internasional sesuai dengan kompetensi kejuruannya.

3. Struktur SMK PGRI 1 Nganjuk



Nganjuk, 15 Juli 2022
Kepala SMK PGRI 1 Nganjuk

Berikut ini Struktur Organisasi SMK PGRI 1 Nganjuk, Yaitu :

Gambar 2.13 Struktur Organisasi
(Sumber : Kantor Tata Usaha SMK PGRI 1 Nganjuk)
Dalam gambar 2.13 menjelaskan struktur organisasi dari SMK

PGRI 1 Nganjuk yang posisi tertinggi diisi oleh kepala sekolah dan dibawah kepala sekolah terdapat staff yang langsung bertanggung jawab terhadap masing-masing anggotanya yaitu wakil kepala sekolah KTU, dan bendahara sekolah.

4. Profil SMK PGRI 1 Nganjuk

Berikut ini profil singkat dari SMK PGRI 1 Nganjuk :

1. NPSN : 20538346
2. Status : Swasta
3. Bentuk Pendidikan : SMK
4. Status Kepemilikan : Yayasan
5. SK Pendirian Sekolah : 105/I04.5.1/E-80
6. Tanggal SK Pendirian : 1901-01-01
7. SK Izin Operasional : 1051/104.5.1/E-80
8. Tanggal SK Izin Operasional : 1900-01-01

5. Kompetensi Keahlian

SMK PGRI 1 Nganjuk Memiliki 8 Jurusan yaitu :

- a. Teknik Gambar Bangunan
- b. Teknik Instalasi Pemanfatan Tenaga Listrik
- c. Teknik Pemesinan
- d. Teknik Las
- e. Teknik Kendaraan Ringan

- f. Teknik Bisnis Sepeda Motor
- g. Teknik Audio Video
- h. Teknik Komputer Jaringan

6. Ekstrakurikuler

SMK PGRI 1 Nganjuk Memiliki 6 Ekstrakurikuler yaitu :

- a. Paskibraka
- b. PMR
- c. Olahraga
- d. Pramuka
- e. Majelis Tak'lim
- f. English Club

BAB III

ANALISIS DAN PERANCANGAN

Berisi tentang gambaran umum sistem, gambaran lebih detail tentang kasus yang disajikan, dan sistem yang dikerjakan.

A. Analisa

Analisis adalah pembagian suatu masalah menjadi komponen-komponen yang lebih kecil untuk mengidentifikasi dan mengevaluasi masalah dan hambatan yang ditemui, dan kebutuhan yang diharapkan sehingga kedepannya dapat diusulkan perbaikan-perbaikannya.

Bab ini menguraikan proses analisis pengujian terhadap konfigurasi mikrotik yang berjalan di SMK PGRI 1 Nganjuk, serta melakukan perancangan dan implementasi metode yang digunakan dalam meningkatkan keamanan sistem jaringan. Sebelum mengembangkan dan merencanakan sistem, terlebih dahulu harus dilakukan analisis kebutuhan dasar sistem keamanan jaringan yang akan dibangun dan diimplementasikan.

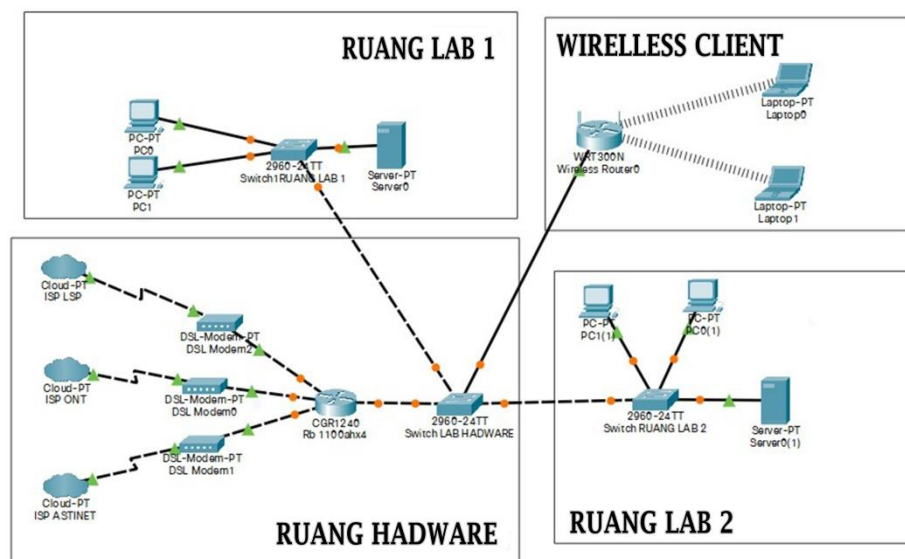
1. Analisa sistem yang berjalan

Dalam penerapan keamanan jaringan di SMK PGRI 1 Nganjuk saat ini masih belum terbentuk dengan sempurna. Konfigurasi yang berjalan saat ini masih rentan penyerangan terhadap server. Dalam hal

ini konfigurasi yang berjalan masih sebatas *management interface*, *bandwidth*, WiFi, pemblokiran situs terlarang dan beberapa konfig lain.

2. Analisa jaringan internet

SMK PGRI 1 Nganjuk mempunyai sumber *bandwidth* dengan menggunakan 3 *line ISP (Internet Service Provider)* yang *diload balancingkan* dengan masing-masing *line bandwidth 20Mbps*, sehingga total *bandwidth* yang dikelola oleh SMK PGRI 1 Nganjuk sebesar 60Mbps.

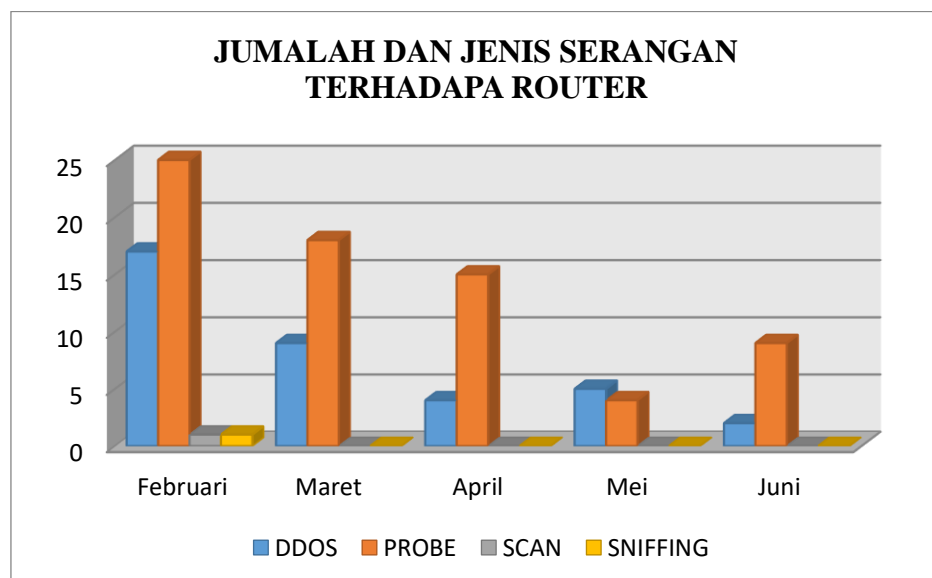


Gambar 3.1 Topologi Yang Berjalan

Dari topologi 3.1 sumber internet dari ISP di transfer kedalam sebuah router lalu disebar lagi melalui beberapa jalur. Yang pertama jalur kabel yang disalurkan seperti ruang lab 1 dan lab 2. Selain menggunakan jalur kabel penyebaran koneksi internet juga disebar melalui jalur *nirkabel* atau *Wireless*.

3. Analisa permasalahan

Setelah dilakukan wawancara terhadap admin jaringan yaitu bapak sidiq, pak sidiq menjelaskan bahwa sistem penganmanan mikrotik *Router Rb 1100ahx4* yang menjadi pusat manajemen jaringan memiliki beberapa kelemahan. Selain itu adanya serangan terhadap *Router Rb 1100ahx4* yang dilakukan pihak yang tidak bertanggung jawab agar dapat mendapatkan koneksi secara ilegal maupun merusak sistem yang berjalan dalam waktu 7 bulan terakhir.



Gambar 3.2 Grafik jumlah serangan terhadap mikrotik
(Sumber : Hasil Wawancara)

Penjabaran dari serangan yang terjadi pada mikrotik pada SMK PGRI 1 Nganjuk yang telah di tunjukkan pada gambar 3.2 meliputi jenis serangan, jumlah serangan, periode bulan penelitian bisa di lihat pada tabel 3.1.

Tabel 3.1 Jumlah serangan terhadap mikrotik

	DDOS	PROBE	SCAN	SNIFFING
Februari	17	25	1	1
Maret	9	18	0	0
April	4	15	0	0
Mei	5	4	0	0
Juni	2	9	0	0

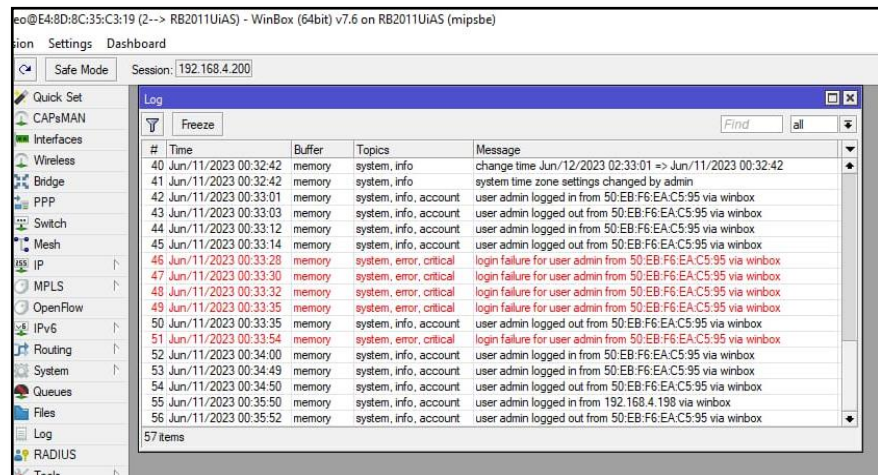
Dari Tabel 3.1 menunjukkan jumlah serangan yang terjadi selama 5 bulan terakhir. Serangan-serangan tersebut bersumber dari bapak Sidik effendi selaku penanggung jawab jaringan di SMK PGRI 1 Nganjuk. Bisa disimpulkan bahwa sebelum melakukan penelitian di lokasi SMK PGRI 1 Nganjuk, serangan-serangan tersebut sudah sering terjadi dan masih belum ditemukan jalan keluarnya.

4. Analisa metode serangan

Kegiatan dan masalah yang mengancam keamanan jaringan *server* antara lain misalnya :

a. Probe

Serangan ditemukan dengan cara *probe*, atau sering disebut *probing* terhadap *server* atau bisa dikatakan sebuah percobaan *login* secara berulang-ulang. Yang bertujuan *login* kedalam mikrotik atau mendapatkan akses internet secara gratis.



Gambar 3.3 Tindakan *Probing*
(Sumber : Router SMK PGRI 1 Nganjuk)

Dari gambar 3.3 ditemukannya seseorang yang mencoba memaksa login terhadap sebuah akun baik dari akun *administrator* ataupun akun dari siswa dan guru. Terlihat jelas di dalam log dari mikrotik menunjukkan tanda merah yang berulang dengan keterangan yang sama yaitu “*login failure for user admin from via winbox*”. Dan beberapa keterangan lainnya yang hampir sama akan tetapi berbeda-beda masing-masing *user* yang digunakan.

b. *Scan*

Pada sistem yang berjalan saat ini, ketika dilakukan *scanning* port terhadap Mikrotik *Server* SMK PGRI 1 Nganjuk yang ditemukan beberapa port yang terbuka. Port-port yang sedang terbuka tersebut bisa dimanfaatkan oleh *attacker* untuk melakukan

penetrasi atau serangan-serangan dengan tujuan mendapatkan informasi atau melakukan pengrusakan terhadap sistem.

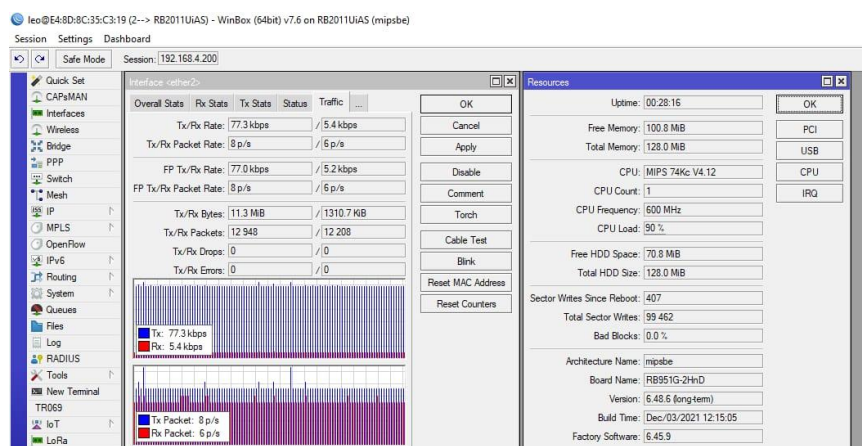
c. Sniffing

selanjutnya adalah terjadinya pencurian data *user login* mikrotik *server* yang di sadap guna untuk mendapatkan *username* dan *password*. Bisa jadi selain data dari *log login* yang didapatkan masih banyak hal-hal yang belum diketahui.

Dalam ilmu *hacking sniffing* juga bisa digunakan untuk melakukan tindakan kejahatan seperti pencurian database, uang, akses sebuah server, kartu kredit dan masih banyak yang lainnya.

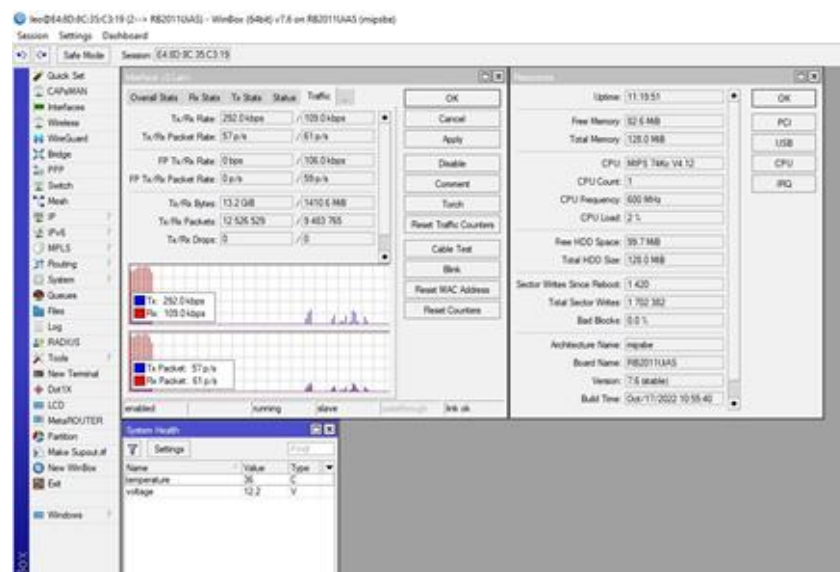
d. DDOS

Selain itu, bentuk serangan-serangan terhadap mikrotik *server* SMK PGRI 1 Nganjuk yaitu serangan DDOS, penyerang mengirimkan sejumlah besar paket ke *server* Mikrotik, menyebabkan peningkatan beban CPU dan peningkatan lalu lintas.



Gambar 3.4 Tindakan DDOS
(Sumber : Router SMK PGRI 1 Nganjuk)

Pada gambar 3.4 terlihat koneksi pada jaringan mikrotik sangat padat dan proses *cpu load* sangat besar. Sehingga menyebabkan kondisi *Router* menjadi berhenti berfungsi sementara. Akibatnya koneksi yang seharusnya bisa disalurkan kesetiap ruangan menjadi bermasalah.



Gambar 3.5 Sebelum terkena DDOS
(Sumber : Router SMK PGRI 1 Nganjuk)

Berbeda dari gambar 3.4, pada gambar 3.5 menunjukkan proses *traffic* jaringan yang sangat baik serta penggunaan *cpu load* yang sangat kecil. Hal ini dikarenakan tidak terjadinya serangan DDOS terhadap mikrotik *server*. Dan menjadikan mikrotik berjalan dengan baik serta menjalankan servicenya sesuai dengan rule yang berjalan.

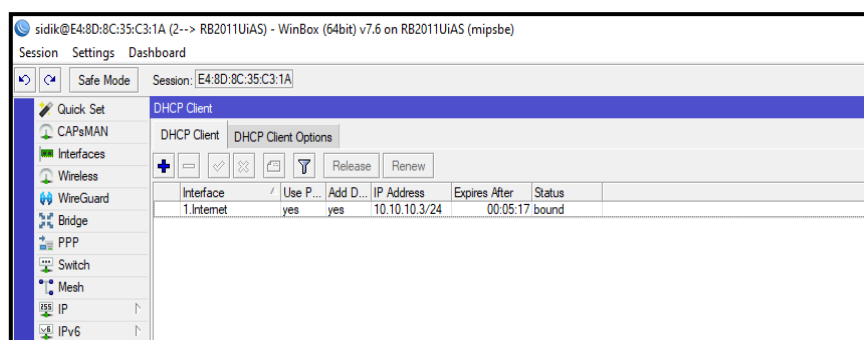
5. Analisa Metode Pengamanan

Metode yang digunakan *administrator* saat mengalami permasalahan seperti tidak ada koneksi internet, *load* cpu mikrotik *server* berat dan sebagainya adalah mereset ulang konfigurasi yang sedang berjalan. Dan akan melakukan proses *import* ulang konfigurasi yang sudah di *backup* sebelumnya.

