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 :

<u>YANTO SETIAYOKO</u> 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 : Danar 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 diajukjan 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

<u>YANTO SETIAYOKO</u> 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 Setiayoko : 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.
- Yang terhormat Drs. Suryo Widodo, M.Pd., Selaku Dekan FT Universitas Nusantara PGRI Kediri.
- 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.
- Istri tercinta yang selalu memberikan semangat, motivasi, dan kasih sayang dan dukungan yang luar biasa.
- Anakku tercinta dan tersayang yang menjadi motivasi dan semangat dalam menyelesaikan penulisan karya tulis ini.
- 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

Skrips	i Oleh :ii
Skrip	i Oleh :ii
SURA	T PERNYATAANiv
мот	TO PENULISv
Abstr	ackvi
KAT	A PENGANTARvii
DAF	ʿAR ISIix
DAF	AR TABEL
DAF	AR GAMBARxiii
BAB	[1
PENI	PAHULUAN1
A.	Latar Belakang1
В.	Identifikasi Masalah3
C.	Rumusan Masalah4
D.	Batasan Masalah4
E.	Tujuan Penelitian5
F.	Manfaat Dan Kegunaan Penelitian6
G.	Metode Penelitian7
H.	Jadwal Penelitian11
I.	Sistematika Penulisan Laporan11
BAB	П13
TINJ	AUAN PUSTAKA
A.	Dasar Teori13
1	. Analisis13
2	. Lalu Lintas Komputer14
3	. <i>Topologi</i> Jaringan19
4	. Keamanan Jaringan21
5	. Metode Pengamanan Jaringan21
6	. Port Knocking22
7	. Bentuk serangan pada jaringan23

	8.	Metode Port Knocking	24
	9.	Firewall	24
	10.	NAT	26
	11.	TCP/IP	27
	12.	Unit Dan Alat Jaringan	29
	13.	Mikrotik	36
	14.	Ip Address	37
B.	K	ajian Pustaka	41
C.	K	Leunggulan Penelitian	43
D.	F	lowchart Alur Penelitian	44
E.	L	okasi Penelitian	45
BAB	S III		50
ANA	LIS	SIS DAN PERANCANGAN	50
A.	A	nalisa	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.	D	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	S IV		82
IMP	LEI	MENTASI DAN PEMBAHASAN	82
A.	I	nplementasi	82
	1.	Pengujian <i>port knocking</i>	83
	2.	Pengujian scan port	89
	3.	Pengujian <i>sniffing</i>	91
	4.	Pengujian DDOS	95

В.	Monitoring	97
C.	Management	98
D.	Pembahasan	98
BAB	V	100
PENU	JTUP	100
А.	KESIMPULAN	100
B.	SARAN	101
DAFI	FAR PUSTAKA	102
LAM	PIRAN	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 Unicast IP versi 4	
2.1 Tabel Kepengurusan	46
3.2 Spesifikasi <i>Router</i> RB1100x4	66
3.3 Spesifikasi Pc <i>Client</i>	67
3.4 Operating Sistem <i>Router</i>	67
3.5 Operating Sistem Pc <i>Client</i>	67
4.1 Hasil Pengujian	100

DAFTAR GAMBAR

Gambar

Halaman

1.1 Proses tahapan penelitian NDLC
2.1 Jaringan LAN 15
2.2. Jaringan Metropolitan Area Network
2.3. Skema topologi Wide Area Network
2.4. Topologi Star
2.5. Skema <i>Firewall</i> Pada Jaringan
2.6. OSI Model (Kiri) dan TCP/IP Model (Kanan)
2.7. Modem Internal dan Modem External
2.8. LAN Card
2.9. <i>Switch</i>
2.10. Gambar <i>Router</i> dan Simulasinya
2.11. Access Point
2.12 Alur <i>Flowchart</i> Penelitian
2.13 Struktur Organisasi
3.1 Topologi Yang Berjalan
3.2 Grafik jumlah serangan terhadap mikrotik
3.3 Tindakan <i>Probing</i>
3.4 Tindakan DDOS
3.5 Sebelum terkena DDOS
3.6 DHCP <i>Client</i>
3.7 DHCP Server
3.8 NAT <i>Masqurade</i>
3.9 Address List

3.10 Pengaturan DNS	61
3.11 Topologi Yang diusulkan	63
3.12 Alur simulasi pengujian	65
3.13 <i>Router</i> RB1100x4	66
3.14 Gambar alur flow chart port knocking	69
3.15 Tampilan awal winbox	72
3.16 Tampilan Rule Port knocking	73
3.17 Tampilan Action Rule Port knocking	74
3.18 Tampilan Action Rule Port knocking update	75
3.19 Tampilan Action	76
3.20 Tampilan Blokir Winbox	77
3.21 Tampilan Advenced Blokir Winbox	77
3.22 Tampilan Action Blokir Winbox	78
3.23 Tampilan <i>Firewall</i> Menampung Ip	79
3.24 Tampilan Advanced Menampung Ip	80
3.25 Tampilan Action Menampung Ip	80
3.26 Tampilan <i>Drop</i> IP DDOS	81
3.27 Tampilan Action Drop IP DDOS	81
3.28 <i>Mac interface</i> winbox	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 Ping terhdap port service	88

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

SMK PGRI 1 Nganjuk memilih *server* r*outer* 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 permaslahan 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 efektik 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 sesusdah 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.
- 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*.
- 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.

- 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. Menganilis seberapa efisien penggunaan metode *port knocking* dalam penangamanan keamanan jaringan.
- 6. Menganilis 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 :

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

- 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 :

- Wawancara dengan pihak-pihak terkait mulai dari manajemen puncak hingga level bawah atau operator untuk mendapatkan informasi yang spesifik dan komprehensif.
- 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 permaslahan 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 Hadware

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

		Bulan																							
			Bulan-1				Bulan-2				Bulan-3				ula	n- 4	ŀ	Bulan-5				Bulan-6			
No	Kegiatan	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	Library																								
1	Research																								
2	Observasi																								
3	Interview																								
4	Perancang																								
4	an sistem																								
5	Implement																								
3	asi sistem																								
6	Uji coba																								
7	Laporan																								

Tabel 1.1 Rencana Penelitian

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

Pengertia 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 komponenkomponennya 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 permaslaahan 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, shutdows, kehilangan file atau kerusakan sistem.

a. Jaringa Komputer Berdasarkan Kelompoknya

Jaringan komputer terdiri dari beberapa komputer yang terhubung ke komputer lain dengan kabel atau nirkabel (*wirreless*). 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 : <u>morning.computer</u>)

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 digunakan. WAN digunakan juga bisa 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.

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

WAN adalah jaringan yangn 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: <u>arduinoindonesia.id</u>)

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 membutuhkkan 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 flektibilitas. 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

- 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 : <u>yuliatwn.wordpress.com</u>)

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 layar

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 Diagram 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 : <u>irmaningsihblog.wordpress.com</u>)

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 tepasang 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 penggunaanya 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 : <u>www.temukanpengertian.com</u>)

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 *Router*OS.

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 : <u>citraweb.com</u>)

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

13. Mikrotik

MikroTik adalah sebuah *operating system* yang dalam penggunaanya 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 difungskan 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 *Router*OS 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 :

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

Tabel 2.1 Alamat Unicast IP versi 4

			alamat unicast).
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 masingmasing 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 alamatalamat 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. :

 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 selanjutanya 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 berikutnnya 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*.

- 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.
- Jalannya penelitian yang terstruktur dengan baik, berdasarkan penerapan kaidah NDLC.
- 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 anlisa 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 selanjutanya adalah monitoring hasi dari tahap implementasi dan sampai akhirnya di terapkan.

E. Lokasi Penelitian

Dalam penulisan Tugas Akhir skripsi ini yang menjadi objek penelitian adalah kemanan 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 SMKPGRI Nganjuk yaitu tanggal 01-01-1901, dengan No.SK: 105/I04.5.1/E-80. Adapun kepengurusan saat ini sebagai berikut :

Tabe	el 3.1	Tabel	Kepeng	gurusan
------	--------	-------	--------	---------

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

SMK PGRI 1 Nganjuk Memliki 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

- Meningkatkan kwalitas pembelajaran terhadap peserta didik perkembangan IPTEK dan berwawasan IMTAQ.
- Menyelenggarakan kegiatan DIKLAT yang relevan dengan kebutuhan kehidupan masyarakat, berorientasi pada " Key Competencies ".
- 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.
- 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 beradabtasi serta berkompetisi di dunia kerja internasional sesuai dengan kompetensi kejuruannya.

3. Struktur 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 Memliki 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 Memliki 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 komponenkomponen 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 disebarkan 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 *Wirelless*.

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.

	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

Tabel 3.1 Jumlah serangan terhadap mikrotik

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 akases internet secara gratis.