6. Analisa Konfigurasi Perangkat Jaringan Saat Ini

Konfigurasi yang berjalan saat ini ditempat lokasi penelitian bisa dikatakan adalah konfigurasi yang sudah baik, namun masih belum dilengkapi dengan fitur penunjang keamanan jaringan dan berikut ini adalah konfigurasi yang sudah berjalan :

a. DHCP Client

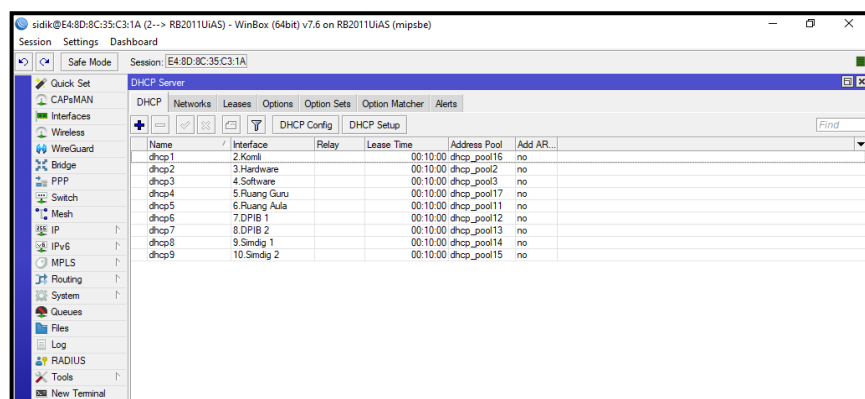


Gambar 3.6 DHCP Client
(Sumber : Router SMK PGRI 1 Nganjuk)

DHCP *client* adalah perangkat yang melakukan sinkronisasi dengan *server* DHCP untuk menerima berbagai informasi seperti alamat IP dan lain sebagainya. Pada gambar 3.6 service DHCP *Client* telah aktif dengan melihat status *bound*.

b. DHCP Server

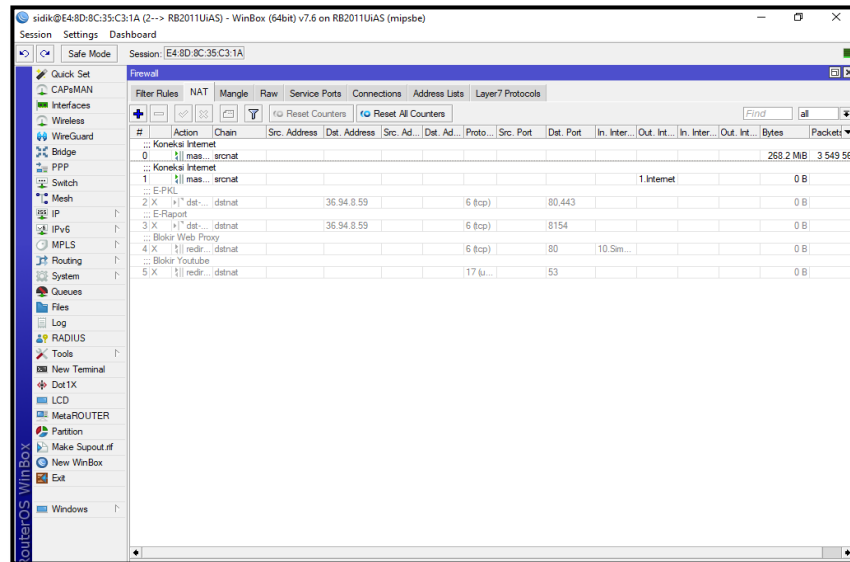
DHCP *server* adalah Sebuah fitur yang digunakan untuk menyediakan *Ip Address*, *Gateway*, DNS dan sebagainya. perangkat yang bertugas memberikan konfigurasi jaringan secara otomatis. Biasanya, DHCP Server hanya ada satu dalam satu jaringan. (Wikipedia.org)



Gambar 3.7 DHCP Server
(Sumber : Router SMK PGRI 1 Nganjuk)

Dari gambar 3.7 menunjukkan proses pembagian *Ip Address*, *Gateway*, DNS yang dilakukan oleh server mikrotik dengan melihat status di masing-masing interface. Selain melihat status aktif dan tidaknya sebuah DHCP Server, pada tampilan DHCP server juga di lihatkan *pool* alamat IP dari masing-masing interface.

c. NAT Masquerade

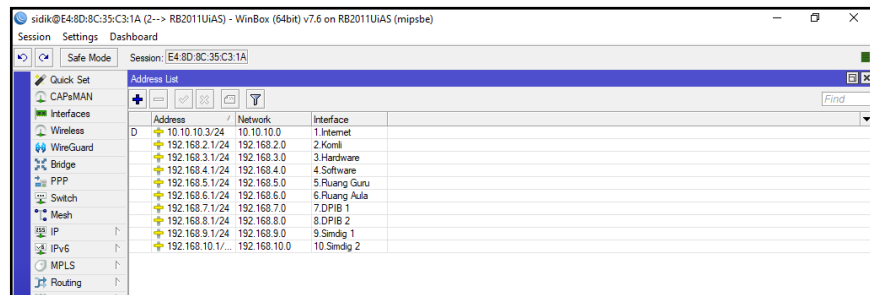


Gambar 3.8 NAT Masquerade
(Sumber : Router SMK PGRI 1 Nganjuk)

Secara sederhana dan singkat, fungsi dan guna *masquerade* ini agar komputer *client* bisa berkomunikasi dengan jaringan publik. Pada gambar 3.8 diperlihatkan konfigurasi NAT yang berada pada menu IP dan sub Firewall.

d. IP Address

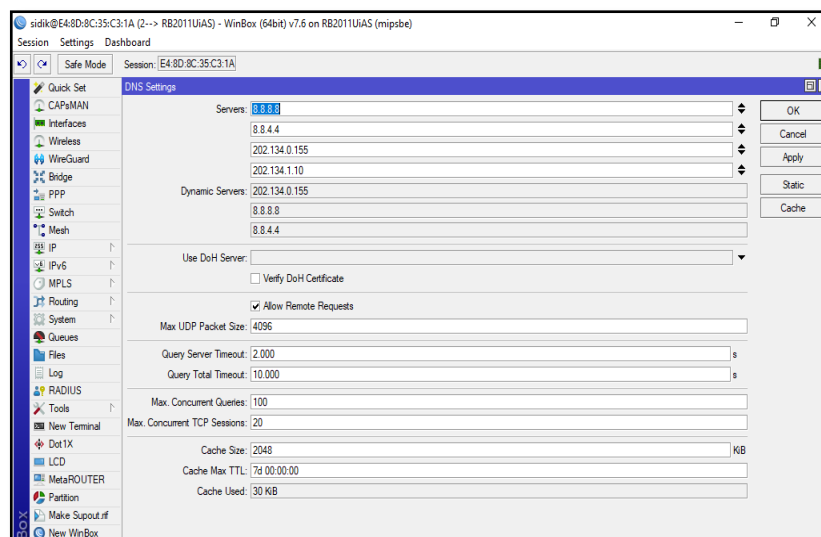
Ip Address adalah deretan angka yang digunakan untuk identitas sebuah perangkat yang terhubung dalam *infrastruktur* jaringan. Berikut ini konfigurasi *IP Address* yang sudah disesuaikan dengan masing-masing port.



Gambar 3.9 Address List
(Sumber : Router SMK PGRI 1 Nganjuk)

Pada gambar 3.9 menu *Address List* berfungsi menunjukkan IP yang telah dibuat serta interface mana saja yang digunakan beserta batas panjang networknya.

e. DNS



Gambar 3.10 Pengaturan DNS
(Sumber : Router SMK PGRI 1 Nganjuk)

Pada gambar 3.10 DNS (*Domain Name System*) adalah sistem yang bertanggung jawab untuk menghubungkan nama *host* atau nama domain situs Internet ke alamat IP.

7. Analisa NDLC

a. Tahap Analisa

Tahapan ini merupakan tahapan pengumpulan data yang telah penulis lakukan sehingga mendapatkan data-data yang dibutuhkan, seperti :

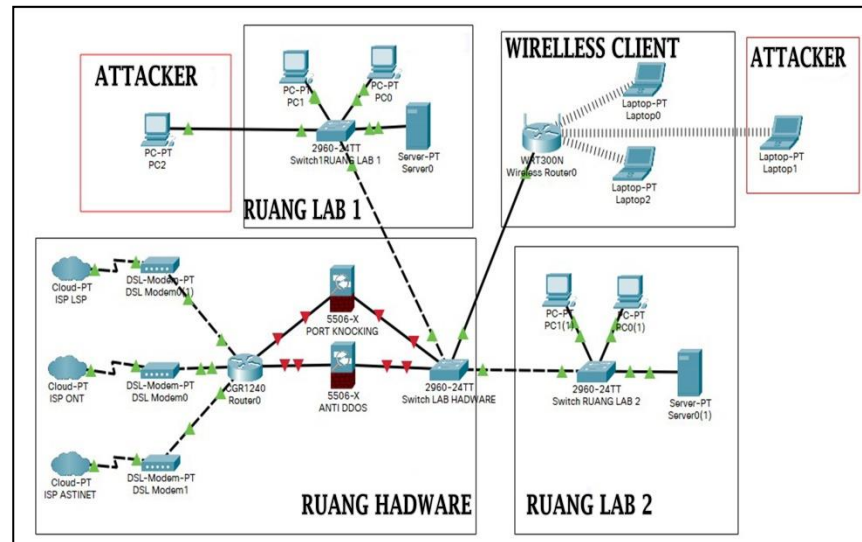
- 1) Permasalahan yang timbul.
- 2) *Topologi* jaringan.
- 3) Sistem yang sedang berjalan.
- 4) Metode serangan terhadap *server* mikrotik.
- 5) Metode pengamanan yang dilakukan oleh pengelola jaringan.
- 6) Dan konfigurasi apa saja yang telah diterapkan.

b. Tahap Desain

Tahapan ini menjabarkan proses desain *topologi* keamanan yang diusulkan pada jaringan mikrotik SMK PGRI 1 Nganjuk. Dalam jalannya proses desain *topologi* jaringan ini menggunakan sebuah aplikasi cisco paket tracer.

Tujuan dari sistem yang diusulkan dalam penelitian ini adalah untuk menganalisis sistem keamanan yang diterapkan oleh instansi terkait, dengan fokus pada mikrotik *server* sebagai pusat sistem. Untuk melakukan analisis, hak akses setiap komputer yang

terhubung ke dalam jaringan diperiksa dan proses penyadapan port dilakukan untuk menilai keamanan akses port di jaringan saat ini.



Gambar 3.11 *Topologi* Yang diusulkan

Gambar 3.11 menunjukkan *topologi* jaringan yang terfokus pada ruang perangkat keras, di mana sumber Internet dari ISP langsung ke modem dan didistribusikan ke *Router* Rb 1100ahx4 dan ruang lain seperti ruang laboratorium, ruang kantor, dan wifi. *Administrator* jaringan dapat menggunakan Mikrotik dari lokasi manapun untuk memantau jaringan atau memperbaiki konfigurasi.

Namun, *topologi* ini juga memberikan kemudahan akses ke jaringan inti bagi penyerang atau pihak yang tidak diinginkan. Oleh karena itu, penulis merekomendasikan penambahan *Firewall* pada konfigurasi *server* untuk membatasi akses yang tidak diinginkan dan meningkatkan keamanan jaringan pusat yaitu mikrotik RB 1100ahx4.

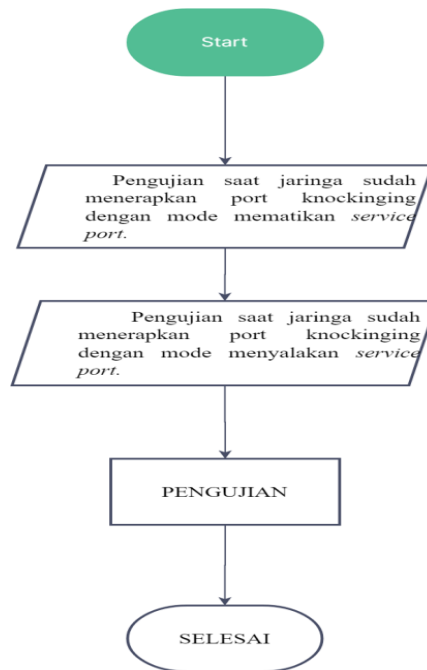
c. Tahap Simulasi

Tahapan ini adalah tahapan dimana simulasi atas desain jaringan yang telah dibuat dengan paket tracer dan implementasi konfigurasi pada *Router* uji coba. Dalam tahap simulasi ini ada beberapa aturan yang telah di terapkan seperti berikut ini :

- 1) Konfigurasi sistem keamanan jaringan *port knocking*.
- 2) Konfigurasi sistem keamanan jaringan anti DDOS.
- 3) Penutupan dan pembukaan *mac* dari *interface Router*.
- 4) Pengembangan sistem *port knocking* dan anti DDOS.

Pada tahapan simulasi ini juga akan dijalankan simulasi pengujian sistem yang telah dibuat diatas. Skenario uji coba dilakukan dalam tiga proses, yaitu :

- 1) Pengujian saat jaringan normal.
- 2) Pengujian saat jaringa sudah menerapkan *port knocking* dengan mode menyalakan *service port*.
- 3) Pengujian saat jaringa sudah menerapkan *port knocking* dengan mode mematikan *service port*.



Gambar 3.12 Alur simulasi pengujian

Pada gambar 3.12 tahapan pengujian dengan metode normal dan mematikan *service port* itu tidak jauh berbeda. Selanjutnya dari metode penelitian NDLC adalah tahapan implementasi, tahapan monitoring, dan tahapan *management*. Ketiga tahapan tersebut akan di jabarkan secara jelas dan terperinci pada bab empat dalam tahapan implementasi dan pembahasan.

B. Desain Sistem (Perancangan)

Pada perancangan sistem usulan akan dijelaskan juga mengenai, perancangan arsitektur, *topologi* jaringan, perangkat lunak yang akan digunakan oleh *hardware*, sistem yang direncanakan atau metode usulan yang akan digunakan dalam penulisan penelitian ini dan perencanaan

pengaturan konfigurasi rancangan serta beberapa percangangan yang akan dibutuhkan kedepannya.

1. Spesifikasi alat

a. Router RB1100x4



Gambar 3.13 *Router* RB1100x4
(Sumber : mikrotik.com)

Pada gambar 3.13 *Router* RB1100x4 Adalah produk penerus dari varian RB1100 series yang menggunakan spesifikasi hardware yang lebih baru yaitu processor Alpine AL21400 1.4GHz Quad Core , 1GB RAM , routerOS level 6, dan casing 1U rackmount.

Berikut ini adalah Spesifikasi dasar dari *Router* RB1100x4, yaitu :

Tabel 3.2 Spesifikasi *Router* RB1100x4

Nama Produk	<i>Router</i> RB1100x4
CPU	AL21400, 4 cores, 1.4 GHz
RAM	1 GB
Storage size	128 MB

Pada Tabel 3.2 memperlihatkan spesifikasi *Router* RB1100x4 dengan kemampuan CPU 4 cores, 1.4 GHz serta memiliki RAM sebesar 1 GB dan media penyimpanan sebesar 128 MB.

b. Pc Client

Tabel 3.3 Spesifikasi Pc Client

PC Processor	Intel Pentium G4400 3.30 GHz
RAM	DDR III 4 GB
HDD	250 GB
Monitor	14"

Pada Tabel 3.3 memperlihatkan Spesifikasi Pc Client yang akan digunakan yaitu kemampuan *processor* Intel Pentium G4400 3.30 GHz dan didukung RAM 4GB lalu dibekali media penyimpanan sebesar 250 GB dan menggunakan monitor 14 in.

2. Perangkat Lunak Yang Digunakan Saat Ini

a. Router RB1100x4

Tabel 3.4 Operating System Router

OS (<i>Operating System</i>)	RouterOS Level6
--------------------------------	-----------------

Tabel 3.4 menjelaskan sistem operasi yang digunakan oleh *router* yaitu RouterOS Level6 dan sistem operasi tersebut adalah sistem operasi terbaru yang telah dikeluarkan oleh mikrotik dan bisa di update ketika ada pembaruan dikemudian hari.

b. Pc Client

Tabel 3.5 Operating System Pc Client

OS (<i>Operating System</i>)	Windows 10
--------------------------------	------------

Tabel 3.5 menjelaskan sistem operasi yang digunakan oleh komputer *client* yaitu *windows* 10 dan sistem operasi tersebut adalah sistem operasi yang dikeluarkan tahun 2015 dan disempurnakan samapai tahun 2020 oleh *windows*. Saat ini *windows* telah mengeluarkan sistem operasi terbaru yaitu *windows* 11.

3. Sistem Yang Direncanakan

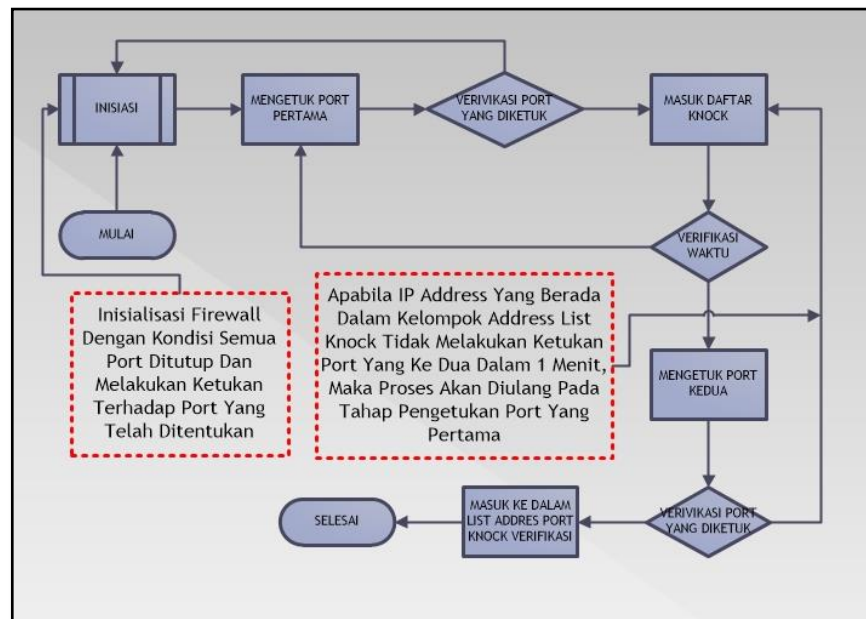
Penulis memerlukan metode yang memenuhi kedua kriteria tersebut untuk mendapatkan keamanan yang diperlukan dan mengizinkan pengguna resmi untuk mengakses *server* mikrotik. Salah satu metode baru yang memenuhi kedua kriteria tersebut adalah *port knocking*.

Berdasarkan analisis masalah yang diterima, beberapa serangan terhadap *server* mikrotik didasarkan pada penyalahgunaan port komunikasi *server* yang terbuka, sehingga tujuan penerapan *port knocking* adalah untuk memberikan perlindungan berlapis dan memfilter IP mana ke *server* Mikrotik.

Daripada itu kelebihan-kelebihan dari *port knocking* pada pengimplementasian mikrotik *Router* diantaranya :

- a. Di mana komputer jarak jauh berhubungan dengan *server* melalui port yang tidak terbuka.
- b. Walaupun port tidak terbuka, layanan yang diberikan tetap beroperasi.

Dalam penggunaan metode ini ada beberapa proses yang harus dilewati, berikut ini skema dari proses perjalanan dari memulai pengetukan pintu sampai selesai.



Gambar 3.14 Gambar alur flow chart *port knocking*

Pada gambar 3.14 dijelaskan alur pengimplentasian *port knocking* pada *Router OS*. Sesuai dengan alur yang telah dibuat terdapat 11 proses yang harus dilewati, yaitu :

- a. Proses memulai akan melakukan knocking port.
- b. Proses nomor 2 menunjukkan inisialisasi port berapa yang akan diketuk agar koneksi atau port yang dikehendaki dapat terbuka.
- c. Nomor 3 menunjukkan proses mengetuk port tahap pertama,

- d. Validasi port yang diketuk , apabila port yang diketuk sudah benar maka ip *address* akan dikelompokan pada *address list* “alamat *port knocking*”, apabila salah akan diulang ke proses Nomor 2.
- e. Proses nomor 5 menunjukkan ip *address* yang mengetuk sesuai dengan port yang telah diatur akan dikelompokan dalam *address list* “alamat *port knocking*”.
- f. Nomor 6 validasi waktu, apabila ip *address* yang berada dalam kelompok *address list* “alamat *port knocking*” dalam waktu kurang dari 2 menit tidak melakukan ketukan port selanjutnya, maka akan proses akan diulang dari Nomor 3.
- g. Tahap ini menunjukkan proses mengetuk port tahap ke dua dalam waktu 1 jam.
- h. Verifikasi port yang di ketuk, apabila port yang diketuk sesuai dengan port yang telah ditentukan, maka ip *address* nya akan dikelompokan pada *address list* “verivikasi alamat *port knocking*”, apabila salah akan diulang ke proses Nomor 5.
- i. IP *address* yang mengetuk port sesuai dengan port yang telah ditentukan, maka ip *address* nya akan dikelompokan pada *address list* “verivikasi alamat *port knocking*”.
- j. IP *address* yang telah berada dalam kelompok *address list* “verivikasi alamat *port knocking*” akan diperkenan kan untuk mengakses *Router server*.
- k. selesai.

4. Usulan Pengaturan Mikrotik

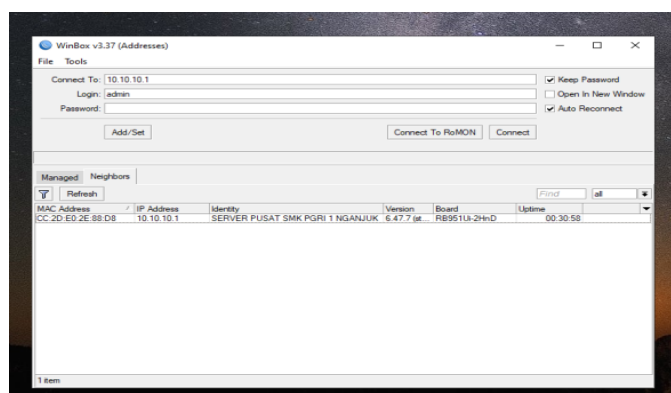
Setelah desain *topologi* selesai, langkah selanjutnya adalah mendesain konfigurasi yang akan digunakan dengan Mikrotik RouterOS. Berikut adalah rencana perakitan pengaturan mikrotik :

a. Pengaturan Router Os via winbox

Ada beberapa jalan untuk digunakan masuk kedalam pengaturan Mikrotik, antara lain :

- 1) Putty
- 2) Web browser
- 3) Winbox
- 4) *telnet*

Penulis_menggunakan aplikasi Winbox untuk masuk kedalam pengaturan Mikrotik. Aplikasi ini disediakan oleh produsen Mikrotik dan memiliki antarmuka pengguna grafis (GUI). Fitur ini memudahkan petugas dalam menjalankan tugas dalam pengaturan Mikrotik.



Gambar3.15 Tampilan awal winbox

Gambar 3.15 memperlihatkan sebuah tampilan *interface* dari aplikasi winbox.

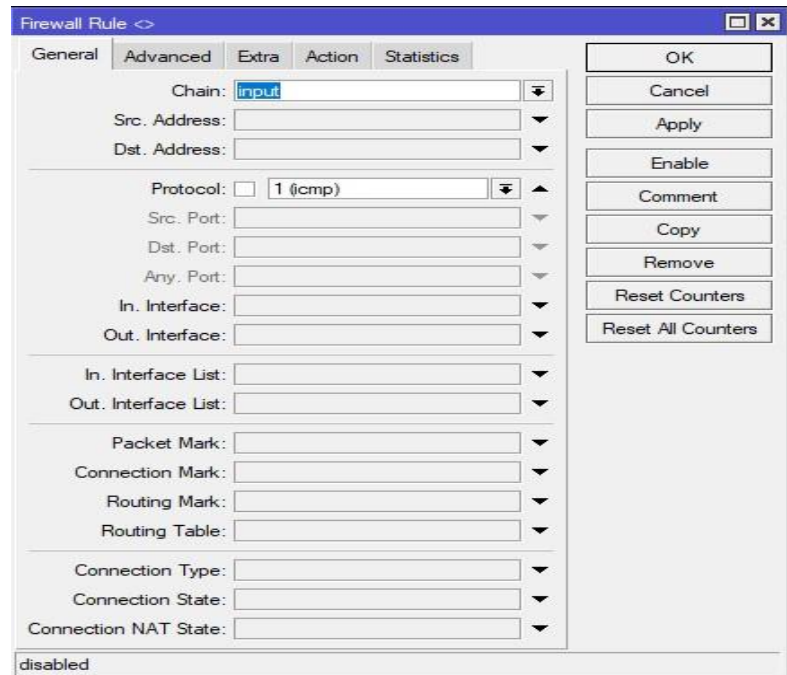
b. Menambahkan *Rule Port knocking* Pada *Firewall*

Agar dapat menyelesaikan masalah yang timbul pada jaringan di SMK PGRI 1 Nganjuk, berikut adalah beberapa langkah-langkah untuk membuat aturan *Port knocking* pada *Firewall* :

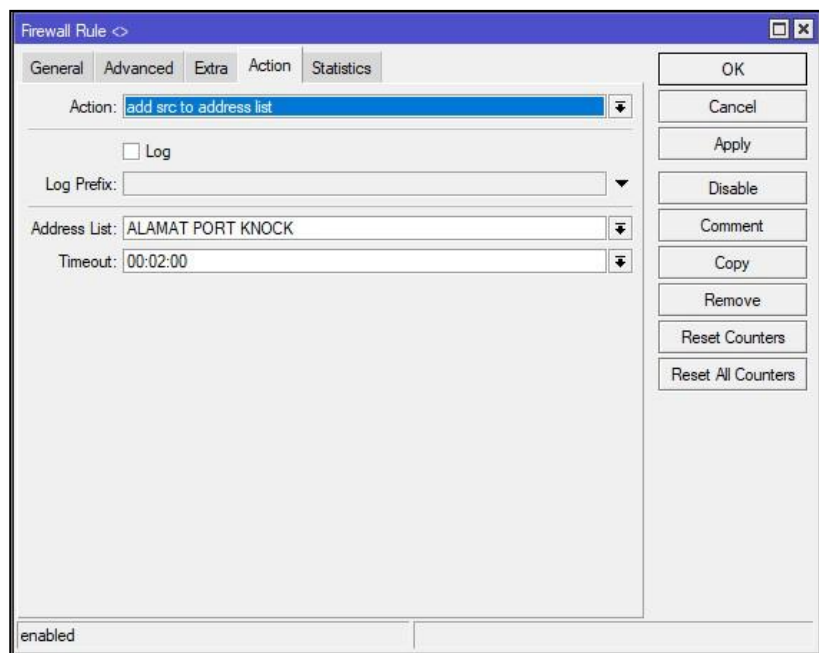
- 1) *Login* ke Mikrotik via Winbox.
- 2) Buat *rule* pertama agar dapat menampung ip yang mencoba masuk kedalam mikrotik, masuk ke Menu "IP" pilih "*Firewall*" pilih pada tab "*Filter*" Add (+) *rule*.
- 3) Pada gambar 3.16 tab "*General*" *Chain: input* dan *protocol: icmp*
- 4) Pilih *interface* yang akan diterapkan metode *port knocking*.
- 5) Pada tab "*Action*": *action: add src to address list* dan *address list: alamat port knocking* (bisa diganti dengan nama lain)
Timeout: 00.02.00 Apply: OK
- 6) Atau bisa menggunakan *Script* sebagai berikut ini :

```
/ip Firewall filter
```

```
add action=add-src-to-address -list address -list="ALAMAT  
PORT KNOCKING" \ address -list-timeout=2m Chain=input  
comment="PORT KNOK TAHAP 1" \in-interface=INTERNET  
protocol=icmp
```



Gambar 3.16 Tampilan *Rule Port knocking*



Gambar 3.17 Tampilan *Action Rule Port knocking*

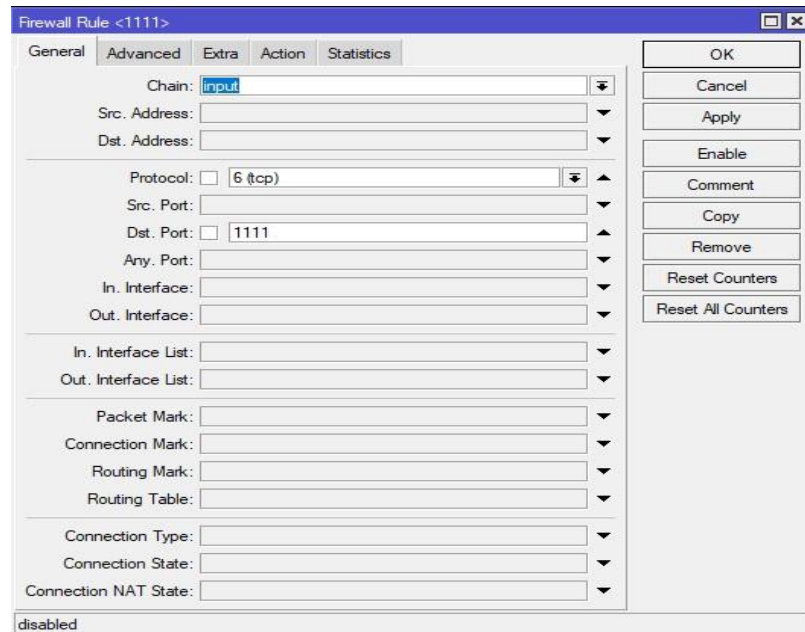
- 7) Pada gambar 3.17 tambahkan *rule* selanjutnya untuk membuat pintu kedua agar penggunaan metode ini lebih efektif dan

berkembang. masuk ke Menu "IP" pilih "*Firewall*" pilih pada tab "*Filter*" Add (+) rule.

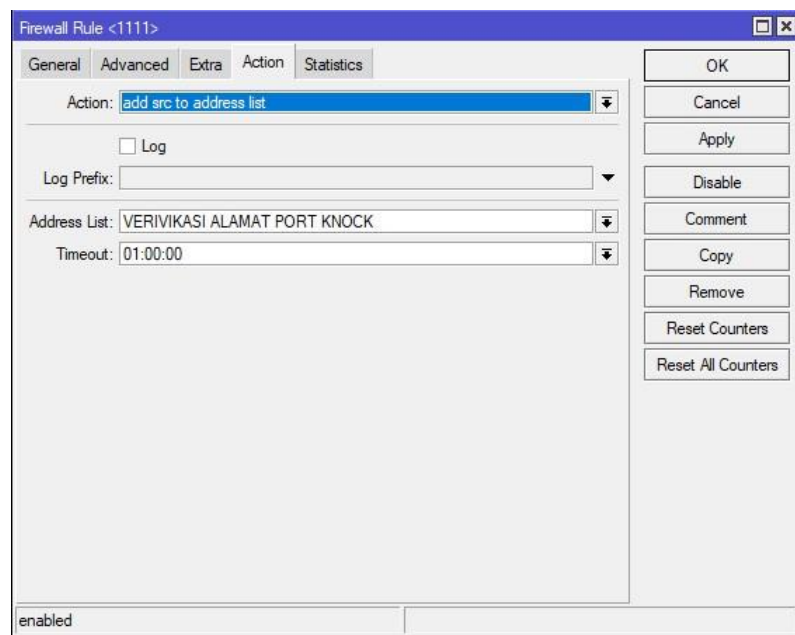
- 8) Pada gambar 3.18 tab "*General*" Chain: *input* dan *protocol*: *tcp*
- 9) Pada tab "*dst.port*" isikan port 1111 (bisa disesuaikan)
- 10) Pilih *interface* yang akan diterapkan metode *port knocking*.
- 11) Pada gambar 3.19 tab "*Action*": *action*: *add src to address list* dan *address list*: verifikasi alamat *port knocking* (bisa diganti dengan nama lain) Timeout: 01.00.00 Apply: OK
- 12) Atau bisa menggunakan *Script* sebagai berikut ini :

/ip Firewall filter

```
add action=add-src-to-address -list address -list=\
"VERIVIKASI ALAMAT PORT KNOCKING" address -list-
timeout=1h Chain=input \ comment="PORT KNOCKING
VERIFIKASI" dst-port=1111 in-interface=INTERNET \
protocol=tcp.
```