C Safe Mode	Sessio	n: 192.168.4.200						
🖋 Quick Set	Log						[
CAPsMAN	7	Freeze				Find	all	4
Interfaces		The	D. #	Tanta		L		1.
Wireless	#	Hime	Buffer	1 opics	Message	(2022.00.22.42		
Didas	40	Jun/11/2023 00:32:42	memory	system, into	change time Jun/ 12/2023 02:33:01 => Jun/ 11.	2023 00:32:42		
s brage	41	Jun/11/2023 00:32:42	memory	system, info	system time zone settings changed by admin	in ministration		-1
PPP	42	Jun/11/2023 00.33.01	momony	system, into, account	user admin logged at from 50:EB-EC-EA-C5-95	via winbox		-1
E Switch	43	km/11/2022 00:33:03	memory	system, into, account	user admin logged out norm 50-EB-FC-EA-C5-95	in winbox		-1
* Meeh	45	Jun/11/2023 00:33:12	memory	system, info, account	user admin logged in from 50-EB-E6-EA-C5-95	via winbox		
	46	Jun/11/2023 00:33:28	memory	system, empr. critical	login failure for user admin from 50 EB E6 EA C5	95 via winhov		-1
P P	47	Jun/11/2023 00:33:30	memory	system, error, critical	login failure for user admin from 50:EB:F6:EA:C5	5.95 via winbox		
🕑 MPLS 🛛 🗈	48	Jun/11/2023 00:33:32	memory	system error critical	login failure for user admin from 50 EB E6 EA C	95 via winbox		
OpenFlow	49	Jun/11/2023 00:33:35	memory	system, error, critical	login failure for user admin from 50:EB:F6:EA:C5	5:95 via winbox		-1
s in the	50	Jun/11/2023 00:33:35	memory	system, info, account	user admin logged out from 50:EB:F6:EA:C5:95	via winbox		
E II VO	51	Jun/11/2023 00:33:54	memory	system, error, critical	login failure for user admin from 50:EB:F6:EA:C5	5:95 via winbox		
Routing	52	Jun/11/2023 00:34:00	memory	system, info, account	user admin logged in from 50:EB:F6:EA:C5:95 v	ia winbox		
System 🗅	53	Jun/11/2023 00:34:49	memory	system, info, account	user admin logged in from 50:EB:F6:EA:C5:95 v	ria winbox		
Queues	54	Jun/11/2023 00:34:50	memory	system, info, account	user admin logged out from 50:EB:F6:EA:C5:95	via winbox		
Di	55	Jun/11/2023 00:35:50	memory	system, info, account	user admin logged in from 192.168.4.198 via wi	nbox		
riles	56	Jun/11/2023 00:35:52	memory	system, info, account	user admin logged out from 50:EB:F6:EA:C5:95	via winbox		

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 lainya 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* unutk melakukan

penetrasi atau serangan-serangan dengan tujuan mendapatkan informasi atau melakukan pengerusakan 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.

C* Safe Mode	Session: 192.168.4.200			
🖋 Quick Set	Interface <ether2></ether2>		Resources	
CAPSMAN	Overall Stats Rx Stats Tx Stats Status Traffic	ОК	Uptime: 00:28:16	ок
	Tx/Rx Rate: 77.3 kbps / 5.4 kbps	Cancel	Free Memory: 100.8 MiB	PCI
Bridge	Tx/Rx Packet Rate: 8 p/s / 6 p/s	Apply	Total Memory: 128.0 MiB	USB
PPP	FP Tx/Rx Rate: 77.0 kbps / 5.2 kbps	Disable	CPU: MIPS 74Kc V4.12	CPU
Switch Mesh	FP Tx/Rx Packet Rate: 8 p/s / 6 p/s	Comment	CPU Count: 1	IRQ
P P	Tx/Rx Bytes: 11.3 MiB / 1310.7 KiB	Torch	CPU Frequency: 600 MHz	
MPLS N	Tx/Rx Packets: 12 948 / 12 208		CPU Load: 90 %	
OpenFlow	Tx/Rx Drops: 0 / 0	Cable Test	Free HDD Space: 70.8 MiB	
Bouting	Tx/Rx Errors: 0 / 0	Blink	Total HDD Size: 128.0 MiB	
System N		Reset MAC Address	Sector Writes Since Report: 407	
🗣 Queues		Reset Counters	Total Sector Writes: 99.462	
Files	Tx: 77.3 kbps		Bad Blocks: 0.0 %	
BADIUS	Rx: 5.4 kbps		Anakanat an Name (minaka	
X Tools ►			Read Name: PP951G 2HeD	
New Terminal	I bloommaandammaaladadadaanaanaanaan		Version: 6.48.6 (ongterm)	
TR069			Build Time: Dec/03/2021 12:15	-05

Gambar 3.4 Tindakan DDOS (Sumber : Router SMK PGRI 1 Nganjuk) Pada gambar 3.4 terlihat koneksi pada jaringa mirkotik 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 sesui 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 menyediyakan *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)

C* Safe Mode	Session: E4:8D:80	C:35:C3:1A					
🖉 Quick Set	DHCP Server						
CAPsMAN	DHCP Networ	ks Leases Ontions	Option Sets	Ontion Matcher Ale	ds		
Wireless	+- ~	× 🗆 🍸 DH	CP Config DF	ICP Setup			Find
WineGuard	Name	/ Interface	Relay	Lease Time	Address Pool	Add AR	
in nu	dhcp1	2.Komli		00:10:00	dhcp_pool16	no	
Endge	dhcp2	3.Hardware		00:10:00	dhcp_pool2	no	
E PPP	dhcp3	4.Software		00:10:00	dhcp_pool3	no	
🙄 Switch	dhcp4	5.Ruang Guru		00:10:00	dhcp_pool17	no	
Mesh	dhop6	5.Huang Aula		00:10:00	dhop_pool11	no	
IS ID N	dhcp7	8 DPIB 2		00:10:00	dhop_pool12	10	
en n	dhcp8	9 Simdia 1		00:10:00	dhop_pool14	00	
PV6	dhcp9	10.Simdig 2		00:10:00	dhcp_pool15	no	
MPLS P							
🖈 Routing 🛛 🗅							
🖉 System 🗈							
Queues							
Files							
Log							
P BADIUS							
1.00000							

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 Masqurade

	Safe Mode		ession	: E4:	3D:80	:35:C	1:1A																
X	Quick Set		irewal																				Ð
Ŷ	CAPsMAN	-	Filter i	Rules	NA	ТМ	angle	Ra	w Service	Porte	Conne	ctions A	ddress List	lave	r7 Protocola								
	Interfaces		- 10				ingio –			1 0110	1	000010 7		0 20,0									
Ω.	Wireless		+			3 6	9 1	ſ	(© Reset C	ounters	(O F	leset All C	ounters								nd	al	
64	WireGuard		#	A	tion	Cha	in	S	irc. Address	Dst. A	ddress	Src. Ad.	Dst. Ad	Proto	Src. Port	Dst. Port	In. Inter	Out. Int	. In. Inter	. Out. Int	Bytes	P	ackets
ü	Bridge		.:: K	onek	i Inte	met																	
2	PPP		0	i anak	i Inte	srci	hat														268.2	MIB	3 549
-	FFF		1	UNER	mas	srci	at											1 Interne				0 B	
-	Switch		.:: E	PKL																			
1	Mesh		2 X	•	`dst-	dst	nat			36.94	8.59			6 (tcp)		80,443						0 B	
+	IP	1	::: E	-Rapo	et .					20.04	0.50			C A		0154						0.0	
얯	IPv6	1	3 X) ⊧ okir\	∵dst- Veb F	dst	hat			36.94.	8.59			6 (tcp)		8154						0.8	
0	MPLS	1	4 X	2	redi	dst	nat							6 (tcp)		80	10.Sim					0 B	
3	Routing	1	::: B	lokir 1	outul	e																	
8	System	1	5 X	- P	redi	dst	nat							17.6		53						0 B	
														i i qui i		55							
*	Files Log RADIUS Tools New Terminal Dot1X LCD MetaROUTER Partition Make Supout n New WinBox Ext	ŕ												** [0.11									

Gambar 3.8 NAT *Masqurade* (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 dugunakan untuk idenditas sebuah perangkat yang terhubung dalam *insfrastruktur* jaringan. Berikut ini konfigurasi *IP Address* yang sudah disesuiakan dengan masing-masing port.

Sidik@E4:8D:8C:35:C	3:1A (2> RB2011UiAS) - WinBox (64bit)	v7.6 on RB2011UiAS (r	nipsbe)		-	٥	×
Session Settings Da	shboard						
ら 🖓 Safe Mode	Session: E4:8D:8C:35:C3:1A						
🏏 🗶 Quick Set	Address List						6 ×
CAPsMAN	+ - / × 6 7						nd
Interfaces	Address / Network	Interface					•
Wireless	D + 10.10.10.3/24 10.10.10.0	1.Internet					
😝 WireGuard	+ 192.168.2.1/24 192.168.2.0	2.Komli					
💥 Bridge	+ 192.168.3.1/24 192.168.3.0 + 193.169.4.1/34 193.169.4.0	3.Hardware					
2 PPP	+ 192 168 5 1/24 192 168 5 0	5 Buang Gunu					
T Switch	+ 192.168.6.1/24 192.168.6.0	6.Ruang Aula					
"T" Mesh	+ 192.168.7.1/24 192.168.7.0	7.DPIB 1					
85 ID N	+ 192.168.8.1/24 192.168.8.0	8.DPIB 2					
	- 192.168.9.1/24 192.168.9.0 - 192.168.10.1/ 192.168.10.0	9.5imdig 1 10.Simdia 2					
	132.100.10.17 132.100.10.0	To Jilling 2					
O MPLS P	-						
C Routing ►	-						

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

sidik@E4:8D:8C:35:C3 ssion Settings Das	:1A (2> RB2011UiAS) - WinBo hboard	xx (64bit) v7.6 on RB2011UiAS (mipsbe)	-	٥	×
C Safe Mode	Session: E4:8D:8C:35:C3:1A				
🚀 Quick Set	DNS Settings				Ð
CAPsMAN	Servers:	8.8.8	ŧ	0	к
Interfaces		8.8.4.4	ŧ	Car	
Wireless		202 134 0 155	۵		
😝 WireGuard		202 124 1 10		Ap	ply
Bridge	Durania Conversi	202.104.0.155	-	Sta	atic
The poper state of the poper sta	Dynamic Servers:	202.134.0.100			aha
∰ Switch		8888		Cal	a ic
Mesh		8.8.4.4			
₩ IP	Use DoH Server:		•		
🖞 IPv6 🗈		Verfu DoH Cettinate			
MPLS P		winy born celuicate			
JI Houting		Allow Remote Requests			
System P	Max UDP Packet Size:	4096			
🖤 Queues		2.000	-		
Hes .	Query Server Timeout:	2.000	;		
	Query Total Timeout:	10.000	1		
Trata	Max. Concurrent Queries:	100	٦.		
Nous Transland	Max Concurrent TCP Sessions:	20			
A Det1Y					
	Cache Size:	2048	GΒ		
MetaDOUTER	Cache Max TTL:	7d 00:00:00			
Partico	Cache Used:	30 KiB			
Make Support of					
Naw Win Pay					

Gambar 3.10 Pengaturan DNS (Sumber : Router SMK PGRI 1 Nganjuk) Pada gamabar 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 jaringa mikrotik SMK PGRI 1 Nganjuk. Dalam jalanannya 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 Miktorik 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.
- Pengujian saat jaringa sudah menerapkan *port knocking* dengan mode menyalakan *service port*.
- 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 peracangan sistem usulan akan dijelaskan juga mengenai, perancangan arsitektur, *topologi* jaringan, perangkat lunak yang akan digunakan oleh *hadware*, sistem yang direncanakan atau medote usulan yang akan digunakan dalam penulusan 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 : <u>mikrotik.com</u>)

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	Router 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

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

Tabel 3.3 Spesifikasi Pc Client

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 (Operating System)	RouterOS Level6

Tabel 3.4 menjelaskan sistem operasi yang digunakan oleh *router* yaitu *Router*OS 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 (Operating System)	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 menunjukan inisialisasi port berapa yang akan diketuk agar koneksi atau port yang dikehendaki dapat terbuka.
- c. Nomor 3 menunjukan 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 menunjukan 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 menunjukan 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.
- 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 *Router*OS. 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.

File Tools	.37 (Add	iresses)					-		\times
Connect To:	10.10.1	0.1					✓ Keep	Password	
Login:	admin						Open	in New V	Indow
Paseword:							🖌 Auto F	Reconnec	t
	Add/S	et		Connect	To RoMON Co	nnect			
Managed Net Refresh	ignoors						Find	al	¥
MAC Address	, 	IP Address	Identity	Version	Board	Uptin	e		
CC:2D:E0:2E:88	:D8	10.10.10.1	SERVER PUSAT SMK PGRI 1 NGANJUK	6.47.7 (st.	RB951UI-2HnD		00:30:58		

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.
- Buat *rule* pertama agar dapat menampung ip yang mencoba masuk kedalam mikrotik, masuk ke Menu "IP" pilih "*Firewall*" pilih pada *tab* "*Filter*" Add (+) rule.
- Pada gamabar 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 are to address, list_"All

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

rewall Ru	ule 🗢						
General	Advanced	Extra	Action	Statistics			ок
	Chain:	input				Ŧ	Cancel
	Src. Address:					-	Apply
	Dst. Address:					-	Enable
	Protocol:		(icmp)		Ŧ	-	Comment
	Src. Port:					-	Сору
	Dst. Port:					-	Remove
	Any. Port:	-				Ţ	Reset Counters
3	Out. Interface:				_	-	Reset All Counters
In.	Interface List:					-	
Out.	Interface List:	[-	
	Packet Mark:					-	
Con	nection Mark:					-	
	Routing Mark:					-	
F	Routing Table:					-	
Con	nection Type:					-	
Con	nection State:					-	
Connecti	on NAT State:	1			-	-	



	>	
General Ad	Ivanced Extra Action Statistics	ок
Action:	add src to address list	Cancel
	🗌 Log	Apply
Log Prefix:	2	▼ Disable
Address List:	ALAMAT PORT KNOCK	Comment
Timeout:	00:02:00	▼ Сору
		Remove
		Reset Counters
		Reset All Counte
abled		

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 -listtimeout=1h Chain=input \ comment="PORT KNOCKING VERIFIKASI" dst-port=1111 in-interface=INTERNET \ protocol=tcp.

General	Advanced	Extra	Action	Statistics		ОК
	Chain:	input	10			Cancel
	Src. Address:				•	Apply
	Dst. Address:				`	Enable
	Protocol:	6	(tcp)			Comment
	Src. Port:	_			-	Сору
	Dst. Port:		111		^	Remove
	Any. Port:	-			`	Reset Counters
(Dut. Interface:					Reset All Counter
In.	Interface List:	1			•	
Out.	Interface List:				•	
	Packet Mark:					
Con	nection Mark:				•	
1	Routing Mark:				•	
F	Routing Table:					
Con	nection Type:					
Con	nection State:					
onnectio	on NAT State:				-	

Gambar 3.18 Tampilan Action Rule Port knocking update

rewall Rule <11	11>		
General Adva	nced Extra Action Statistics		OK
Action: ac	ld src to address list	•	Cancel
	Log		Apply
Log Prefix:		-	Disable
Address List: VI	ERIVIKASI ALAMAT PORT KNOCK		Comment
Timeout: 01:00:00	1:00:00		Сору
		[Remove
			Reset Counters
			Reset All Counters
nabled			

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* "Advence" 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

ieneral Advanced Ext	ra Action	Statistics		OK
Src. Address List:		ASI ALAMAT PORT KNO	ОСК 🔻 🔺 🔹	Cancel
Dst. Address List:			•	Apply
Layer7 Protocol:			•	Disable
Content:			•	Comment
Connection Bytes:			▼	Сору
Connection Rate:			▼	Remove
er Connection Classifier:			•	Reset Counters
Src. MAC Address:			▼	Reset All Counters
Out. Bridge Port:			•	
In. Bridge Port:			▼	
In. Bridge Port List:			•	
Out. Bridge Port List:			▼	
IPsec Policy:			•	
TLS Host:			▼ •	5

Gambar 3.21 Tampilan Advenced Blokir Winbox

rewall Rule <8291>		
General Advanced Extra Action Statistics		ОК
Action: drop	••••	Cancel
Log		Apply
Log Prefix:	▼ [Disable
		Comment
		Сору
		Remove
		Reset Counters
		Reset All Counters
abled		

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.:

- Pada gambar 2. 23 dan 2.24 *rule Firewall* yang berguna untuk menampung almat serta *mac* dari seorang *attacker* yang melakukan DDOS.
- Pada gambar 2.25 *rule* ini kita memberikan sebuah jarak paket tidak normal guna untuk menangkap seorang *attacker* yaitu sebersa 1500 Kb sampai 65535 Kb.
- 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

General	Advanced	Extra	Action	Statistics		OK
	Chain: pre	routing			Ŧ	Cancel
Src.	Address:				-	Apply
Dst.	Address:				•	Enable
	Protocol:	17 (udp)		₹ ▲	Comment
1	Src. Port:					Сору
	Dst. Port:					Remove
/ In I	ny. Port:	INTER	NET			Reset Counters
Out. I	nterface:				• •	Reset All Counters
In. Inter	ace List:				•	
Out. Inter	ace List:				•	

Gambar 3.23 Tampilan Firewall Menampung Ip

General Advanced	Extra	Action	Statistics		ОК
Src. Address Lis	t: [-	Cancel
Dst. Address Lis	t:			-	Apply
Conten	t: 📃			•	Enable
Per Connection Classifie	r:				Comment
Src. MAC Address	s:				Сору
IPsec Polic	y:			•	Remove
TLS Hos	t:			•	Reset Counters
Ingress Priorit	y:			•	Reset All Counters
Priorit	y:			•	
DSCP (TOS):			•	
TCP MSS	S:			*	
Packet Size	e: 🗆 [1500-655	535	•	
Randon	n: 📃			•	
▼ TCP Flags					
 ICMP Options 	_				
IPv4 Option	s:			•	
TT	:			-	

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

General	Advanced	Extra Action	Statistics		ОК
	Chain: pre	routing		Ŧ	Cancel
Src.	Address:			•	Apply
Dst.	Address:			•	Enable
1	Protocol:] •	Comment
9	Src. Port:			*	Сору
[Dst. Port:			*	Remove
A	rny. Port:	(INTERNET)			Reset Counters
ln. lı Out. lı	nterface:	INTERNET]•	Reset All Counters
In. Interf	ace List:] •	
Out. Interf	ace List:			•	

Gambar 3.26 Tampilan Drop IP DDOS

-		100	0	2.1.2		1200
General	Advanced	Extra	Action	Statistics	1	ОК
Act	ion: drop				Ŧ	Cancel
	🗌 Log					Apply
Log Pre	efix:				-	Enable
						Comment
						Сору
						Remove
						Reset Counters
						Reset All Counters



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 *Router*OS 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.

Safe Moo	le Se	ssion: 1	11.11.11	.1								
🖉 🊀 Quick Set		i.										
CAPsMAN		Firewa	all									
Interfaces		Filter	Rules	NAT	Mangle	Raw S	ervice Po	orts Conne	ections A	ddress Lists	Layer7 Pro	tocols
🔉 Wireless				0 00		Z Co P	and Cours					rescension
30 Bridge		-				to he	eset Cour		Reset All Co	ounters		
1 PPP		#	Ac	tion	Chain	Src. Ac	Idress [)st. Address	Protocol	Src. Port	Dst. Port	In. Inte
TT Contrals	- 1		PORTK	NOKT	AHAP 1							
T SWILCH	_	0 2	X 📑	add	input				1 (icmp)			
C Mesh			PORT K	NOCK	VERIFIKAS	51						
255 10		1)	X III	add	input				6 (tcp)		1111	
The second secon	12		BLOKIR	WINB	OX UNTUK	KNOCK						
MPLS	1	2)	X 22	drop	input				6 (tcp)		21.22.23	
1000				pr	To the second				(- (- ap)			

Gambar 4.2 Hasil login winbox mode normal

Gambar 4.2 memperlihatkan konfigurasi port knocking

dalam mode *disable*.