Gambar 3.18 Tampilan Action Rule Port knocking update

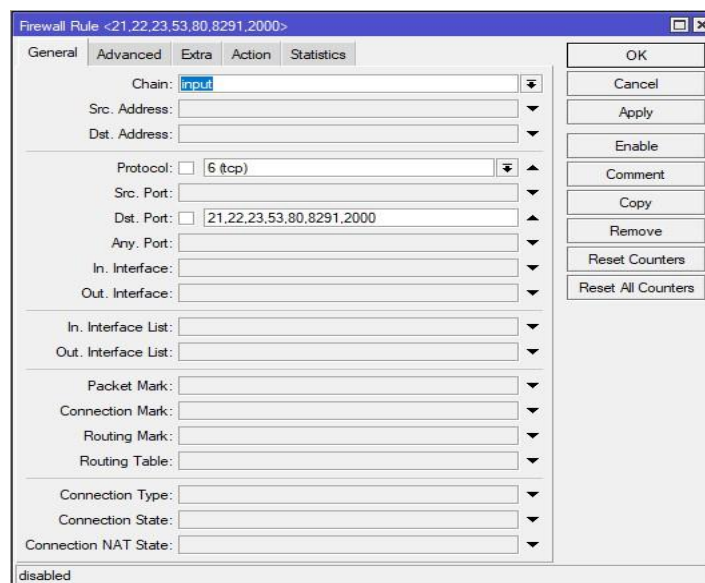


Gambar 3.19 Tampilan Action

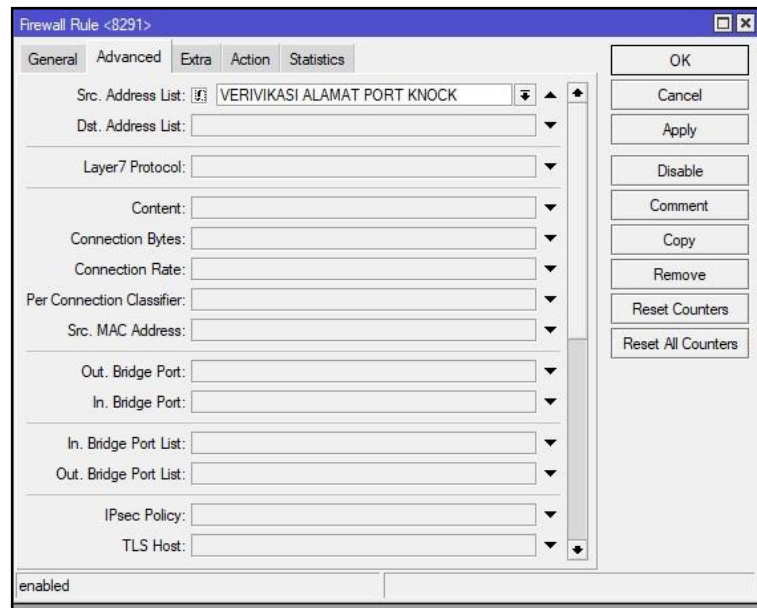
- 13) tambahkan *rule* ketiga agar Mikrotik dapat mengenali mengirimkan paket berupa *ping* untuk membuka *port*. Masuk ke Menu "IP" pilih "Firewall" pilih pada *tab* "Filter" Add (+) *rule*.
- 14) Pada gambar 3.20 *tab* "General" Chain: *input* dan *protocol*: *tcp* dan *Dst. Port* : 21,22,23,53,80,8291,2000.
- 15) Pada *tab* "Advance" *Src. Address List* : verifikasi alamat *port knocking* Pada *tab* "Action":*Drop*. dan *Cek list notif not or*.
- 16) Pada gambar 3.21 dan 3.22 Atau bisa menggunakan *Script* sebagai berikut ini :

/ip Firewall filter

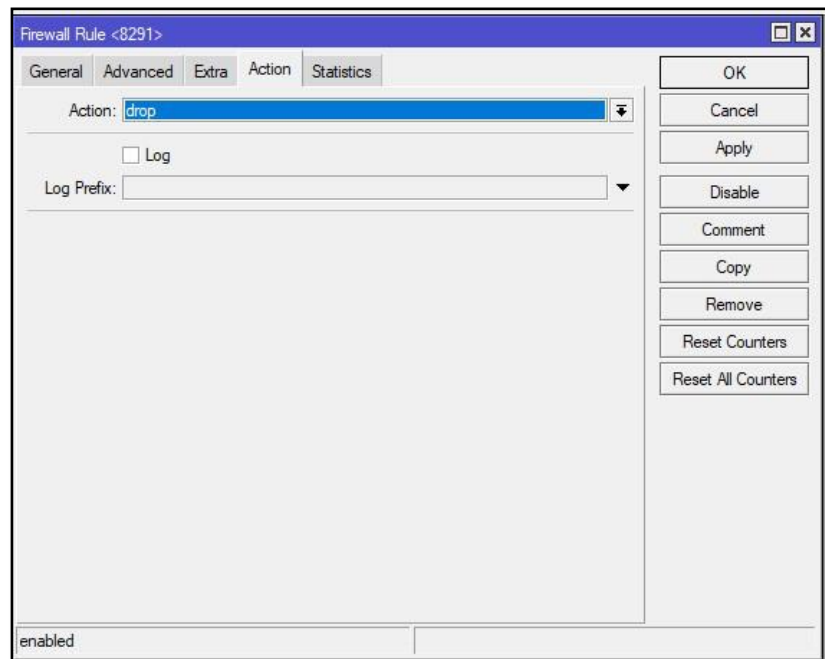
*add action=drop Chain=input comment="BLOKIR WINBOX
UNTUK KNOCK" dst-port=21,22,23,53,80,8291,2000\
protocol=tcp src-address -list="!VERIVIKASI ALAMAT PORT
KNOCKING"*



Gambar 3.20 Tampilan Blokir Winbox



Gambar 3.21 Tampilan *Advanced* Blokir Winbox



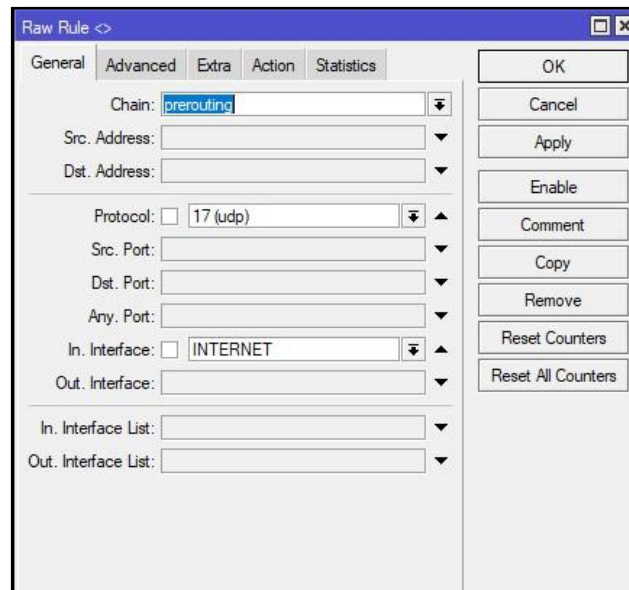
Gambar 3.22 Tampilan *Action* Blokir Winbox

c. Menambahkan *Rule* Alamat DDOS

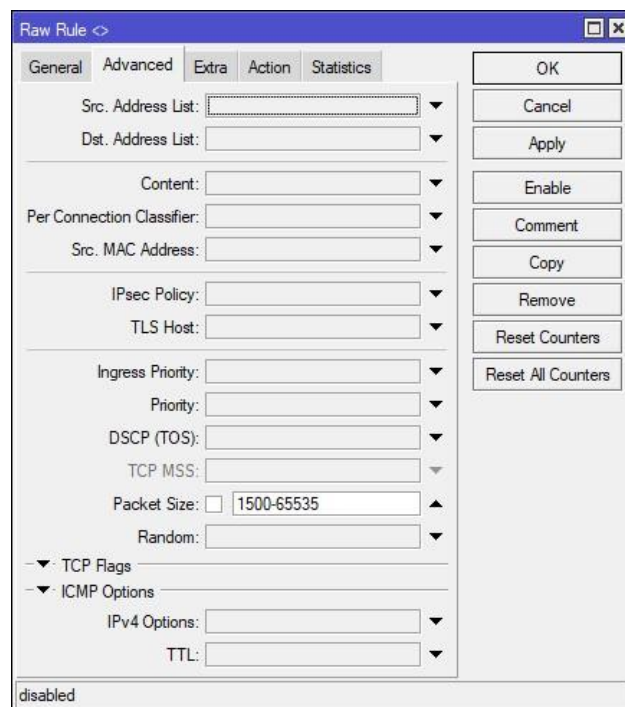
Selain konfigurasi *port knocking*, dan untuk melindungi perangkat Mikrotik dari serangan DDOS, penulis menambahkan aturan yang dapat memblokir dan mendeteksi alamat IP penyerang. Berikut adalah beberapa aturan yang akan ditambahkan.:

- 1) Pada gambar 2. 23 dan 2.24 *rule Firewall* yang berguna untuk menampung alamat serta *mac* dari seorang *attacker* yang melakukan DDOS.
- 2) Pada gambar 2.25 *rule* ini kita memberikan sebuah jarak paket tidak normal guna untuk menangkap seorang *attacker* yaitu sebesar 1500 Kb sampai 65535 Kb.
- 3) Berikut ini adalah script yang bisa digunakan untuk implementasi *Firewall* raw yang bertugas menangkap ip *attacker*.

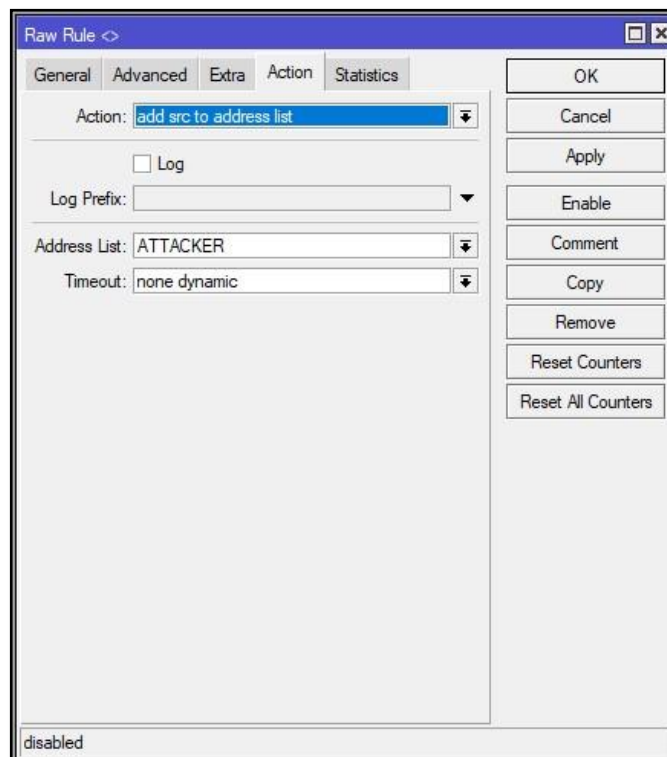
```
/ip Firewall raw add action=add-src-to-address -list address -
list=ATTACKER \ address -list-timeout=none-dynamic
Chain=prerouting comment="\ANTI DDOS RULE ME"
disabled=yes in-interface=INTERNET packet-size=\ 1500-
65535 protocol=udp
```



Gambar 3.23 Tampilan *Firewall* Menampung Ip



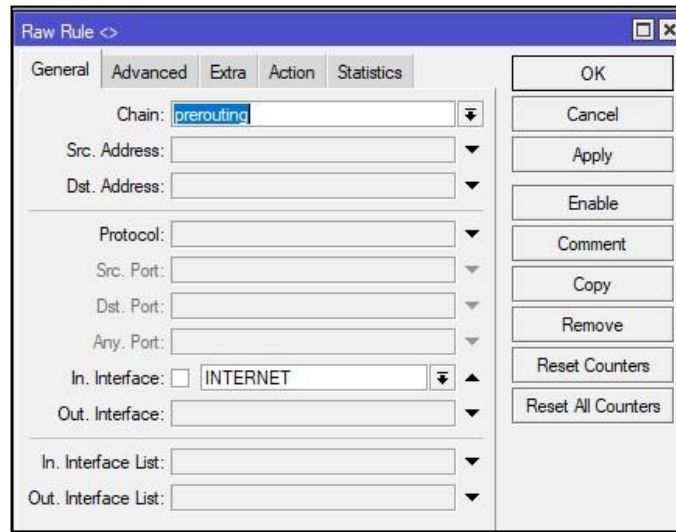
Gambar 3.24 Tampilan *Advanced* Menampung Ip



Gambar 3.25 Tampilan *Action* Menampung Ip

- 4) Membuat *rule Firewall* yang berguna untuk mengatasi seorang *attacker* melakukan serangan DDOS dengan drop IP Address yang digunakan gambar 2.26 dan 2.27. Konfigurasi ini mengambil data dari *rule* yang dibuat sebelumnya. Berikut ini *script* yang digunakan :

```
add action=drop Chain=prerouting comment="DROPP
DDOS RULE ME" disabled=yes \ in-interface=INTERNET
```

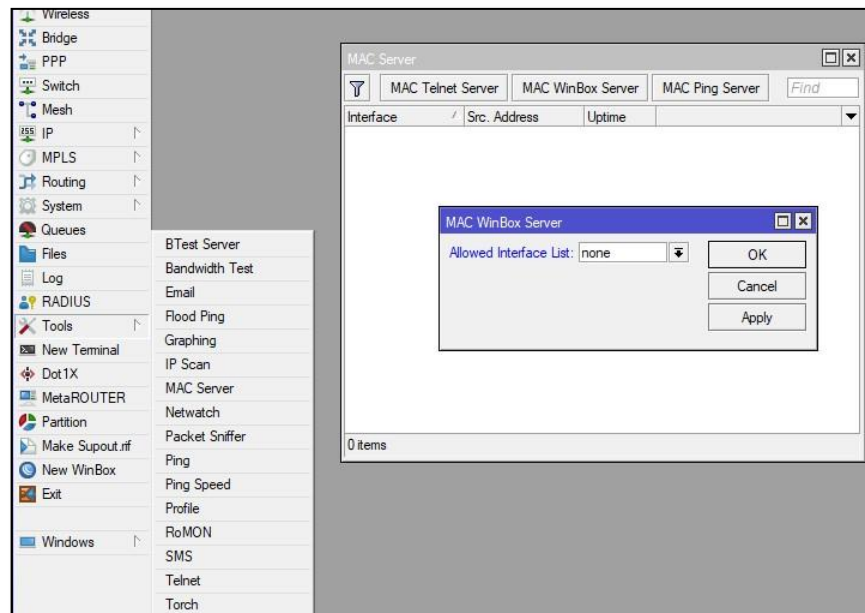
Gambar 3.26 Tampilan *Drop* IP DDOSGambar 3.27 Tampilan *Action Drop* IP DDOS

d. Mematikan Fitur *Mac Interface* Winbox

Dalam penerapan metode *port knocking* masih ada kekurangan yang sangat besar yang dimana masih bisa di aksesnya sebuah mikrotik dari *mac interface*. Dalam implementasinya *port knocking* hanya akan menutup dan membuka jalannya sebuah port dan alamat *address* mikrotik bukan *mac address*.

Jadi pengembangan dari metode *port knocking* ini adalah tetap mempertahankan sistem buka tutup port dengan cara ketukan port dan didukung dengan cara mematikan fitur *mac interface*.

Dengan begitu walaupun seorang *attacker* telah mengetahui alamat *address* dan port dari *Router* tetap tidak bisa melakukan *login* kedalam *server* mikrotik kecuali dia harus melakukan proses *port knocking* terlebih dahulu gambar 3.28.



Gambar3.28 *Mac interface* winbox

BAB IV

IMPLEMENTASI DAN PEMBAHASAN

Penjelasan tentang objek investigasi atau kegiatan yang akan dilakukan, termasuk kondisi objek investigasi atau konfigurasi jaringan sebelum dilakukan investigasi. Penjelasan penanganan data dan analisa sistem *Firewall* menggunakan metode *port knocking* dan anti-DOOS pada Mikrotik *Router OS*. Serta pembahasan lanjutan dari metode penelitian NDLC yang telah dijabarkan pada bab 3 tentang analisis dan perancangan.

A. Implementasi

Tahapan ini menerapkan sistem keamanan jaringan yang telah di desain pada tahap sebelumnya. Pada tahapan implementasi ini nantinya akan dilakukan pengujian *hacking* terhadap *RouterOS* yang telah dikonfigurasi sesuai tahapan sebelumnya seperti skema pada gambar 4.1.

Fungsi dari pengujian ini adalah untuk mengetahui apakah konfigurasi serta implementasi yang telah direncanakan dan diterapkan sebelumnya bisa berhasil dengan baik dan sesuai dengan harapan.



Gambar 4.1 skema penyerangan *hacker*

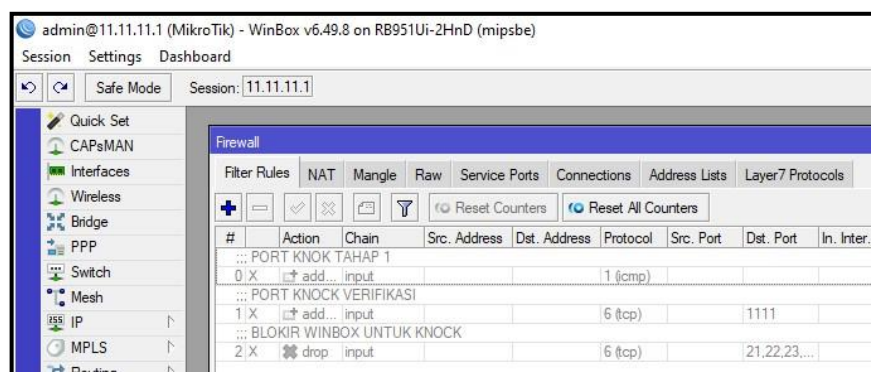
Seperti yang telah disebutkan di tahap simulasi bahwasanya pengujian yang dijalankan ada empat jenis pengujian yakni *port knocking*, *scanning*, *sniffing*, dan DDOS. Yang dimana dalam tahap pengujian ini dilakukan pada kondisi sistem jaringan berada pada dua mode yaitu mode normal (*enable acces*), dan mode menutup akses (*disable acces*).