🚱 WebFig	× +			v - 0)
← → C ▲ Not sect active	rre 11.11.11.1/webfig/			⊶ ¥ ૯ ☆ <mark>0</mark> 券 □ 🥝
		Wireless		Configuration
Wireless Protocol	€802.11 Onstreme Onv2		Mode	Router OBridge
Network Name	SKRIPSI			Internet
Frequency	2412 VMHz		Address Acquisition	Static OAutomatic OPPPoE
Band	2GHz-B/G ¥		IP Address	10.10.10.1
Channel Width	20MHz 🗸		Netmask	255 255 255 0 (/24) 👻
Country	etsi 🗸		Gateway	0.0.0.0
MAC Address	CC:2D:E0:2E:88:DB		DNS Servers	•
Use Access List (ACL)	0		MAC Address	CC-2D-E0-2E-88-D6
Security	WPA WPA2		Firewall Router	0
		Wireless Clients		Local Network
MAC Address	In ACL Last IP Uptime	Signal Strength	IP Address	13.13.13.1
			Netmask	255 255 255 0 (/24)
			Bridge All LAN Ports	0
			DHCP Server	0
			DHCP Server Range	▲ 11.11.11.2-11.11.11.254
			NAT	0



Gambar 4.3 memperlihatkan hasil login mikrotik dengan

menggunakan web browser.

🛃 11.11.11.1 - Pu	TTY	88	- 0	×
1				^
anner anner				
MANAN MANAN	ккк тттттттт		KKK	
MAN MANN WAN	III KKK KKK RRRRRR 000000 TTT	III	KKK KKK	2
MMM MM MMM	III KKKKK RRR RRR 000 000 TTT	III	KKKKK	
MMM MMM	III KKK KKK RRRRRR 000 000 TTT	III	KKK KKK	
MMM MMM	III KKK KKK RRR RRR 000000 TTT	III	KKK KKK	
MikroTik Rout	er05 6.49.8 (c) 1999-2023 http://www.mik	rotik	.com/	
[2]	Gives the list of available commands			
command [?]	Gives help on the command and list of argumer	its		
[Tab]	Completes the command/word. If the input is a	mbigu	ous,	
	a second [Tab] gives possible options			
1	Move up to base level			
	Move up one level			
/command	Use command at the base level			
Fadmin@NikcoTik	1 .			
Facility in the strengt the	[1] Man			

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.

SinBox v3 File Tools	37 (Addresses)	– 🗆 X
Connect To: Login: Password:	11.11.11.1 admin	Keep Password Open In New Window V Auto Reconnect Cancel
Connecting to 11	11.11.1	



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.

Session	Basic options for your PuTTY session					
Logging Terminal Keyboard Rell	Specify the destination you want to con Host Name (or IP address)	Port				
- Features Window	Connection type: O SSH O Serial O Other: Tel	net ~				
Behaviour Translation Selection Colours	Load, save or delete a stored session Saved Sessions					
- Connection	Default Settings	Load				
Data Proxy		Save				
⊕ SSH		Delete				

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*.

C:\Windows\system32\cmd.exe		×
C:\Users\SMILE>ping 11.11.11.1		^
Pinging 11.11.11.1 with 32 bytes of data: Reply from 11.11.11.1: bytes=32 time<1ms TTL=64 Reply from 11.11.11.1: bytes=32 time<1ms TTL=64 Reply from 11.11.11.1: bytes=32 time<1ms TTL=64 Reply from 11.11.11.1: bytes=32 time<1ms TTL=64		
<pre>Ping statistics for 11.11.11.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms C:\Users\SMILE>_</pre>		

Gambar 4.9 Ping terhdap 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.

regsowen.co	m Port Knock		-	
11.11.11.1		Desc		
11.11.11.1 Type	Port	Desc Text		
11.11.11.1 Type TCP V	Port 1111	Desc Text		
11.11.11.1 Type TCP ~	Port 1111	Desc Text		
11.11.11.1 Type TCP ~ None ~	Port 1111	Desc Text		
11.11.11.1 Type TCP ~ None ~ None ~	Port 1111	Desc Text		
11.11.11.1 Type TCP None None None	Port 1111	Desc [Text		
11.11.11.1 Type TCP None None None	Port 1111	Desc Text		

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 sperti halnya untuk monitoring *server* dari jarak jauh. Menjalankan aplikasi, pelacakan data dan sebagainya.

Berdasarkan hasi uji coba yang telah dilakasanakan, didapatkan hasil bahwa port yang ada pada jaringan mode normal masih bisa di*scan* 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 sperti halnya untuk monitoring *server* dari jarak jauh. Menjalankan aplikasi, pelacakan data dan sebagainya.

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

🕞 Zenm Scan To	nap pols Profile H	lelp				14 <u>1</u> 14	
Target:	11.11.11.1	-	Profile:	Quick scan	•	Scan	Cancel
Command	d: nmap - T4 - F	11.11.11.1					
Hosts	Services	Nmap Output	Ports /	/ Hosts Topology	Host Details	Scans	
OS	Host 🔺	nmap - T4 - F 11.1	1.11.1			•	Details
	un brust	Starting Nmap Standard Time Nmap scan repo Host is up (0. Not shown: 94 PORT STAT 21/top filt 22/top filt 23/top filt 53/top filt 2000/top filt 2000/top filt 2000/top filt MAC Address: (1)	7.94 (P ort for 1 0025s la closed t set ftp ered ftp ered telf ered telf ered doma ered http ered doma cC:2D:E0:	<pre>https://nmap.org) https://nmap.org) https://nmap.org) https://nce http://cce https://nce https://cce htttps://cce https://cce httt</pre>	at 2023-06-23 oard.com) nned in 15.16	18:19 SE	Asia

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) memungkinan 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.

	1 1 1 1						
40	ily a display filter <	cm-/>					• +
	Time	Source	Destnation	Protocol	Length Info		
	7 11.865905	11.11.11.254	239.255.255.255	UDP	46 52456 + 5678 Len=4		
	8 11.866096	11.11.11.254	11.11.11.255	UDP	46 52457 + 5678 Len=4		
	9 11.866231	11.11.11.254	239.255.255.255	UDP	46 52458 + 5678 Len=4		
	10 11.866327	11.11.11.254	239.255.255.255	UDP	46 52459 → 5678 Len=4		
	11 13.830901	Routerbo_2e:88:d7	CDP/VTP/DTP/PAgP/UD.	CDP	103 Device ID: MikroTik Port ID: LOCAL		
	12 13.830938	11.11.11.1	255.255.255.255	MNDP	158 5678 + 5678 Len=116	_	
	13 16.484345	11.11.11.254	11.11.11.1	TCP	66 14566 → 8291 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM		
	14 16.484545	11.11.11.1	11.11.11.254	TCP	66 8291 → 14566 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16		
	15 16.484670	11.11.11.254	11.11.11.1	TCP	54 14566 + 8291 [ACK] Seq=1 Ack=1 Win=1051136 Len=0		
	16 16.505643	11.11.11.254	11.11.11.1	TCP	95 14566 + 8291 [PSH, ACK] Seq=1 Ack=1 Win=1051136 Len=41		
	17 16.505886	11.11.11.1	11.11.11.254	TCP	60 8291 → 14566 [ACK] Seq=1 Ack=42 Win=14608 Len=0		-
	18 16.603485	11.11.11.1	11.11.11.254	TCP	105 8291 + 14566 [PSH, ACK] Seq=1 Ack=42 Win=14608 Len=51		
	19 16.614487	11.11.11.254	11.11.11.1	TCP	88 14566 + 8291 [PSH, ACK] Seq=42 Ack=52 Win=1051136 Len=34		
	20 16.614816	11.11.11.1	11.11.11.254	TCP	60 8291 + 14566 [ACK] Seq=52 Ack=76 Win=14608 Len=0		
	21 16.668989	11.11.11.1	11.11.11.254	TCP	88 8291 - 14566 [PSH, ACK] Seq=52 Ack=76 Win=14608 Len=34		
	22-16-669442	51-11-11-254	11-11-11-1	TEP	151 11566 - 8291 [PSH, 16K] Seq 76 Ack 86 Win 1858889 Len 188		
	23 16.669778	11.11.11.1	11.11.11.254	TCP	60 8291 → 14566 [ACK] Seq=86 Ack=176 Win=14608 Len=0		
	24 16.671674	11.11.11.1	11.11.11.254	TCP	234 8291 → 14566 [PSH, ACK] Seq=86 Ack=176 Win=14608 Len=180		
	25 16.672253	11.11.11.254	11.11.11.1	TCP	154 14566 + 8291 [PSH, ACK] Seq=176 Ack=266 Win=1050880 Len=100		
	26 16.673336	11.11.11.1	11.11.11.254	TCP	154 8291 + 14566 [PSH, ACK] Seq=266 Ack=276 Win=14608 Len=100		
	AR 20 000000	11 11 11 254	11.11.11.1	TCP	154 14566 + 8291 [PSH, ACK] Seg=276 Ack=366 Win=1050624 Len=100		

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.

Apply a display filter	:Ctrl-/>			0
Time	Source	Destination	Protocol	Length Info
208 25.264249	11.11.11.254	239.255.255.255	UDP	46 52463 → 5678 Len=4
209 25.264386	11.11.11.254	11.11.11.255	UDP	46 52464 → 5678 Len≈4
210 25.264438	11.11.11.254	239.255.255.255	UDP	46 52465 → 5678 Len=4
211 25.264487	11.11.11.254	239.255.255.255	UDP	46 52466 + 5678 Len=4
212 26.319295	Routerbo_2e:88:d7	CDP/VTP/DTP/PAgP/UD.	CDP	103 Device ID: MikroTik Port ID: LOCAL
212 26 219221	11 11 11 1	226 226 226 226	INDD	158.5678 + 5678 en=116
214 36.151321	11.11.11.254	11.11.11.1	TCP	66 14567 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
215 36.151526	11.11.11.1	11.11.11.254	TCP	66 80 → 14567 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
216 36.151627	11.11.11.254	11.11.11.1	TCP	66 14568 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
217 36.151642	11.11.11.254	11.11.11.1	TCP	54 14567 → 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
218 36.151779	11.11.11.1	11.11.11.254	TCP	66 80 + 14568 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16
219 36.151877	11.11.11.254	11.11.11.1	TCP	54 14568 + 80 [ACK] Seq=1 Ack=1 Win=1051136 Len=0
220 36.161746	11.11.11.254	11.11.11.1	HTTP	500 GET / HTTP/1.1
221 36,162028	11.11.11.1	11.11.11.254	TCP	60 80 + 14567 [ACK] Seq=1 Ack=447 Win=15680 Len=0
222 36.297745	11.11.11.1	11.11.11.254	TCP	1514 80 + 14567 [ACK] Seq=1 Ack=447 Win=15680 Len=1460 [TCP segment of a reassembled PDU]
223 36.297923	11.11.11.1	11.11.11.254	TCP	1514 88 → 14567 [ACK] Seq=1461 Ack=447 Win=15688 Len=1468 [TCP segment of a reassembled PDU]
224 36.297923	11.11.11.1	11.11.11.254	TCP	1230 80 + 14567 [PSH, ACK] Seq=2921 Ack=447 Win=15680 Len=1176 [TCP segment of a reassembled PDU]
225 36.298031	11.11.11.254	11.11.11.1	TCP	54 14567 → 80 [ACK] Seq=447 Ack=4097 Win=1051136 Len=0
226 36.298865	11.11.11.1	11.11.11.254	TCP	1514 80 + 14567 [ACK] Seq=4097 ACK=447 Win=15680 Len=1460 [ICP segment of a reassembled PDD]
227 36.298119	11.11.11.254	11.11.11.1	TCP	54 14567 + 80 [ACK] Seq=447 Ack=5557 Win=1051136 Len=0
220 26 300100	11.11.11.1	11.11.11.254	TCP	1514 88 + 14567 [ACK] Seq=5557 Ack=447 Win=15680 Len=1460 [TCP segment of a reassembled PDU]

Gambar 4.15 Hasil sniffing Router jalur webpage

tream eq 15					
Time	Source	Destination	Protocol	Length Info	
1332 75.546724	11.11.11.254	11.11.11.1	TCP	66 14581 + 23 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM	
1333 75.546925	11.11.11.1	11.11.11.254	TCP	66 23 + 14581 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM WS=16	
1334 75.547005	11.11.11.254	11.11.11.1	TCP	54 14581 + 23 [ACK] Seq=1 Ack=1 Win=1051136 Len=0	
1335 75.556683	11.11.11.254	11.11.11.1	TELNET	75 Telnet Data	
1336 75.556877	11.11.11.1	11.11.11.254	TCP	60 23 + 14581 [ACK] Senel Acke32 Wine14608 Lene0	_
1337 75.623266	11.11.11.1	11.11.11.254	TELNET	66 Telnet Data 📕 Wireshark · Follow TCP Stream (tcp.stream eq 15) · Ethernet 🦳 🗆	X
1338 75.623536	11.11.11.254	11.11.11.1	TELNET	57 Telnet Data	
1339 75.623713	11.11.11.1	11.11.11.254	TELNET	66 Telnet Data	^
1340 75.623938	11.11.11.254	11.11.11.1	TELNET	63 Telnet Data	
1341 75.624097	11.11.11.1	11.11.11.254	TELNET	72 Telnet Data	
1342 75.624311	11.11.11.254	11.11.11.1	TELNET	71 Telnet Data Password: smkpgriinganjuk	
1343 75.624372	11.11.11.254	11.11.11.1	TELNET	60 Telnet Data	
1344 75.624399	11.11.11.254	11.11.11.1	TELNET	65 Telnet Data	
1345 75.625331	11.11.11.1	11.11.11.254	TCP	60 23 + 14581 [ACM	
1346 75.637592	11.11.11.1	11.11.11.254	TELNET	61 Telnet Data	
1347 75.679253	11.11.11.254	11.11.11.1	TCP	54 14581 + 23 [ACM	
1367 78.836716	11.11.11.254	11.11.11.1	TELNET	55 Telnet Data	
1368 78.837116	11.11.11.1	11.11.11.254	TELNET	60 Telnet Data	~
1369 78,882140	11.11.11.254	11.11.11.1	TCP	54 14581 + 23 [ACI Packet 1421. 41 client pht/s]. 21 server pht/s]. 37 turn(s). Click to select.	
1370 78.971228	11.11.11.254	11.11.11.1	TELNET	55 Telnet Data Entire conversation (1570 bytes) v Show data as ASCII v Stream	15 \$
1371 78.971663	11.11.11.1	11.11.11.254	TELNET	60 Telnet Data	

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 jaringa 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) memungkinan 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 *eror* dalam pembacaan port dan mengakibatkan kebuntuan sistem pencurian data terhadap *Router* mikrotik. Seperti yang terlihat pada gambar 4.17. dan 4.18

oply a display filter <	Ctrl-/>			
Time	Source	Destination	Protocol	Length Info
25 14.936620	11.11.11.254	11.11.11.1	TCP	66 [TCP Retransmission] [TCP Port numbers reused] 14555 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
27 18.387220	Routerbo_2e:88:d7	CDP/VTP/DTP/PAgP/UD.	. CDP	103 Device ID: MikroTik Port ID: LOCAL
28 18.387257	11.11.11.1	255.255.255.255	MNDP	158 5678 → 5678 Len=116
29 22.842708	11.11.11.254	11.11.11.1	TCP	66 14557 + 8291 [SYN] Seq=0 Win+64240 Len=0 MSS=1460 WS=256 SACK_PERM
30 22.947425	11.11.11.254	11.11.11.1		66 [TCP Retransmission] [TCP Port numbers reused] 14555 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
				66 [TCP Retransmission] [TCP Port numbers reused] 14557 + 8291 [SYN] Seq=0 Win=64240 Len=0 MSS=14
35 29.573655	11.11.11.254	255.255.255.255	UDP	46 5678 → 5678 Len=4
36 29,573755	11.11.11.254	239.255.255.255	UDP	46 49729 → 5678 Len=4
37 29.573817	11.11.11.254	239.255.255.255	UDP	46 49730 + 5678 Len=4
38 29.573979	11.11.11.254	11.11.11.255	UDP	46 49731 + 5678 Len=4
39 29.574054	11.11.11.254	239.255.255.255	UDP	46 49732 + 5678 Len=4
40 29.574120	11.11.11.254	239.255.255.255	UDP	46 49733 → 5678 Len=4
41 30.034896	Routerbo_2e:88:d7	CDP/VTP/DTP/PAgP/UD.	. CDP	103 Device ID: MikroTik Port ID: LOCAL
42 30.034932	11.11.11.1	255.255.255.255	NNDP	158 5678 → 5678 Len=116
43 30.326695	11.11.11.254	11.11.11.1	TCP	66 14558 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
44 30.327437	11.11.11.254	11.11.11.1	TCP	66 14559 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
45 30.449614	HewlettP b4:bd:9d	Routerbo 2e:88:d7	ARP	42 Who has 11.11.11.1? Tell 11.11.1254

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-point 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 terkurangi 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 Pgengujian
	Mode Normal	Port knocking	Port knocking Client	Berhasil <i>login</i> dan normal
	Mode Normal	Scan Port	Nmap	Semua port service terlihat dan terbuka.
	Mode Normal	Sniffing	Wireshark	Terenkripsi keseluruhan data kecuali dari paket <i>telnet</i> .
	Mode Normal			Kinerja cpu menjadi besar dan banyak paket yang
		DDOS	LOIC	masuk kedalam Routerbord. Mengakiabtkan Router
				menjadi panas dan tidak berfungsi.
	Mode Disable	Port knocking	Port knocking Client	Gagal Login, diperlukan proses knock.
	Mode Disable	Scan Port	Nmap	Semua port service <i>filtered</i> .
	Mode Disable	Sniffing	Wireshark	Terenkripsi keseluruhan data tanpa terkecuali
	Mode Disable	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

- Sistem peningkatan *firewall* jaringan yang diusulkan yaitu pengembagan 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.
- 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.