1. Pengujian *port knocking*

a. Pengujian *port knocking* mode normal

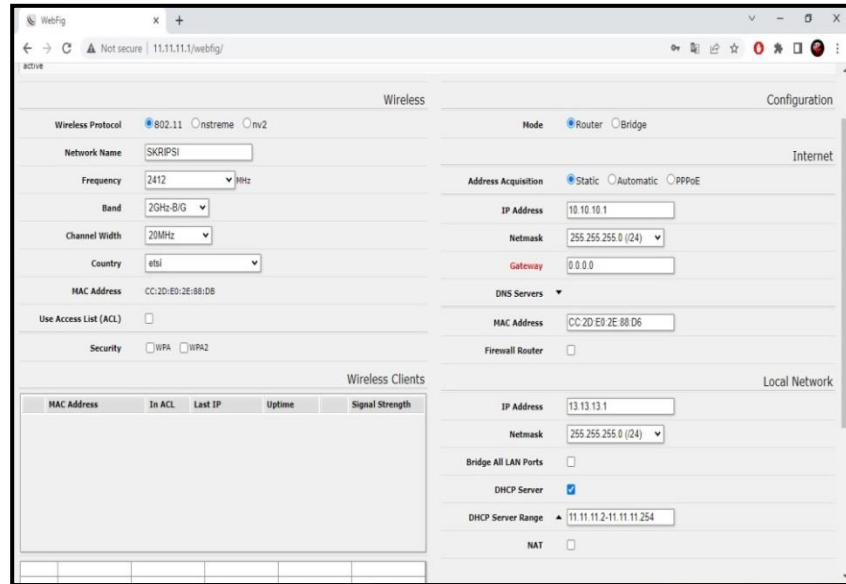
Pengujian *port knocking* dilakukan pada *Router* mikrotik dengan alamat (11.11.11.1/24). Dari hasil uji coba melakukan proses *login* kedalam mikrotik jalur winbox (8921) berjalan lancar tanpa ada halangan apapun.

Begitupula ketika melakukan proses *login* mikrotik jalur *webpage* (80) dan jalur *telnet* (23) juga berjalan dengan baik. Berikut ini Tampilan saat melakukan proses *login* mikrotik menggunakan aplikasi winbox.



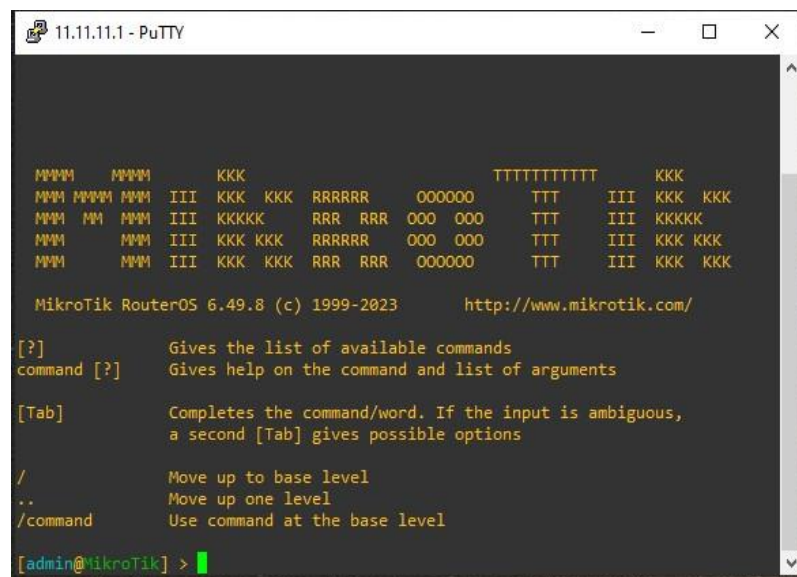
Gambar 4.2 Hasil *login* winbox mode normal

Gambar 4.2 memperlihatkan konfigurasi *port knocking* dalam mode *disable*.



Gambar 4.3 *login* mikrotik via web

Gambar 4.3 memperlihatkan hasil *login* mikrotik dengan menggunakan *web browser*.



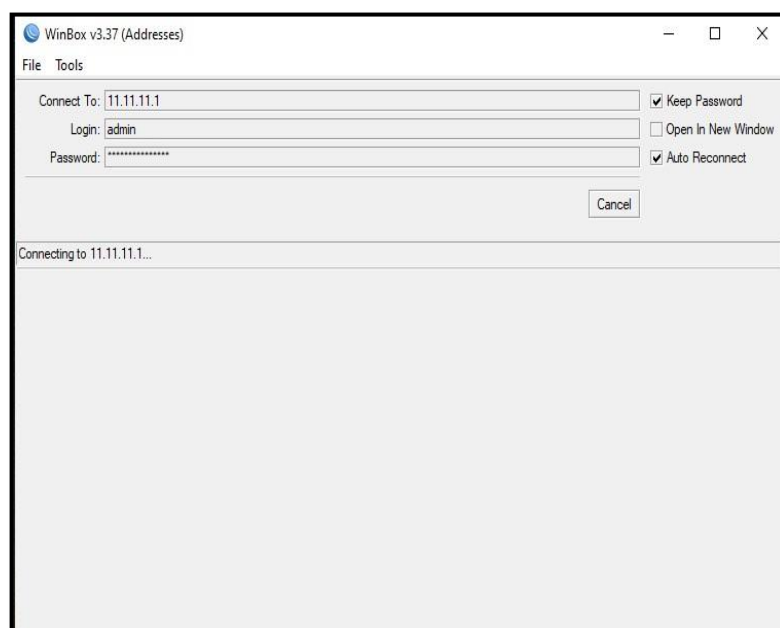
Gambar 4.4 *Login* mikrotik jalur *telnet*

Gambar 4.4 memperlihatkan hasil *login* mikrotik dengan menggunakan *telnet*.

b. Pengujian *port knocking mode enable*

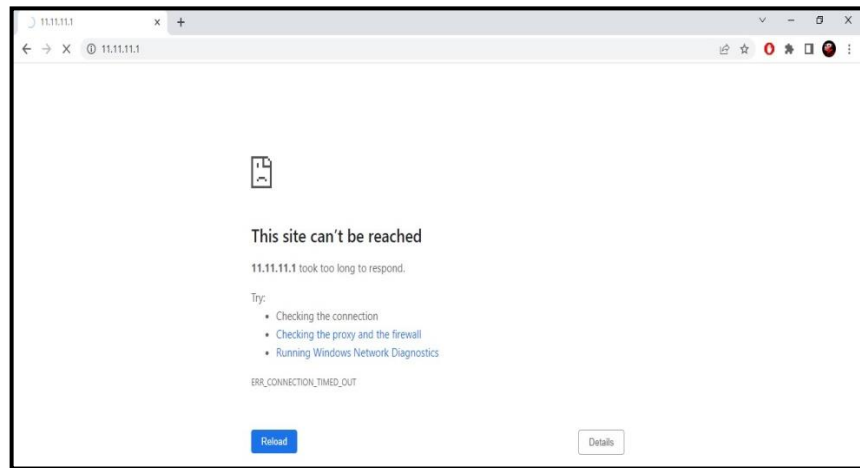
Pada bagian ini pengujian *port knocking* dilakukan pada *Router* mikrotik dengan alamat (11.11.11.1/24). Dari hasil uji coba melakukan proses *login* kedalam mikrotik jalur winbox (8921) terdapat permasalahan dan tidak dapat berjalan.

Begitupula ketika melakukan proses *login* mikrotik jalur *webpage* (80) dan jalur *telnet* (23) juga tidak dapat berjalan. Pada tahap ini menjelaskan bahwa *rule port knocking* sudah berjalan dengan baik. Berikut ini Tampilan saat melakukan proses *login* mikrotik tanpa melakukan proses pengetukan port menggunakan aplikasi winbox.



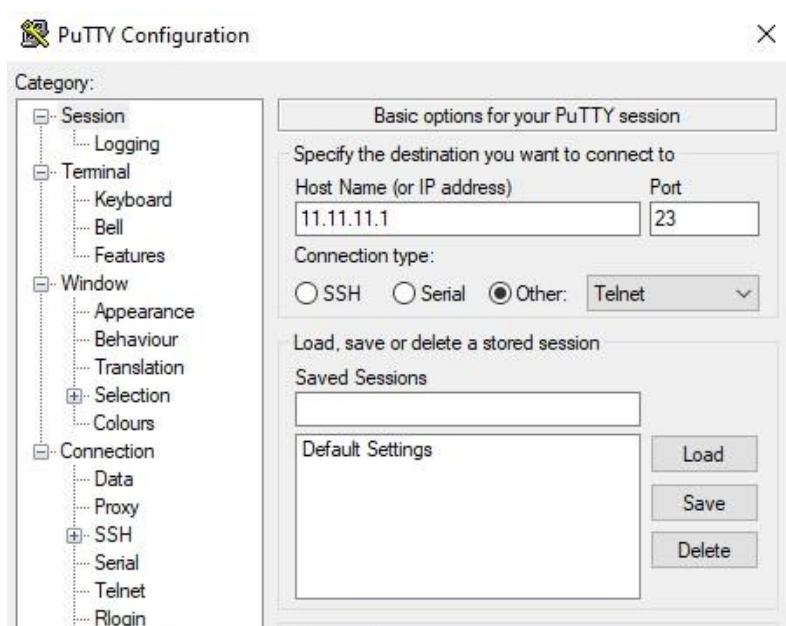
Gambar 4.5 Gagal *Login* mikrotik via winbox

Gambar 4.5 memperlihatkan hasil *login* mikrotik ketika *firewall port knocking* di jalankan mengakibatkan gagal login sebelum port tertentu diketuk terlebih dahulu.



Gambar 4.6 Gagal *login* mikrotik dari *webpage*

Gambar 4.6 memperlihatkan hasil *login* mikrotik dengan menggunakan *web browser* mengalami gagal login.



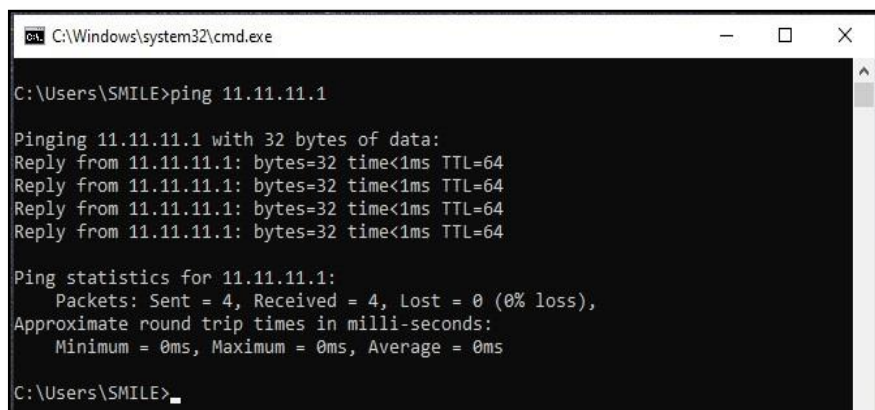
Gambar 4.7 *login* mikrotik jalur *telnet*

Gambar 4.7 memperlihatkan hasil *login* dan digambarkan 4.8 memperlihatkan hasil mikrotik dengan menggunakan *telnet* mengalami gagal login.



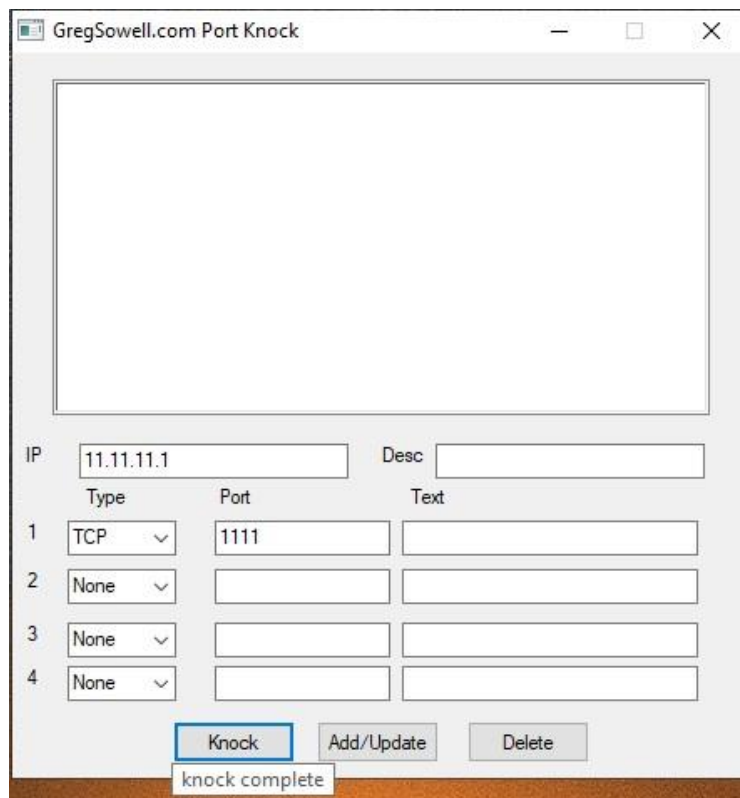
Gambar 4.8 Gagal *login* mikrotik jalur *telnet*

Setelah memastikan keberhasilan *rule port knocking* dalam menangkal seorang *user* melakukan *login* kedalam *Router* tanpa pengetukan port terlebih dahulu. Selanjutnya berikut ini proses *login* kedalam *server Router* dengan metode *port knocking*.



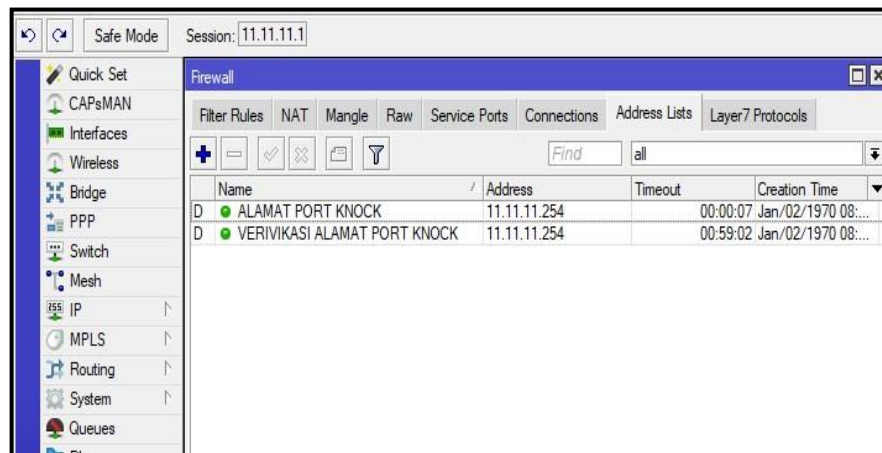
Gambar 4.9 *Ping* terhadap *port service*

Gambar 4.9 di atas menjelaskan proses *ping* terhadap alamat dari *server* mikrotik yang bertujuan untuk memanggil konfigurasi *rule* pertama. Tujuan dari *ping* ini agar *IP Address* dari *device* terfilter dan agar dapat melakukan pemanggilan konfigurasi ke dua.



Gambar 4.10 Aplikasi *Port knocking Client*

Gambar 4.10 aplikasi *port knocking client* ini berfungsi untuk memanggil *rule* kedua yang telah diterapkan pada mikrotik *server*. Setelah *IP Address device* telah terfilter oleh *rule* pertama, langkah selanjutnya adalah memanggil *rule* kedua dengan melakukan *knock* terhadap port 1111. Sehingga *IP Address device* dapat terverifikasi oleh *rule* ke dua.



Gambar 4.11 Berhasil *Login* Mikrotik

Setelah berhasil melakukan pemanggilan *rule* tahap satu dan dua, yang dibuktikan oleh gambar 4.11 melakukan proses *login* kedalam mikrotik *Router*. Didalam *tab address list* telah muncul *verifikasi* terhadap *IP Address device* yang menandakan proses knocking berhasil.