100

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.
- Diperlukannya pengujian yang dilakukan menggunakan *tools hacking* lainnya yang lebih tinggi tingkat teknologi pengujiannya.
- 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-areaapplication-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-keamananjaringan#:~:text=Sistem%20keamanan%20jaringan%20merupakan%20se buah,mengakses%20sistem%20jaringan%20komputer%20kita.
- Kompirasi. (2022, September 22). Retrieved Januari 10, 2023, from Kompirasi Media: https://www.kompirasi.com/inilah-jenis-jenis-serangan-jaringanpada-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

TRAD VALIDASI DEDOMAN WAWANCADA
IDAR VALIDASI FEDOMAN WAWANCARA
MENTASI METODE PORT KNOCKING DENGAN SISTEM
IIS DAN ANTI DDOS MENGGUNAKAN PROTOKOL TCP
DA KEAMANAN JARINGAN SMK PGRI 1 NGANJUK
: FEBRINA EKA CAHYARISTI, S.Pd.
: Pendidikan Bahasa Indonesia
: SMK PGRI 1 NGANJUK

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

B. PENILAIAN TERHADAP PENGGUNAAN BAHASA S = Setuin

S = Sc	etuju			TS : Tidak Setuju
NO	Kriteria Penilaian	Ska	ala laian	Saran/Perbaikan
		S	TS	
	Pedoman wawancara	V		

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 = So	etuju			TS : Tidak Setuju
NO	Kriteria Penilaian	Ska Penil	ala laian	Saran/Perbaikan
		S	TS	
	Pedoman wawancara dapat menggali aspek-aspek teknologi jaringan internet.	2		
	Pedoman wawancara dapat menggali informasi untuk mendeskripsikan permasalahan dalam penggunaan fasilitas internet di SMK PGRI 1 Nganjuk.	7		



ID		Lande Dismanlan	
LDR		Tidak Lavak Digunakan dengan Revisi	
TD	•	Tidak Layak Digunakan	
		at to a the start of the	

2. Hasil Pertanyaan Guru



3. Hasil Pertanyaan Staff



DAFTAR PERTANYAAN WAWANCAKA 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 : Mirna Ari Kusrinda.
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 / Sodon
2. Dalam penerapan tasilitas internet di SMK PORI i Nganjuk, menurut
anda seberapa sering terjadi gangguan dalam koneksi internet yang anda
3 like dalam nalakeanaanya saring terjadi kandala saharana saring terjadi
cancouan dalam 1 hulan terakhir ? 2 across sor
4. Dalam cituaci tertentu anakah anda nernah mengalami kejadian seperti
kehilangan data, atau gangguan lain seperti internet yang tiba-tiba blank
atau ada akun media social anda yang bermasalah ? 140 Pernah

- 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 ? Songot boik



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.

lomor Responden	SAHAW SETEMBUDI
Vama	: SAHRUI SETIADURI
enis Kelamin	(Laki-Laki) Perempuan
Pekerjaan	: Guru / Staff (Siswa)
Sekolah	: SMK PGRI 1 Nganjuk

- Apakah akses internet di SMK PGRI 1 Nganjuk sudah dapat memenuhi kebutuhan anda dalam melakukan pencarian data di internet saat ini ? 1 Ya.
- Dalam penerapan fasilitas internet di SMK PGRI 1 Nganjuk, menurut anda seberapa sering terjadi gangguan dalam koneksi internet yang anda gunakan ? setimetrical.com
- Jika dalam pelaksanaanya sering terjadi kendala, seberapa sering terjadi gangguan dalam 1 bulan terakhir ? 5 kani
- 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 ? βετααh
- 5. Menurut anda seberapa besar tingkat kenyamanan yang anda rasakan selama menggunakan internet di SMK PGRI 1 Nganjuk ? ${\mathfrak G} \circ {\mathfrak G} / {\mathfrak o}$
- 6. Bagaimana menurut anda akses dengan menggunakan fasilitas area hotspot di area SMK PGRI 1 Nganjuk ? bak (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

Call Sate Mode	Session: 10.10.0.1																	
¥ Quick Set	Interface List					Torch												
CAPSMAN	Interface Interface List P	themet FolP Tur	nel IP Turnel	GRE Tunnel	VIAN VXIAN	- Basic					- Filters							Start
Interfaces					Tott more	linterfac	e: ethe	1			∓ Src. Ac	ddress : [0.0.0/	0				
Wireless	+	P Detect Int	emet			Entry Timery	e 00-0	1/13			le Det Ar	- Hrace -		0		<u> </u>		Stop
🙌 WireGuard	Name /	Туре	Actual MTU	L2 MTU	Tx		u. 00.0	2.00			ja bacine	Juices . [0.0.0.0	•			1	Close
12 Bidge	R 🚸 ether1	Ethernet	15	00 1598	19						Src. Add	dressb :				^	Mau	Weden
*= PPP	R @ ether2	Ethemet	15	1598	325						Dst. Add	dress6 : [:/0				Iven	THEODW
The Curitada	H @ ether3	Einemet	15	10 1598	118						MAC Pr	otocol : i	al			T		
T SWECH	 ether5 	Ethernet	15	0 1598							D.							
" [™] Mesh	R 🚸 ether6	Ethernet	15	0 1598	6.						PT	otocol : [any			• •		
∰ P ►	ether7	Ethernet	15	00 1598								Port :	any			₹ ▲		
🗐 IPv6 🛛 🗅	ether8	Ethernet	15	0 1598							VL	AN Id :	any			₹ ▲		
🕑 MPLS 🛛 🗅	ethers	Einemet	15	10 1598								DSCP -	anv					
🕽 Routing 🗈 🗈	4	-	1.															
🔯 System 🗈	11 tems					Eth / Pn	otocol	Src.		Dst.			VLAN	d DSCP	Tx Rate	Rx Rate	Tx Pack	Rx Pa
Queues						800 (ip)	6 (tcp)	193.217.14	3.8:445 (smb)) 192.1	68.1.2:54216				0 bps	: Obps		0
Rae Rae	Log					800 (p)	6 (tcp)	50.20.18.96	:445 (smb) 77.44E (carb)	192.1	58.1.2:5421/				0 bps	0 bps		0
	T Freeze					800 (p)	6 (µcµ) 17 (µdn)	157 240 21	7 63:443 (silid) 7 63:443 (http:	(132.1 (ne) 192.1	58.1.2.34243				0 bps	bos Obos		0
AY HADIUS	# lime 6	utter Topics emony system	info ch	essage anne time, kul	/02/2023 11:31:4	•												•
X lools	101 Jul/20/2023 11:31:45 m	emory system,	info sy	stem time zon	e settings change	125 items	To	tal Tx: 46.2	kbps i	Total Rx: 13.3 k	bps To	tal Tx Pa	cket: 34		Total F	Rx Packet: 1	6	
839 New Terminal	102 Jul/20/2023 11:31:49 m	emory system,	info, account us	er admin logg	ed in from 98:90:9													
🚸 Dot1X	103 Jul/20/2023 11:31:50 m	emory system,	info, account us	er admin logg	ed out from 98:90	Frewall												
💷 LCD	104 Jul/20/2023 11:31:52 m	emory system,	into, account us	er admin logg	ed in from 98:90:9	Fiter Rules	NAT	Mannle	Raw Servic	e Ports Coor	ections Ad	dress list	s Laver7	Intonia				
MetaROUTER	105 Jul/20/2023 11:31:55 m	emory system, emory system	info account us	er admin logg er admin logg	ed out from 98:90:9								e aayonn					
Partition	107 Jul/20/2023 11:31:57 m	emory system.	info, account us	er admin logg	ed out from 98:90	• = •		67	(O Reset	Counters 🛛 🔘	Reset Al Cou	inters						
Make Supput of	108 Jul/20/2023 11:32:02 m	emory system,	info, account us	er admin logg	ed in from 98:90:9	6 # 1		0	Cur Adda		Dute Co	n Deat	Det Red	le leter	0.4 14	la latar (Con Ad
New WinBox	109 Jul/20/2023 11:32:04 m	emory system,	info, account us	er admin logg	ed out from 98:90	4 N	UUUTI VNOV T		arc. Addres	is Usi. Addres	s F1010 31	C. FOIL	USL FOIL	n. mer.		n. n.e v	u. n	SIC. NU
	110 Jul/20/2023 11:32:06 m	emory system,	info, account us	er admin logg	ed in from 98:90:9	E FVNI		HINE I			140							
M Du	112 Jul/20/2023 11:32:0/ m	emory system, emory system	info account us	er auniñ 1099 er admin loog	ed in from 98-90-9	E DODT	L COO.	IPOL IPOL			1 10							
	113 Jul/20/2023 11:32:13 m	emory system,	info, account us	er admin logg	ed out from 98:90	1	add	inové			6 tm)		1111					
Windows N	114 Jul/20/2023 11:32:15 m	emory system,	info, account us	er admin logg	ed in from 98:90:9	E BLOKE	R WINR	NX LINTLIK I	NOCK		n (pol)		1001			L		
	115 Jul/20/2023 11:32:17 m	emory system,	info, account us	er admin logg	ed out from 98:90	2	dron	inort	- Walt		6 ftcn)		21 22 22					VERIV
	116 Jul/20/2023 11:32:19 m	emory system,	into, account us	er admin logg	ed in from 98:90:9	5 * •	andh				a ficht		-1,66,60,					
	117 JU/20/2023 11:32:20 m	emory system,	into, account us	er admin logg	ed out from 38:30	2												

b. Tanggal 21 Juli 2023

- C- Sale Mode	Session: 10.10.0.1															
🏏 Quick Set	Interface List					Torch										
🗘 CAPsMAN	Interface Interface List	Ethernet EolP Tunnel	IP Tunnel G	RE Tunnel	VLAN VXLAN	- Basic				- Filters					5	Rat
Interfaces						Interface	ether1		Ŧ	Src. Address :	0.0.0/0					dan.
Wireless		The Detect Internet				Entry Timeout	00:00:03		s	Dst. Address :	0.0.0/0					aup
😝 WireGuard	Name	Туре	Actual MTU	L2 MTU T	x					Sm Address .	/1				0	lose
💥 Bridge	R ether1	Ethemet	1500	1598	19.					Sic. Houlesso.					New	Window
The PPP	R ether3	Ehenet	1500	1598	118					Dst. Address6 :				^		
🙄 Switch	ether4	Ethemet	1500	1598						MAC Protocol :	all			₹ ▲		
T Mach	🔶 ether5	Ethernet	1500	1598						Protocol :	any			.		
is in N	R 🚸 ether6	Ethernet	1500	1598	6.1											
₩ F	ether/	Ethernet	1500	1598						Port :	any			•		
2 IPV6 P	ernero de ether9	Phenet	1500	1598						VLAN Id :	any			₹ ▲		
O MPLS P	ether10	Ethernet	1500	1598						DSCP :	any			₹ ▲		
🕽 Routing 🗈 🗎	•	-											_			
¦∰ System I	11 items					Eth / Prot	100 Src.	0.445 (Dst.	2.54210	VLAN k	DSCP	Tx Rate	Rx Rate	Tx Pack	. Rx Pa
🐥 Queues						000 (p)	6 (top) 193.217.146 6 (top) 50 20 18 96	1.0.440 (SMD) 1.445 (emb)	192,168,1	2.54216 2.54217			0 bps	Obps		n
Files	Log					10 (c)	6 (tcp) 173.249.57.	77:445 (smb)	192,168,1	2:54249			0 bos	Obos	i	Ď
🗏 Log	Y Free				ind al	₹ 00 (p) 17	(udp) 157.240.217	7.63:443 (https)	192.168.1.	2:40867			0 bps	Obps	(0
AP RADIUS	# Time Buller	Taks	Wesserger			*									_	
V Toole	61 Jul/21/2023 1/1:23:12 memory	y system, inc. scroot i v system, info	ac adminio/gad e mancetime jul/22	2023 14:23:12	570.47.00 valvenici -> Jul.21/2023 14:2	3	_						_		_	•
MI New Transied	05 Jul/21/202314/2342 memory	y system.info s	ustem time zone se	tings changed	by admin	items	Total Tx: 46.2	kbps Total	Rx: 13.3 kbps	Total Tx P	acket: 34		Total R	x Packet: 1	6	
A Durit	65 JB/2 1/2023 1/1/24/22 heno 67 JB///1/2023 1/1/24/44 memory	y system inc account a	aer adnin kojged i ner adnin kojged i	af ton 38.90%	6394700 Valwindox 63944400 Valwindox	× Frewal										
🌼 Dot1X	00 Jil/21/202314:24:20 memory	n system, inc, scourt u	seradnin logged i	from 00:0000	ADH 7:30 vie window	Ch. D.L.										
💷 LCD	70 Jul/21/202314.24.34 memory	y sydem, info, ecrount o	ær adninksgen i	fren 98.50.96.	A9.4700 vie wirken	* Hiter Hules	NAT Mangle	Raw Service F	Ports Connect	tions Address	Lists Layer7	Protocols				
MetaROUTER	/1 Jal/21/202314/24:35 memory	y ayalom, ind, sceount a	acradhin loggod e	ut ron 589):9	6.NB:41:CC via vinbo	× 🗕 🗆 🛛	/ 🛛 🗗 🍸	(O Reset Cou	unters (O Re	set All Counters						
🦺 Partition	70 Jul/21/202014/24:40 Include	y system, inc. account i n sustan, infu, succuri, i	se adminiogen i se adminiogen i	ut ion 30.3036	994 / 1. W WHHM 6.10.47.CC via visitu			Cu. Addama	Da Addam	Duty Co. Du	Da Da	In Inter-	0.4.14	In Ister	0.1.1.1	C- A
Nake Supout rf	// JJ//1/02314/442 menty T_11/05/00254/0144	y eyelem, into, account a	aer adnin logged i	100058 mm	494 / II vis winhow	- PORT	KNOK TAHAP 1	SIC. Address	USL MULIESS	FIOLO SIC. FUI	Ust. Foil	n. ner.		n. n.e	ou. n	SIC. H
New WinBox	76 Jul/21/202314/24:46 momo	y system, info, account o	acradnin logged i	from 38:90.96	/9:47CC via white:	0 0	add input			1 (ic						
🖬 Eve	// J8/21/202314:24:1/ memory	y system inc. acrount i	ser adnin logged e	ut ton SESDS	6 AB:410L via virbo	×PORT	KNOCK VERIFIKAS	51								
	/0 40/21/202314:24:30 Reno /4 30/21/202314:24:32 memory	y system, inc. sciouri, u y system, inc. sciouri i	ser adminilo)ged r ser adminilo)ged r	at you SEGUR	6 AR-44CE via vinte	× 1 🖬	add input			6 (tcp)	1111					
	80.161/21/20231d:2617 memory	y eystem liftin, anvnunt i	er adminlinged i	fmm 98-90-96	ARE 710 Valuetion	BLOKE	R WINBOX UNTUK	KNOCK		CA 1	21 22 22					1.00
Windows D	82 Jul/2 1/2023 14/24/30 memory	y system, inc, sciouri, u y system, inc, sciouri, u	ser adnin iojqed i ser adnin iojqed i	1 from 38:30:36	ABATCC VA WINDS	2 2	arop input			p (tcb)	21,22,23,					IVERI
	83 Jul/21/202314.25.03 monor	y system info, second o	ac adhirilogad e	ut ion 98.9).9	6.18.4 ² .00 via virbo											
		avalant ind account is	acradnin losood i	1000 35:30.36	7574 / LU Viz Winbox											
	85 Jul/21/202314/25:07 memory	system, info, account u	ser adminilio;ged o	ut iron 98:90:9	6AB:47:00 vta virbo	xI.										

c. Tanggal 22 Juli 2023

Safe Mode	Session: 10.10.0.1																
🎾 Quick Set	Interface List					Torch											
CAPSMAN	Interface Interface List	Phamat FolP Tunnel	IP Turnel G	E Turnel VI		- Basic					Filters						9at
Interfaces						Interfa	ce: ether			Ŧ	Src. Address	0.0.0/)				-
Wireless		Detect Internet				Entry Timer	ve: 00:00	63			Det Address		1		_		stop
😝 WireGuard	Name	∠ Туре	Actual MTU	L2 MTU Tx			00.00				Car Addarde				Ξ.	0	llose
3 Bridge	R	Ethernet	1500	1598	19.	1					SIC. HOURESSO					New	Window
2. PPP	R opener2	Ethemet	1500	1598	325.						Dst. Address6	: 🗌 🗆 🗌			^		1111001
🖳 Suitch	ether4	Ethernet	1500	1598	110	1					MAC Protocol	al					
*1° Mash	ether5	Ethernet	1500	1598							Protocol	anv					
	R 🚸 ether6	Ethernet	1500	1598	6.1							uny					
Ψ.P. Γ	ether?	Ethernet	1500	1598							Port	any			•		
🛫 IPv6 🛛 🗅	ether8	Ethernet	1500	1598							VLAN Id	any			¥		
🕐 MPLS 🛛 🗅	ether10	Ethernet	1500	1598							DSCP	any			7 4		
🕽 Routing 🗈 🗈	•																
🔅 System 🗈	11 items					Eth / P	rotocol	Src.		Dst.		VLAN I	d DSCP	Tx Rate	Rx Rate	Tx Pack.	Rx Pa
Queues						800 (p)	6 (tcp)	193.217.148	3.8:445 (smb)	192.168	1.2:54216			0 bps	Obps		0
Files	Log					800 (p)	6 (tcp)	00.20.18.96 173.249.57	:440 (SMD) 77:445 (emb)	192.168	1.2:04217			0 bps	Obre		0
E log	T Freeze				al	800 (p)	17 (udp)	157.240.217	7.63:443 (https)	192,168	1.2:40867			0 bps	Obos		0
	# linc Buta	opics M	iasogo														
	41 Jul/22/202314:14:48 memor	y system.mio sy	stem time zune setun	as changed by acm	n	•											٠
X Tools	42 Jul/22/202314.14.34 INSTRE 23 14/02/202312.12.56 Instrem	y system, mu, account us y system, min, account us	er atminitigged in in er atminitigged mit i	111 35.51.36 A2.473 98 90 96 49 47	CC vie wintex TCC six winters	125 items	Td	al Tx: 46.21	dops Tot	al Rx: 13.3 kbp	s Total Tx I	Packet: 34		Total F	ik Packet: 1	16	
🕮 New Terminal	44 Jul/22/202314:14:50 memor	y system, mo, account us	eradım loqqed ii fiq	m 90:90:90 AS:475	C vie writex	Dennel											
Dot 1X	45 Ja/22/302314:15:01 moment 40 Ja/20/00/314/15/05 moment	y system, into, account us y system into account us	cradmin logged aut t cradmin lagged is fin	ren 9858-963/947 m 93/93/96 / 5-47-0	PCC via winbox (C via winber	ritewal											
💻 LCD	47 Jul/22/202314.15.06 memory	y yelen, his, account un	er admin logged out l	iun 98.90.96.49.47	7CC via misbox	Filter Rule	S NAT	Mande	Raw Service	Ports Conne	ctions Address	Lists Laver7	Protocols				
🖳 MetaROUTER	/8 H/02/0031/1510 memor	y system, info, account us	er admin logged in fr	m 93 91 96 45 47 (CC via winhex												
🔔 Parttion	50 Jul/22/202014:15:15 memory	y system info, account us	eradnin logged in fit	m 00:00:00 A5:47:	C vie winbcz	+ -		87	(O Reset C	ounters 🛛 🛈 F	leset Al Counters						
Make Support of	51 LL/22/202314-15-16 memor	y system, irfo, account us	eradmin logged out f	ren 9850 96 4947	TCC via winhox		6 m	a -	C AU	D. AU			1.11	0.11	1.1.	0.11	C 11
Mary Was Day	52 JU/22/202314:1521 Inemor	y system, mo, account us	er actin logged in th ar actin logged out f	m 35.3136 A3.4/3 mn 99.90-90-1947	CC via writex	#	ACCON	unan	SIC. ADDress	Ust. Address	PT010 SIC. P0	USL POR	n. rter	v.t. int	. n. mer	ut. n	SIC. AD
View Wribox	54 Jul/22/202314:1528 memor	y system, into, account us	er admin logged in th	m 98:50:36 A5:4/1	CC via winbox	PUK	I KNOK I	ahar i									
🔣 Ext	55 Jul/22/202314(15/2) memory FC LL/20/002317(15/1)	y system, into, account us	eradnin logged aut f	ren 3050:96,4947 	PCC via winbox	0	add	nput			1 (iC						
	57 JJ/22/202314:13:42 memor	y system, info, account us	eradnih logged otti	ren 98.90:96:79:47	TCC via winbox	= POR	I KNOCK	VERIFIKASI			CA 1						
💻 Windows 🛛 🗅	58 Jul/22/202314:1x/6 memory	y eyelen, into, account us	er admin logged in th	m 93:90:96 A\$:4/:	CC via winbox		add	nput			6 (tcp)						
	59 JU/22/902314(1):1/ memor	y system mollaccount us	er actin logged auf 1 er actin logged is fin	101 3030/36/A3R/ m 03:50:30 A5:47:	C via windox	= BLO	CH WIND	JX UNTUK	KNUCK								
	61 Jul/22/202314.15.52 memory	y system, info, account us	er admin logged cut l	on 9850.96.49.47	7CC via windox	2	🐺 drop	nput			e (tcp)	21,22,23,	-				IVERIV
	02 Jul/22/202314:1557 memory	y system, info, account us	er admin logged in fra	m 00:50:00 A5:475	CC via winbox												
	the second state in the	And the second second second second	a summing a sum	and an or an or a	Co. See Provide	-											