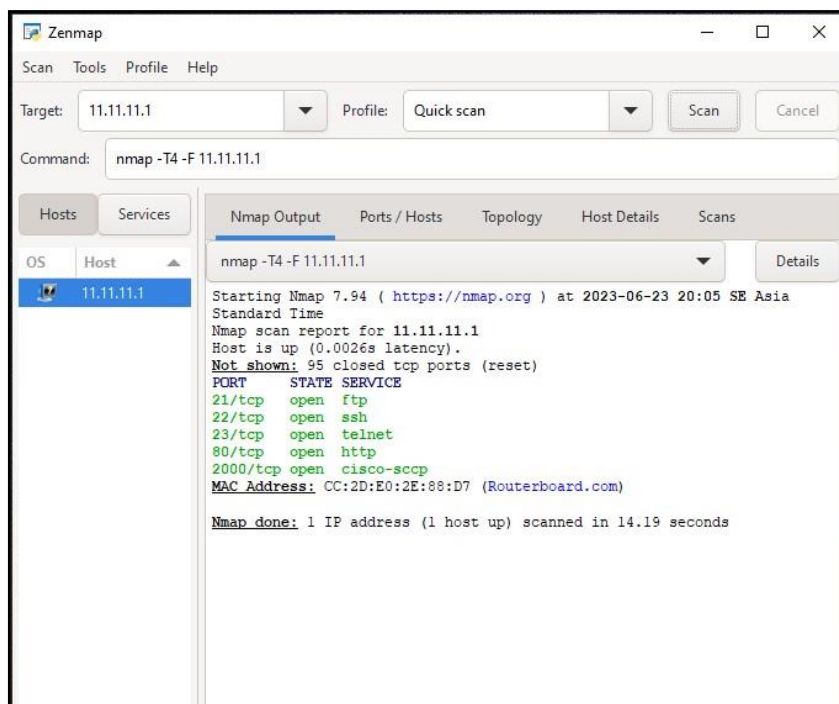
2. Pengujian *scan port*

a. Pengujian *scan port mode normal*

Tahap ini melakukan uji coba *scanning* terhadap *Router* mikrotik guna untuk mendapatkan informasi terkait port mana saja yang bisa digunakan untuk mendapatkan celah serta data dari sebuah *server*. Penggunaan port dalam sebuah *server* bisa sangat beragam seperti halnya untuk monitoring *server* dari jarak jauh. Menjalankan aplikasi, pelacakan data dan sebagainya.

Berdasarkan hasil uji coba yang telah dilaksanakan, didapatkan hasil bahwa port yang ada pada jaringan mode normal

masih bisa *discan* dan terbaca. Adapun hasil dari *scanning* bisa terlihat pada gambar 4.12:



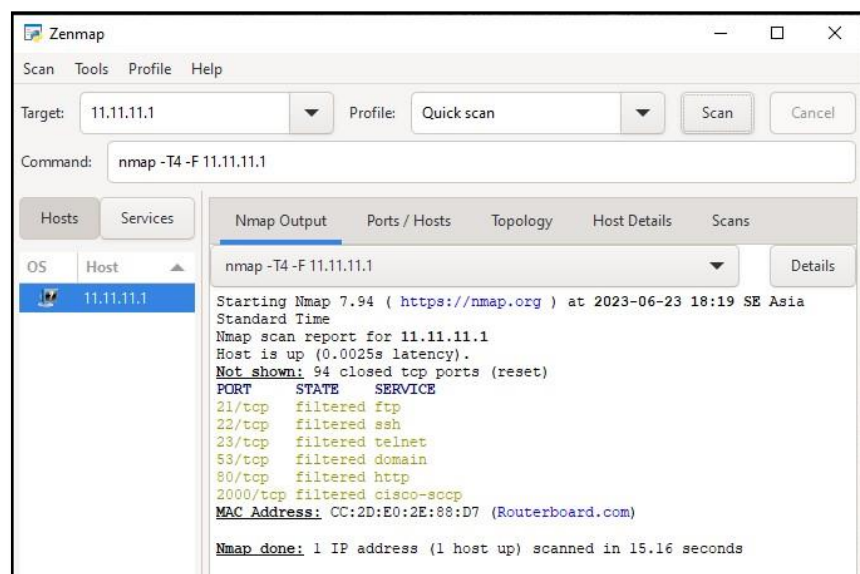
Gambar 4.12 Hasil *Scan port Router*

Gambar 4.12 memperlihatkan hasil scan port terbuka ketika *port knocking mode disable*.

b. Pengujian *scan port mode enable*

Tahap ini melakukan uji coba *scanning* terhadap *Router mikrotik* guna untuk mendapatkan informasi terkait port mana saja yang bisa digunakan untuk mendapatkan celah serta data dari sebuah *server*. Penggunaan port dalam sebuah *server* bisa sangat beragam seperti halnya untuk monitoring *server* dari jarak jauh. Menjalankan aplikasi, pelacakan data dan sebagainya.

Berdasarkan hasil uji coba yang telah dilaksanakan, didapatkan hasil bahwa port yang ada pada jaringan mode *enable* sudah tidak bisa *discan* dan tidak terbaca. Adapun hasil dari *scanning* sebagai berikut :



Gambar 4.13 Hasil *Scan* port *Router* mode *disable*

Gambar 4.13 memperlihatkan hasil scan port tertutup ketika *port knocking* mode *disable*.

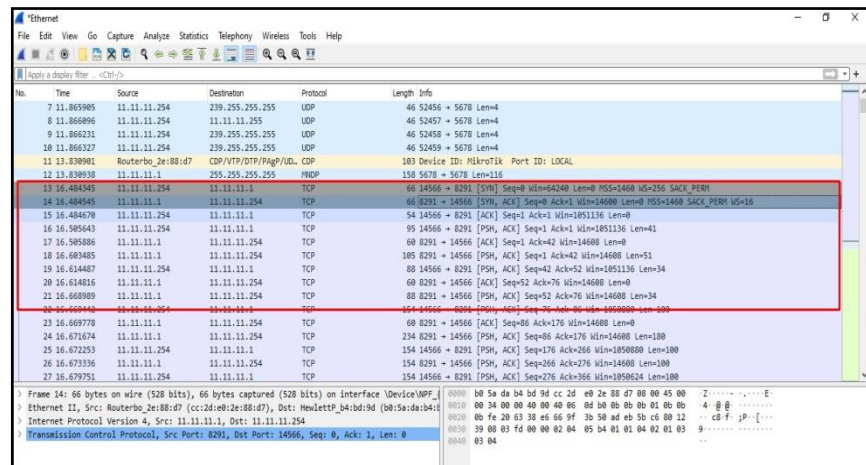
3. Pengujian *sniffing*

a. Pengujian *sniffing* mode normal

Setelah mengetahui port mana saja yang terbuka dari sebuah *server*, langkah selanjutnya adalah melakukan pencurian data atau biasa disebut *sniffing*. Dari hasil uji coba *sniffing* terhadap mikrotik *Router* didapatkan hasil bahwa ketika *Router* mikrotik di akses dari

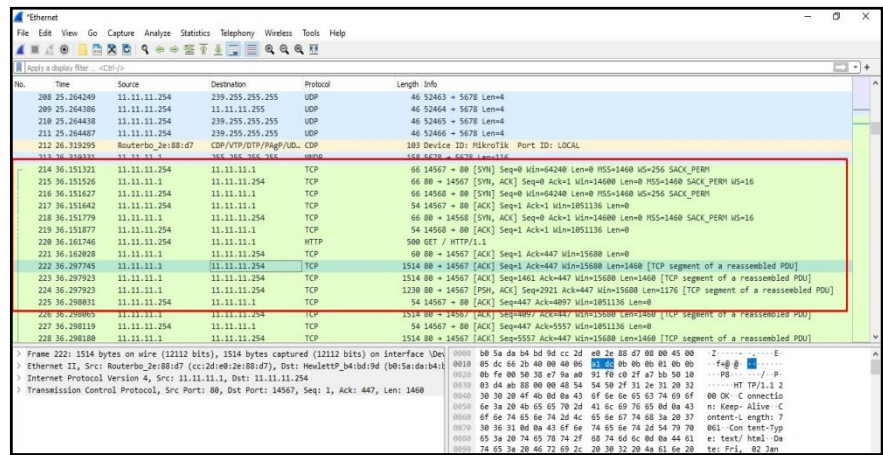
jalur winbox (8291), *telnet* (23), atau *webpage* (80) memungkinkan terjadinya pencurian data sangatlah besar.

Dalam tahap pengujian proses *sniffing* kali ini proses pencurian data dapat dilaksanakan dengan baik. Akan tetapi hasil yang bisa di baca secara langsung oleh aplikasi *wireshark* hanya data pada *login telnet* sedangkan untuk data *login* dari winbox dan *webpage* masih terenkripsi. Seperti yang terlihat pada gambar 4.14.

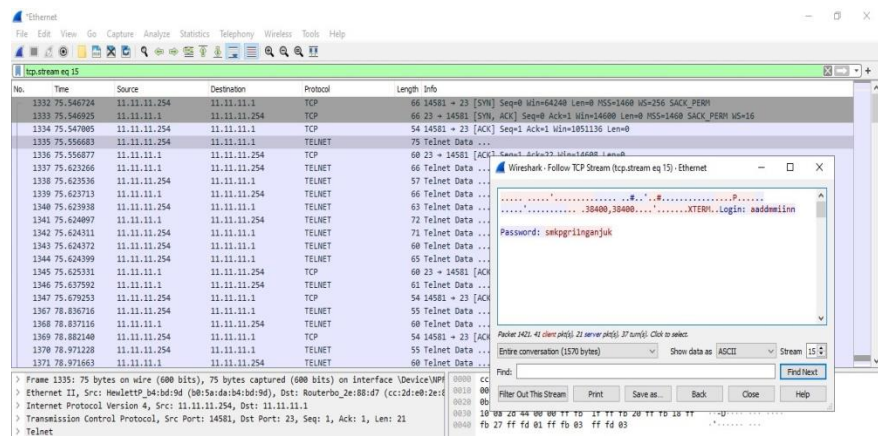


Gambar 4.14 Hasil *Sniffing Router* jalur winbox

Dari Gambar 4.14 terlihat hasil *sniffing* berjalan dengan baik, akan tetapi proses *hash* masih belum berhasil dilakukan karena terlihat pada gambar 4.14 dan 4.15 hasil dari proses *sniffing* masih *terenkripsi* yang menjadikan data tersebut tidak mudah dibaca.



Gambar 4.15 Hasil sniffing Router jalur webpage



Gambar 4.16 Hasil Sniffing Router jalur telnet

Dari gambar 4.16 hasil data yang didapatkan dari hasil sniffing jalur telnet didapatkan *username* dan *password* dari seorang admin jaringan. Yang bisa digunakan oleh *attacker* untuk melakukan *login* terhadap jaringan mikrotik Router.

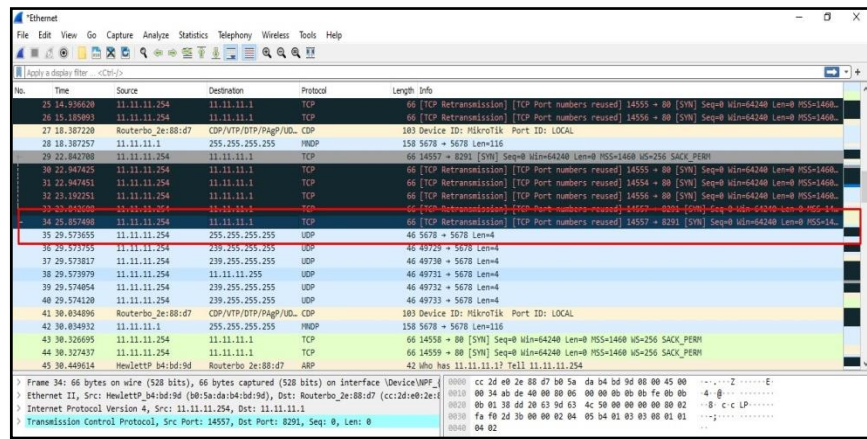
b. Pengujian sniffing mode enable

Dari hasil uji coba sniffing terhadap mikrotik Router didapatkan hasil bahwa ketika Router mikrotik di akses dari jalur

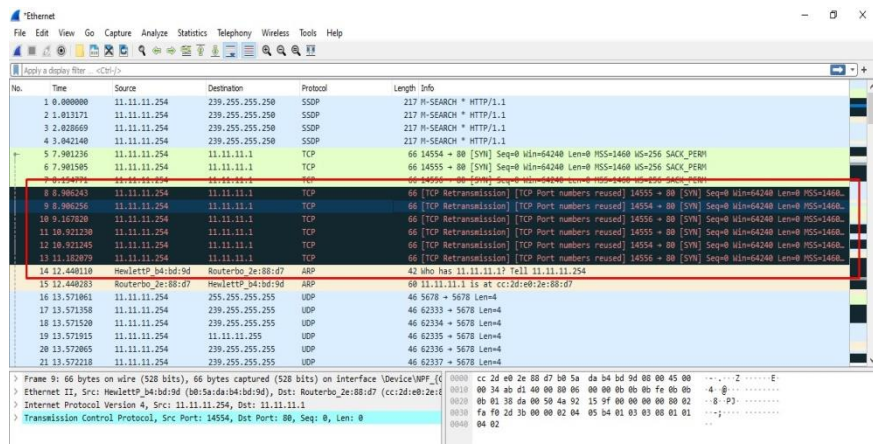
winbox (8291), *telnet* (23), atau *webpage* (80) memungkinkan terjadinya pencurian data sangatlah besar.

Akan tetapi dalam tahap pengujian proses *sniffing* kali ini proses pencurian data tidak dapat dilaksanakan dengan baik.

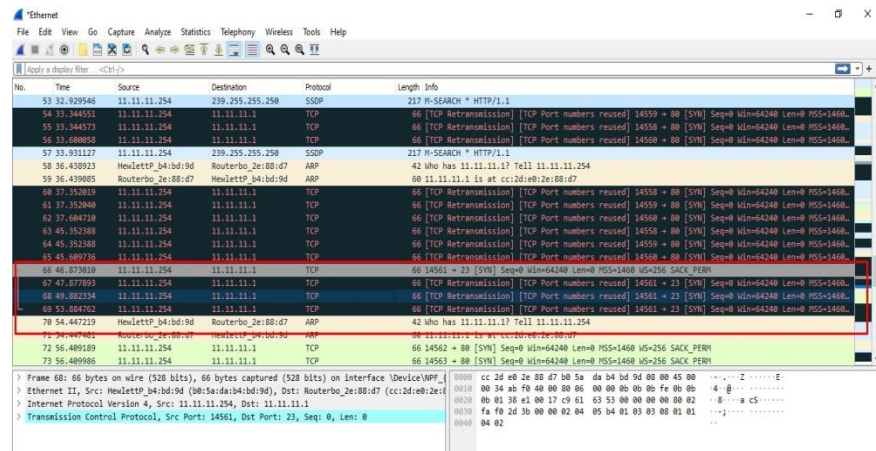
Alasannya adalah terjadinya *error* dalam pembacaan port dan mengakibatkan kebuntuan sistem pencurian data terhadap *Router* mikrotik. Seperti yang terlihat pada gambar 4.17. dan 4.18



Gambar 4.17 Hasil *Sniffing Router* jalur winbox



Gambar 4.18 Hasil *Sniffing Router* jalur webpage



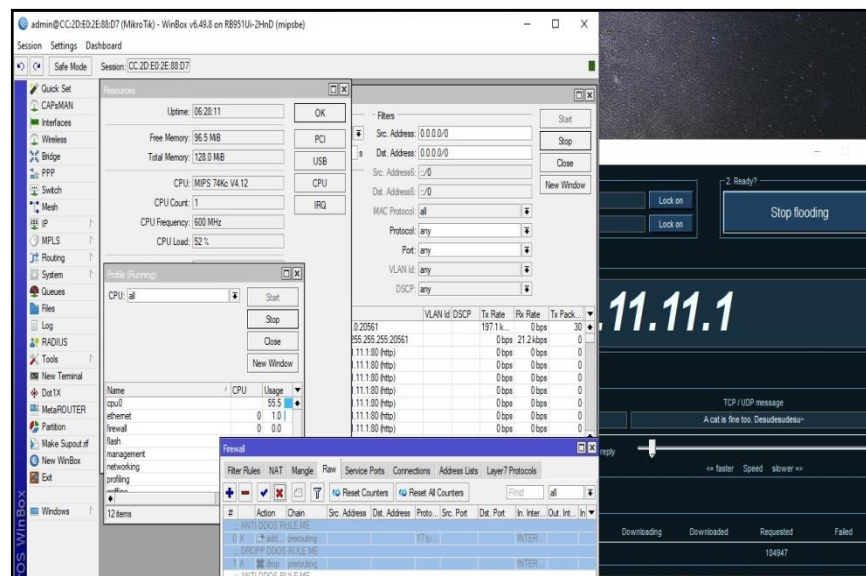
Gambar 4.19 Hasil *Sniffing Router* jalur *telnet*

Dari gambar 4.19 diatas diper oleh hasil hash data yang didapatkan dari hasil sniffing jalur telnet tidak didapatkan username dan password dari seorang admin jaringan.

4. Pengujian DDOS

a. Pengujian mode normal

Setelah implementasi *port knocking* telah selesai, tahap selanjutnya adalah pengujian keamanan jaringan terhadap serangan DDOS. Pada tahap pengujian kali ini dengan cara menonaktifkan *rule raw* anti DDOS yang telah dibuat sebelumnya, sehingga didapatkan hasil seperti pada gambar 4.20 :

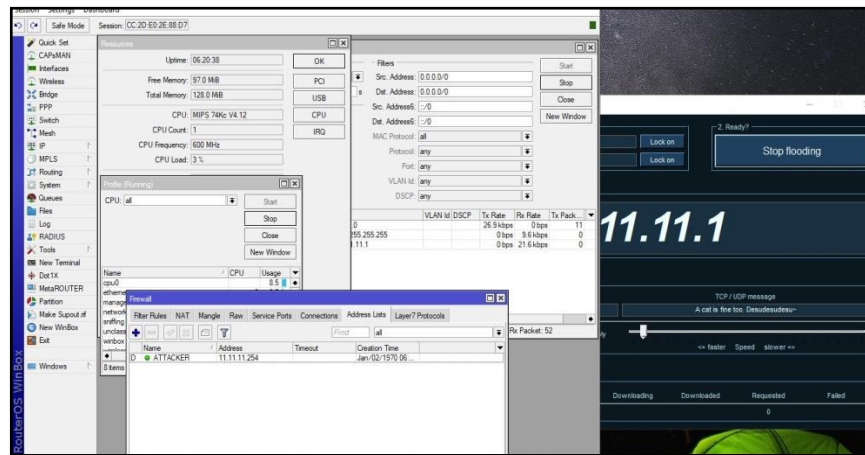


Gambar 4.20 Hasil DDOS Router mode normal

Pada gambar 4.20 sangat terlihat pengiriman paket data yang luar biasa banyak yang dilakukan oleh *attacker*. Dan mengakibatkan *load cpu* dari mikrotik menjadi besar. Dalam tahap simulasi serangan DDOS ini menggunakan aplikasi LOIC.

b. Pengujian *rule anti DDOS aktif*

Setelah melihat betapa efektifnya serangan DDOS untuk melemahkan atau *mentakedown* mikrotik Router. Oleh karena itu pada tahap pengujian selanjutnya dilakukan dengan cara mengaktifkan *rule raw* anti DDOS yang telah dibuat sebelumnya, sehingga didapatkan hasil seperti pada gambar 4.21 :



Gambar 4.21 Implementasi anti DDOS

Setelah di aktifkannya *rule raw* yang telah dibuat untuk menangkal adanya serangan DDOS. Kondisi *server* mikrotik berangsur-angsur kembali normal. *Load cpu* yang kecil dan tidak terjadi pengiriman paket yang berlebihan terhadap *server* yang menjadikan *server* kembali normal. Dari *rule* yang telah dibuat pada Tabel *address list* muncul alamat dari seorang *attacker* yang memudahkan seorang admin jaringan untuk melaksanakan tindakan selanjutnya.

B. Monitoring

Setelah dilakukannya tahap pengujian, tahapan ini berfokus pada dilakukannya monitoring terhadap :

1. *Topologi* yang sudah dibuat.
2. Konfigurasi yang sudah di terapkan dan di uji coba.
3. Insfratruktur yang sudah dibuat

Dengan dilakukannya monitoring terhadap poin-poin diatas diharapkan hasil dari implementasi *port knocking* dapat berjalan sesuai dengan fungsi dan harapan serta memenuhi kebutuhan.

C. Management

Pada tahap *management* merupakan tahapan terakhir, yang dimana perlu dibuatkan sebuah kebijakan *management* untuk mengawasi serta mengatur sistem yang sudah dikembangkan agar dapat berjalan dengan baik dan dapat dikembangkan lagi dikemudian hari.

D. Pembahasan

Berdasarkan hasil dari analisa dan pengujian sistem yang telah dilakukan diatas, diperoleh hasil bahwa konfigurasi *port knocking* dapat berfungsi dengan baik. Melihat hasil pengujian, pada tabel 4.1 saat jaringan berada pada mode normal *Router* dapat dilakukannya *port scan*, *sniffing* dan berhasil *login*. Dan berkebalikan dari mode normal, pada saat mode *disable acces*, *Router* tidak dapat dilakukannya *port scan*, *sniffing* maupun *login* juga tidak berhasil.

Selain dari hasil pengujian sistem *port knocking* didapatkan juga hasil bahwa dari sistem anti DDOS juga berfungsi sesuai harapan. Dari hasil yang didapatkan dalam hasil pengujian *prototype* serangan DDOS juga sudah berkurang dampaknya dan dapat dicegah dengan cara mengetahui pelaku dan bisa di lakukan blokir terhadap pengguna tersebut. Adapun hasil dari tahap pengujian bisa dilihat pada Tabel berikut ini.

Tabel 4.1 Hasil Pengujian

No	Mode Acces	Jenis Pengujian	Alat Uji	Hasil Pngujian
	Mode Normal	<i>Port knocking</i>	<i>Port knocking Client</i>	Berhasil <i>login</i> dan normal
	Mode Normal	<i>Scan Port</i>	<i>Nmap</i>	Semua port service terlihat dan terbuka.
	Mode Normal	<i>Sniffing</i>	<i>Wireshark</i>	Terenkripsi keseluruhan data kecuali dari paket <i>telnet</i> .
	Mode Normal	DDOS	LOIC	Kinerja cpu menjadi besar dan banyak paket yang masuk kedalam <i>Routerbord</i> . Mengakiabtkan <i>Router</i> menjadi panas dan tidak berfungsi.
	Mode <i>Disable</i>	<i>Port knocking</i>	<i>Port knocking Client</i>	Gagal <i>Login</i> , diperlukan proses knock.
	Mode <i>Disable</i>	<i>Scan Port</i>	<i>Nmap</i>	Semua port service <i>filtered</i> .
	Mode <i>Disable</i>	<i>Sniffing</i>	<i>Wireshark</i>	Terenkripsi keseluruhan data tanpa terkecuali
	Mode <i>Disable</i>	DDOS	LOIC	Kinerja cpu menjadi ringan dan berhasil mengamankan alamat <i>attacker</i> tersebut.

BAB V

PENUTUP

Bab ini merupakan bab terakhir yang berisi keinginan dan harapan peneliti demi kelancaran pelaksanaan penelitian. Berdasarkan rumusan masalah yang terjadi serta dilakukannya implementasi sistem yang diusulkan maka dapat di ambil kesimpulan sebagai berikut :

A. KESIMPULAN

1. Sistem peningkatan *firewall* jaringan yang diusulkan yaitu pengembangan *port knocking* serta penambahan *firewall* anti DDOS berhasil diterapkan dan sesuai dengan analisa permasalahan yang terjadi sehingga menghasilkan peningkatan *firewall* untuk sistem yang berjalan.
2. Pembuatan rule *port knocking* dan rule anti DDOS sebagai alternative agar tidak sembarangan orang bisa mengakses mikrtokik dan sebagai penangkal serangan DDOS berjalan dengan baik.
3. Hasil analisa dari penggunaan *port knocking* telah dikembangkan sehingga menghasilkan sebuah konfigurasi yang lebih baik dari sebelumnya.
4. Hasil dari penerapan *port knocking* serta anti DDOS sangat berguna untuk memperkuat keamanan jaringan di SMK PGRI 1 Nganjuk.
5. Dalam proses penerapan *port knocking* dan anti DDOS serta hasil wawancara dan implementasi didapatkan hasil yang memuaskan.

B. SARAN

Untuk mengantisipasi kesalahan-kesalahan di kemudian hari, khususnya dalam perawatan *hardware* serta *software*, dan perawatan layanan jaringan komputer maka perlu dilakukan beberapa hal sebagai berikut :

1. Dilakukan perawatan pada perangkat keras secara berkala.
2. Perlu adanya informasi jatuh tempo secara otomatis layanan berlangganan jaringan komputer demi kenyamanan.
3. Diperlukannya pengujian yang dilakukan menggunakan *tools hacking* lainnya yang lebih tinggi tingkat teknologinya.
4. Selain itu juga perlu dilakukan pengembangan metode *port knocking* yang digunakan.

DAFTAR PUSTAKA

- Amarudin, & Atri. (2018). Analisis Penerapan Mikrotik Router Sebagai User Manager Untuk Menciptakan Internet Sehat Menggunakan Simulasi Virtual Machine. *Jurnal TAM (Technology Acceptance Model)*, 62-66.
- Amarudin, & Ulum, F. (2018). Desain Keamanan Jaringan Pada Mikrotik Router Os. *Jurnal TEKNOINFO*, 72-75.
- Bambang Bagus Harianto, S. M., & Suminar Pujowati, S.Pd., MM. (2021). *Pengenalan Dasar Jaringan Komputer*. Jawa Tengah, Indonesia: Pustaka Rumah C1nta.
- cisco. (2014, april 14). *cisco*. Retrieved 7 3, 2023, from cisco.com:
https://www.cisco.com/c/en/us/products/collateral/routers/wide-area-application-services-waas-software/data_sheet_c78-704923.html
- Dewi, N. K., & Putra, A. S. (2021). Pengembangan Sistem Jaringan Menggunakan Local Area Network Untuk Meningkatkan Pelayanan (Studi Kasus di PT. ARS Solusi Utama). *TEKINFO Vol. 22*, 66-79.
- Indonesia, C. N. (2022, Agustus 2). Retrieved 1 10, 2023, from cni.net.id:
<https://cni.net.id/berita/detail/pengertian-mengenai-keamanan-jaringan#:~:text=Sistem%20keamanan%20jaringan%20merupakan%20sebuah,mengakses%20sistem%20jaringan%20komputer%20kita.>
- Kompirasi. (2022, September 22). Retrieved Januari 10, 2023, from Kompirasi Media: <https://www.kompirasi.com/inilah-jenis-jenis-serangan-jaringan-pada-komputer/>
- morning. (2023, 3 10). *Morning Computer*. Retrieved 7 3, 2023, from <https://morning.computer>: <https://morning.computer/metropolitan-area-network/>
- Ramadhani, F., & Tadjuddin, A. M. (2018). Analisis Dan Implementasi Firewall Dengan Metode Port Address Translation Pada Mikrotik OS. *Universitas Muhammadiyah Makassar*.
- Sanjaya, T., & Setiyadi, D. (2019). etwork Development Life Cycle (NDLC) Dalam Perancangan Jaringan Komputer Pada Rumah Shalom Mahanaim. *Jurnal Mahasiswa Bina Insani*, 1-10.

- Saputro, A., Saputro, N., & Wijayanto, H. (2020). Metode Demilitarized Zone Dan *Port knocking* Untuk Keamanan Jaringan Komputer. *CyberSecurity dan Forensik Digital*, 22-27.
- SELAMATPAGI.ID. (2020, Mei 27). *Teknologi*. Retrieved Januari 10, 2023, from www.selamatpagi.id: <https://www.selamatpagi.id/pengertian-wan-wide-area-network/#!>
- Syafrizal, M. (2020). *Pengantar Jaringan Komputer*. Yogyakarta: ANDI.
- Teddy. (2020). Analisis Keamanan Jaringan Wireless Fidelity Sekolah Menengah Atas Negeri 10 Luwu. *Fakultas Teknik Komputer Universitas Cokroaminoto Palopo*.
- Trimadani, P. (2020). IMPLEMENTASI KEAMANAN JARINGAN PADA MIKROTIK ROUTER OS MENGGUNAKAN METODE *PORT KNOCKING* DIASRAMA JAMBI SULTAN TAHA SYAEFUDDIN (. *Universitas AMIKOM Yogyakarta*.
- trivus. (2022, September 18). Retrieved Januari 2023, 10, from trivus web ID: <https://www.trivusi.web.id/2022/08/tcp-ip-model.html>
- Trivusi. (2022, September 17). Retrieved januari 10, 2022, from Trivusi Web ID: <https://www.trivusi.web.id/2022/08/network-address-translation.html>

LAMPIRAN

1. Daftar Validasi Pertanyaan

LEMBAR VALIDASI PEDOMAN WAWANCARA

ANALISIS IMPLEMENTASI METODE PORT KNOCKING DENGAN SISTEM ROUTING DINAMIS DAN ANTI DDOS MENGGUNAKAN PROTOKOL TCP DAN ICMP PADA KEAMANAN JARINGAN SMK PGRI 1 NGANJUK

Nama Validator : FEBRINA EKA CAHYARISTI, S.Pd.

Ahli Bidang : Pendidikan Bahasa Indonesia

Unit Kerja : SMK PGRI 1 NGANJUK

A. PENILAIAN TERHADAP KONTRUKSI PEDOMAN WAWANCARA
 S = Setuju TS : Tidak Setuju

NO	Kriteria Penilaian	Skala Penilaian		Saran/Perbaikan
		S	TS	
	Pedoman wawancara dirumuskan dengan jelas.	✓		
	Pedoman wawancara mencakup aspek : a. Lokasi b. penjelasan c. Permasalahan d. Masukan	✓		
	Batasan pedoman wawancara dapat menjawab tujuan penelitian.	✓		

B. PENILAIAN TERHADAP PENGGUNAAN BAHASA
 S = Setuju TS : Tidak Setuju

NO	Kriteria Penilaian	Skala Penilaian		Saran/Perbaikan
		S	TS	
	Pedoman wawancara	✓		

	menggunakan bahasa Indonesia yang sesuai dengan kaidah bahasa yang baik dan benar.	✓		
	Pedoman wawancara menggunakan bahasa yang mudah dipahami dan dimengerti.	✓		
	Pedoman wawancara menggunakan bahasa yang komunikatif	✓		
	Pedoman wawancara bebas dari pernyataan yang dapat menimbulkan penafsiran ganda.	✓		

C. PENILAIAN TERHADAP MATERI PEDOMAN WAWANCARA

Berilah tanda centan (✓) pada tempat yang tersedia dengan penilaian Bapak/Ibu.

S = Setuju

TS : Tidak Setuju

NO	Kriteria Penilaian	Skala Penilaian		Saran/Perbaikan
		S	TS	
	Pedoman wawancara dapat menggali aspek-aspek teknologi jaringan internet.	✓		
	Pedoman wawancara dapat menggali informasi untuk mendeskripsikan permasalahan dalam penggunaan fasilitas internet di SMK PGRI 1 Nganjuk.	✓		



Secara umum pedoman wawancara ini :

(Mohon berikan tanda centang (✓) sesuai penilaian Bapak/Ibu)

LD	: Layak Digunakan	✓
LDR	: Tidak Layak Digunakan dengan Revisi	
TD	: Tidak Layak Digunakan	

Nganjuk, Juni 2023



EBRINA EKA CAHYARISTI, S.Pd.
NIP.

2. Hasil Pertanyaan Guru



DAFTAR PERTANYAAN WAWANCARA GUNA UNTUK PENELITIAN SKRIPSI

"ANALISIS IMPLEMENTASI METODE PORT KNOCKING DENGAN SISTEM ROUTING DINAMIS DAN ANTI DDOS MENGGUNAKAN PROTOKOL TCP DAN ICMP PADA KEAMANAN JARINGAN SMK PGRI 1 NGANJUK"

A. Petunjuk pelaksanaan :

Jawablah pertanyaan berikut ini sesuai dengan kondisi yang anda alami.

Nomor Responden : 03
 Nama : Nirna Ari Kusrianda
 Jenis Kelamin : Laki-Laki / Perempuan
 Pekerjaan : Guru / Staff / Siswa
 Sekolah : SMK PGRI 1 Nganjuk

1. Apakah akses internet di SMK PGRI 1 Nganjuk sudah dapat memenuhi kebutuhan anda dalam melakukan pencarian data di internet saat ini? Sudah
2. Dalam penerapan fasilitas internet di SMK PGRI 1 Nganjuk, menurut anda seberapa sering terjadi gangguan dalam koneksi internet yang anda gunakan? 20% sering terjadi
3. Jika dalam pelaksanaannya sering terjadi kendala, seberapa sering terjadi gangguan dalam 1 bulan terakhir? 2 gangguan
4. Dalam situasi tertentu apakah anda pernah mengalami kejadian seperti kehilangan data, atau gangguan lain seperti internet yang tiba-tiba blank atau ada akun media social anda yang bermasalah? yo pernah
5. Menurut anda seberapa besar tingkat kenyamanan yang anda rasakan selama menggunakan internet di SMK PGRI 1 Nganjuk? 90%
6. Bagaimana menurut anda akses dengan menggunakan fasilitas area hotspot di area SMK PGRI 1 Nganjuk? sangat baik

3. Hasil Pertanyaan Staff



DAFTAR PERTANYAAN WAWANCARA GUNA UNTUK PENELITIAN SKRIPSI

"ANALISIS IMPLEMENTASI METODE PORT KNOCKING DENGAN SISTEM ROUTING DINAMIS DAN ANTI DDOS MENGGUNAKAN PROTOKOL TCP DAN ICMP PADA KEAMANAN JARINGAN SMK PGRI 1 NGANJUK"

A. Petunjuk pelaksanaan :

Jawablah pertanyaan berikut ini sesuai dengan kondisi yang anda alami.

Nomor Responden : 2
 Nama : Hiki Dwinas
 Jenis Kelamin : Laki-Laki / Perempuan
 Pekerjaan : Guru / Staff / Siswa
 Sekolah : SMK PGRI 1 Nganjuk

1. Apakah akses internet di SMK PGRI 1 Nganjuk sudah dapat memenuhi kebutuhan anda dalam melakukan pencarian data di internet saat ini? belum
2. Dalam penerapan fasilitas internet di SMK PGRI 1 Nganjuk, menurut anda seberapa sering terjadi gangguan dalam koneksi internet yang anda gunakan? sering
3. Jika dalam pelaksanaannya sering terjadi kendala, seberapa sering terjadi gangguan dalam 1 bulan terakhir? 7 buah
4. Dalam situasi tertentu apakah anda pernah mengalami kejadian seperti kehilangan data, atau gangguan lain seperti internet yang tiba-tiba blank atau ada akun media social anda yang bermasalah? pernah
5. Menurut anda seberapa besar tingkat kenyamanan yang anda rasakan selama menggunakan internet di SMK PGRI 1 Nganjuk? 70%
6. Bagaimana menurut anda akses dengan menggunakan fasilitas area hotspot di area SMK PGRI 1 Nganjuk? Cukup

4. Hasil Pertanyaan Siswa



DAFTAR PERTANYAAN WAWANCARA GUNA UNTUK PENELITIAN SKRIPSI

“ANALISIS IMPLEMENTASI METODE PORT KNOCKING DENGAN SISTEM ROUTING DINAMIS DAN ANTI DDOS MENGGUNAKAN PROTOKOL TCP DAN ICMP PADA KEAMANAN JARINGAN SMK PGRI 1 NGANJUK”

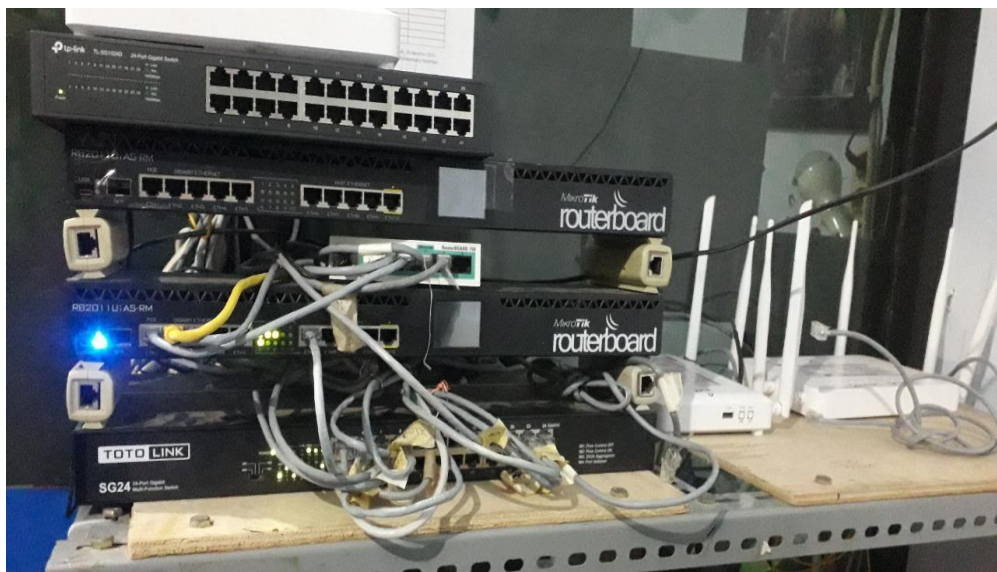
A. Petunjuk pelaksanaan :

Jawablah pertanyaan berikut ini sesuai dengan kondisi yang anda alami.

Nomor Responden : SAHRU SETIABUDI
Nama : SAHRU SETIABUDI
Jenis Kelamin : Laki-Laki / Perempuan
Pekerjaan : Guru / Staff / Siswa
Sekolah : SMK PGRI 1 Nganjuk

1. Apakah akses internet di SMK PGRI 1 Nganjuk sudah dapat memenuhi kebutuhan anda dalam melakukan pencarian data di internet saat ini ? *Ya*
2. Dalam penerapan fasilitas internet di SMK PGRI 1 Nganjuk, menurut anda seberapa sering terjadi gangguan dalam koneksi internet yang anda gunakan ? *Sering*
3. Jika dalam pelaksanaannya sering terjadi kendala, seberapa sering terjadi gangguan dalam 1 bulan terakhir ? *5 kali*
4. Dalam situasi tertentu apakah anda pernah mengalami kejadian seperti kehilangan data, atau gangguan lain seperti internet yang tiba-tiba blank atau ada akun media social anda yang bermasalah ? *Pernah*
5. Menurut anda seberapa besar tingkat kenyamanan yang anda rasakan selama menggunakan internet di SMK PGRI 1 Nganjuk ? *90%*
6. Bagaimana menurut anda akses dengan menggunakan fasilitas area hotspot di area SMK PGRI 1 Nganjuk ? *baik / cepat*

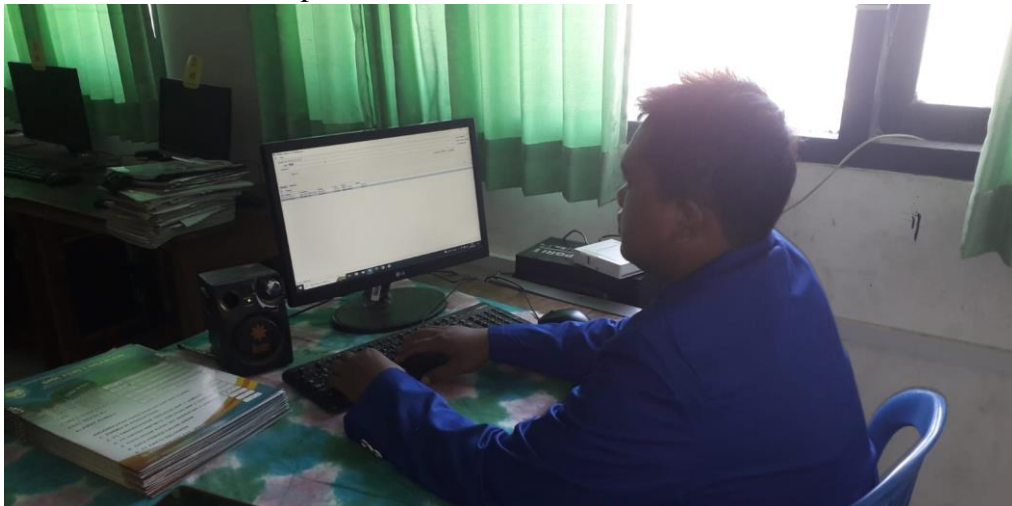
5. Mikrotik Router SMK PGRI 1 Nganjuk



6. Melakukan Tinjauan Langsung Ruang Server



7. Melakukan Penerapan Hasil Penelitian



8. Hasil Penerapan Port Knocking dan Anti DDOS

a. Tanggal 20 Juli 2023

The screenshot shows the Mikrotik WinBox interface for Router/WinBox v7.6 on RB2011UAS. The 'Interface List' window displays the configuration for 10 Ethernet interfaces (ether1 to ether10). The 'Filter Rules' window shows a rule named 'PORT KNOCK TAHAP 1' with the following configuration:

#	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Src. Ad.	Dst. Ad.
0	add	input			1								
1	add	input	6 (ftp)	1111									
2	drop	input	6 (ftp)	21,22,23									IVERV...

The 'Log' window shows a series of system messages indicating user logins and system changes. The 'Filter Rules' window also shows a table of traffic statistics:

Eth.	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pa
800 (p)	6 (ftp)	193.217.148.8:445 (mb)	192.168.1.2:54216			0 bps	0 bps	0	0
800 (p)	6 (ftp)	50.20.18.96:445 (mb)	192.168.1.2:54217			0 bps	0 bps	0	0
800 (p)	6 (ftp)	173.249.57.77:445 (mb)	192.168.1.2:54249			0 bps	0 bps	0	0
800 (p)	17 (udp)	157.240.217.63:443 (https)	192.168.1.2:40867			0 bps	0 bps	0	0

b. Tanggal 21 Juli 2023

The screenshot shows the Mikrotik WinBox interface for Router/WinBox v7.6 on RB2011UAS. The 'Interface List' window displays the configuration for 10 Ethernet interfaces (ether1 to ether10). The 'Filter Rules' window shows a rule named 'PORT KNOCK TAHAP 1' with the following configuration:

#	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Src. Ad.	Dst. Ad.
0	add	input			1								
1	add	input	6 (ftp)	1111									
2	drop	input	6 (ftp)	21,22,23									IVERV...

The 'Log' window shows a series of system messages indicating user logins and system changes. The 'Filter Rules' window also shows a table of traffic statistics:

Eth.	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pa
800 (p)	6 (ftp)	193.217.148.8:445 (mb)	192.168.1.2:54216			0 bps	0 bps	0	0
800 (p)	6 (ftp)	50.20.18.96:445 (mb)	192.168.1.2:54217			0 bps	0 bps	0	0
800 (p)	6 (ftp)	173.249.57.77:445 (mb)	192.168.1.2:54249			0 bps	0 bps	0	0
800 (p)	17 (udp)	157.240.217.63:443 (https)	192.168.1.2:40867			0 bps	0 bps	0	0

c. Tanggal 22 Juli 2023

Session: 10.10.0.1 (1. RB2011UAS) - WinBox v7.6 on RB2011UAS (mipsbe)

Session Settings Dashboard

Safe Mode Session: 10.10.0.1

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN
R	ether1	Ethernet					
R	ether2	Ethernet					
R	ether3	Ethernet					
R	ether4	Ethernet					
R	ether5	Ethernet					
R	ether6	Ethernet					
R	ether7	Ethernet					
R	ether8	Ethernet					
R	ether9	Ethernet					
R	ether10	Ethernet					

Log

Time	Buffer	Topic	Message
11 Jul 22 02:23:14.14:46	system	info	system time settings changed by admin
11 Jul 22 02:23:14.14:54	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.14:56	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.14:59	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:01	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:05	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:08	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:10	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:12	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:15	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:16	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:18	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:20	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:22	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:25	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:27	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:29	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:31	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:34	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:36	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:38	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:41	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:42	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:44	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:47	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:49	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:51	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:52	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:54	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:56	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:58	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
11 Jul 22 02:23:14.15:59	system	info	user admin logged in from 59:51:36.45:47:0C via winbox

Torch

Basic

Interface: ether1

Entry Timeout: 00:00:03

Filters

Src. Address: 0.0.0.0

Det. Address: 0.0.0.0

Src. Address6: ::0

Det. Address6: ::0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Eth	Protocol	Src	Det.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pa
800 (lp)	6 (tcp)	193.217.148.8-445 (amb)	192.168.1.2-54216			0 bps	0 bps	0	0
800 (lp)	6 (tcp)	50.20.18.96-445 (amb)	192.168.1.2-54217			0 bps	0 bps	0	0
800 (lp)	6 (tcp)	173.249.57.77-445 (amb)	192.168.1.2-54249			0 bps	0 bps	0	0
800 (lp)	17 (udp)	157.240.217.63-443 (https)	192.168.1.2-40867			0 bps	0 bps	0	0

125 Items Total Tx: 46.2 kbps Total Rx: 13.3 kbps Total Tx Packet: 34 Total Rx Packet: 16

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters

#	Action	Chain	Src. Address	Det. Address	Proto.	Src. Port	Det. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Src. Ad...
0	add	input			1 (c...							
1	add	input		6 (tcp)	1111							
2	drop	input		6 (tcp)	21,22,23...							VERIV...

d. Tanggal 23 Juli 2023

Session: 10.10.0.1 (1. RB2011UAS) - WinBox v7.6 on RB2011UAS (mipsbe)

Session Settings Dashboard

Safe Mode Session: 10.10.0.1

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN
R	ether1	Ethernet					
R	ether2	Ethernet					
R	ether3	Ethernet					
R	ether4	Ethernet					
R	ether5	Ethernet					
R	ether6	Ethernet					
R	ether7	Ethernet					
R	ether8	Ethernet					
R	ether9	Ethernet					
R	ether10	Ethernet					

Log

Time	Buffer	Topic	Message
12 Jul 23 02:23:23.21:02:02	system	info	user admin logged in from 38:36:36.45:47:0C via winbox
12 Jul 23 02:23:23.01:05:02	system	info	change time Jan 01 2002 01:05:02 + Jul 23 2023 01:05:02
12 Jul 23 02:23:14.14:49	system	info	system time settings changed by admin
12 Jul 23 02:23:14.14:54	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.14:56	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.14:59	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:01	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:05	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:08	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:10	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:12	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:15	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:16	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:18	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:20	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:22	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:25	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:27	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:29	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:31	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:34	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:36	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:38	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:41	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:42	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:44	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:47	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:49	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:51	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:52	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:54	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:56	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:58	system	info	user admin logged in from 59:51:36.45:47:0C via winbox
12 Jul 23 02:23:14.15:59	system	info	user admin logged in from 59:51:36.45:47:0C via winbox

Torch

Basic

Interface: ether1

Entry Timeout: 00:00:03

Filters

Src. Address: 0.0.0.0

Det. Address: 0.0.0.0

Src. Address6: ::0

Det. Address6: ::0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Eth	Protocol	Src	Det.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pa
800 (lp)	6 (tcp)	193.217.148.8-445 (amb)	192.168.1.2-54216			0 bps	0 bps	0	0
800 (lp)	6 (tcp)	50.20.18.96-445 (amb)	192.168.1.2-54217			0 bps	0 bps	0	0
800 (lp)	6 (tcp)	173.249.57.77-445 (amb)	192.168.1.2-54249			0 bps	0 bps	0	0
800 (lp)	17 (udp)	157.240.217.63-443 (https)	192.168.1.2-40867			0 bps	0 bps	0	0

Total Tx: 46.2 kbps Total Rx: 13.3 kbps Total Tx Packet: 34 Total Rx Packet: 16

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Reset Counters Reset All Counters

#	Action	Chain	Src. Address	Det. Address	Proto.	Src. Port	Det. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Src. Ad...
0	add	input			1 (c...							
1	add	input		6 (tcp)	1111							
2	drop	input		6 (tcp)	21,22,23...							VERIV...

e. Tanggal 24 Juli 2023

sidik@10.10.0.1 (1. R82011U4AS) - WinBox v7.6 on R82011U4AS (mipobe)

Session Settings Dashboard

Safe Mode Session: 10.10.0.1

Interface List

Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VXLAN
R	ether1	Ethernet					
R	ether2	Ethernet					
R	ether3	Ethernet					
R	ether4	Ethernet					
R	ether5	Ethernet					
R	ether6	Ethernet					
R	ether7	Ethernet					
R	ether8	Ethernet					
R	ether9	Ethernet					
R	ether10	Ethernet					

11 Items

Freeze

Time Buffer Topics Message

983	Jul/24/2023 15:28:45	memory	dhcp, info	dhcp1 assigned 10.10.7.105 for 24
984	Jul/24/2023 15:29:11	memory	dhcp, info	dhcp1 assigned 10.10.7.92 for 82
985	Jul/24/2023 15:30:08	memory	dhcp, info	dhcp1 deassigned 10.10.0.162
986	Jul/24/2023 15:30:08	memory	dhcp, info	dhcp1 assigned 10.10.0.162
987	Jul/24/2023 15:30:14	memory	dhcp, info	dhcp1 assigned 10.10.7.105
988	Jul/24/2023 15:32:54	memory	dhcp, info	dhcp1 deassigned 10.10.7.10
989	Jul/24/2023 15:34:12	memory	dhcp, info	dhcp1 assigned 10.10.7.90
990	Jul/24/2023 15:39:11	memory	dhcp, info	dhcp1 assigned 10.10.7.93
991	Jul/24/2023 15:40:14	memory	dhcp, info	dhcp1 deassigned 10.10.7.10
992	Jul/24/2023 15:40:29	memory	dhcp, info	dhcp1 assigned 10.10.7.92/14
993	Jul/24/2023 15:42:13	memory	dhcp, info	dhcp1 deassigned 10.10.0.16
994	Jul/24/2023 15:42:13	memory	dhcp, info	dhcp1 assigned 10.10.0.162
995	Jul/24/2023 15:45:09	memory	system, info, account	user sidik logged in from 10.11
996	Jul/24/2023 15:47:00	memory	dhcp, info	dhcp1 assigned 10.10.3.22
997	Jul/24/2023 15:47:02	memory	dhcp, info	dhcp1 assigned 10.10.7.107
998	Jul/24/2023 15:48:40	memory	dhcp, info	dhcp1 deassigned 10.10.7.94
999	Jul/24/2023 15:48:40	memory	dhcp, info	dhcp1 assigned 10.10.7.92/14

1000 Items (1 selected)

Torch

Basic

Interface: ether1

Entry Timeout: 00:00:03

Src. Address: 0.0.0.0

Dst. Address: 0.0.0.0

Src. Address6: ::0

Dst. Address6: ::0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Eth	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pa
800 (p)	6 (tcp)	193.217.148.8-445 (mb)	192.168.1.2-54216			0 bps	0 bps	0	0
800 (p)	6 (tcp)	50.20.18.96-445 (mb)	192.168.1.2-54217			0 bps	0 bps	0	0
800 (p)	6 (tcp)	173.249.57.77-445 (mb)	192.168.1.2-54249			0 bps	0 bps	0	0
800 (p)	17 (udp)	157.240.217.63-443 (mp)	192.168.1.2-40867			0 bps	0 bps	0	0

125 Items Total Tx: 45.2 kbps Total Rx: 13.3 kbps Total Tx Packet: 34 Total Rx Packet: 16

Filter Rules

#	Action	Chain	Src. Address	Dst. Address	Proto.	Src. Port	Dst. Port	In. Inter.	Out. Int.	In. Inter.	Out. Int.	Src. Ad.	Dst. Ad.
0	add	input			1 (c...								
1	add	input			6 (tcp)		1111						
2	drop	input			6 (tcp)		21.22.23...						IVERIV...

31°C Cerah 15:52 24/07/2023