d. Tanggal 23 Juli 2023

Cafe Mode	Session: 10.10.0.1													
🖌 Quick Set	Interface List						Torch							ļ
🔉 CAP\$MAN	Interface Interface	list Phy	amet FolP Tunnel	IP Tunnel G	RE Turnel	VIAN VXIA	Basic			Fiters				Qat
Interfaces						1011 1101	Interface:	ether1	ī	Src. Address : 00	0.0/0			
Wireless	+• - 🗸 🖄		Detect Internet					00.00.00			0.0.0		=	Stop
WireGuard	Name	I.T	ype	Actual MTU	L2 MTU	Tx	Entry limeout:	00:00:03	5	Ust. Address : 0.0	.0.0/0		^	Close
Pideo	R 🚸 ether 1	B	shemet	1500	1598	19				Src. Address6 : 📃 🗆	J			
s bioge	R 🚸 ether2	B	themet	1500	1598	325				Det Address6 · .				New Winde
E PPP	R 🚸 ether3	B	themet	1500	1598	118	•							
Switch	 ether4 	B	shemet	1500	1598					MAC Protocol : al			₹ ▲	
Mesh	ether5	B	themet	1500	1598					Protocol : any			₹ ▲	
BIP N	H @ ether6	8	shemet	1500	1598	6.				0.1				
Aller N	wether/		themet	1500	1500					Port : any			+ •	
PV0 I	de ether9	P	themet	1500	1598					VLAN Id : any			₹ ▲	
J MPLS P	dether10	B	themet	1500	1598					DSCP - any			T A	
🖈 Routing 🛛 🗅										boor . uny				
🗄 System 🗈	11 itame						Eth / Proto	col Src.	Dst.	V	LAN IJ DSCP T	x Rate Rv	x Rate	Tx Pack Rx
							800 (ip) 6	(tcp) 193.217.148.8:445	(smb) 192.168	1.2:54216		0 bps	0 bps	0
F doctors						-		(tcp) 50.20.18.96:445 (sn	nb) 192.168	1.2:54217		0 bps	0 bps	0
Files	log					_		(tcp) 173.249.57.77:445	(smb) 192.168	1.2:54249		0 bps	0 bps	0
Log	Y Freeze						7	(udp) 157.240.217.63:443	3 (https) 192.168	1.2:40867		0 bps	0 bps	0
P RADIUS	// Tne	Eufer	Topice N	Hotage			•							
Tools N	15 Jan/01/2002 01:05:32 16 Jan/01/2003 01 05:02	THEFTON,	eyeten info, account us	er admin logged in h anne line, lan/01/2	om 38:30:36:4 002 01 05 02	#947CC via wirbox #93/07CC via wirbox	· ·							
II New Terminal	1/ 44/3/28/310 (542	heroy	system into si	den fine zone setti	gs changed h	y adhir		Total Tx: 46.2 kbps	Total Rx: 13.3 kbp	os Total Tx Packet: 3	4	Total Rx F	Packet: 16	\$
M New Tellinia	TE ad//3/2021(11(5-14	neroty	system into 18	ernie changed by a	dirin		6	rewal						
P Dot IX	20 Jul/23/2023 01:65:14	TOPON	aviton nic ili	erruic changed by a erruic changed by a	arın dirin				1					
LCD	21 Jul/23/2023 01:55:16	neros,	dhop, linfe di	cp3 deaptigned 12	12.12.251 from	n 80 5A:CA 81:80 90		Filter Rules NAT Man	igle Raw Service	Ports Connections Addr	ess Lists Layer7	Protocols		
MetaROUTER	22 Jul/23/2023 01 05:24	net ony	system nic, account us	er adminikuqed in fi	um 10.10.10.2	23 via visitos			To Paul Ca	mine Co Devel M Course				
Patition	25 JU/25/2425 U 15/27	teroy	system mic, account ina system mic ina	er admin logged out while changed by a	101 26.30 36 trin	AGA/JUC Warwindox			I TO Reset CO	uniers IN Reset Air Court	leis			
Mile Court of	75.44/23/2023.01(5:29	neroy	system mic in a	walls changed by a	tinn			# Action Chain	Src. Address	Dst. Address Proto Src	. Port Dst. Port	In. Inter	. Out. Int	In. Inter ()
Make Supout m	26 Jul/23/2023 0 105:33 27 Jul/23/2023 0 105:33	TOPON TOPON	system rife, account up avidem rife, account up	er admin legged o.t. er admin legged in fi	fon: 10, 0, 0 nn: 90-96-96-0	1253 va wrbez 19:1700 vis wiekw		PORT KNOK TAHAP	1					
New WinBox	26 Jul/23/2023 01:05:48	THEONY	eyeten infc, account us	er admin logged in fi	om 38:30,96:4	19:17 OC via wirbox		0 📑 add input		1 (c				
🕻 Exit	25 Jul/23/2023 01 05:49	neroty	system info, account i us	er adminiktyged oct	fun 98.90 96	AB.47.00 via ministra		PORT KNOCK VERI	HKASI	(t +)				
	30 Jul/23/2023 010559	teroy	system nic, account us	er adminitigged in h er adminitioned o f	um 36.30.36.4 tmm 10.10.16	RSA/CE valimbox Abb/IT via winterv		1 add input	TURNOCK	6 (tcp)	1111			
Madaura N	32 Jul/23/2023 0 106:03	nerroty	choo.urfe dr	cp5dcaaagnod 14	14.14.254 from	n B0 5/\:C/\ B4:BD 90		BLOKIH WINBUX UN	NTUK KNUCK	(Arra)	21 22 22			
- WEIDOWS	33 Jul/23/2023 0 156:03	10105	system info, account up	er admin logged in fi	om 98:90:96:/	947CE va wrbox		z 🐥 urop input		o (cch)	21,22,23,	-		
	35 Jul/23/2123 01 06.09	THEFOY,	evelan nic, account up	er admin izgeed o.c. er admin kuued in fi	nom 38.90 96.4 um 98.90 96.4	8.470C via whock								
	36 Jul/23/2023 01.06.10	nenoy	system info, account i us	er admin logged out	fium 58.90 96	AB.47.00 via ministra								
	3/ al//3/2010(614	teroy	system into account un	er admin logged in h	om (BHIDHD) Inne Underson	94/OD via without								

e. Tanggal 24 Juli 2023

•														_		_	_
🖌 Quick Set	Interface List					Torch											
CAP\$MAN	Interface Interface List	Ethernet EoIP T	unnel IP Tunnel	GRE Tunne	VLAN VXLA	N Basic					- Fiters					Sta	t
Interfaces						Interfac	e: ether1			Ŧ	Src. Address	: 0.0.	0.0/0				_
Wireless		The section of the se	ntemet			Fritry Times	+ 00.00.03				Det Address	- 00	0.0/0			Sto	ρ
🙌 WireGuard	Name	/ Type	Actual MT	U L2 MTU	Tx	uniy mico	a. 00.00.00				0		0.0/0			Clos	æ
C Bridge	R @ ether1	Ethernet	1	500 159	3 1	2					Src. Addressb	: [] []/0			-	New M	lada
- PPP	R dether3	Bhemet	1	500 155	3 32	2					Dst. Address6	: 🗌 :/0				IVEW IVI	nuo
T Switch	ether4	Ethernet	1	500 159	3	1					MAC Protocol	al			₹ ▲		
"I" Mash	🚸 ether5	Bhemet	1	500 159	3						Destaced	200					
	R 🚸 ether6	Ethernet	1	500 159	3 6	1					Pittocol	. driy					
	ether?	Ethernet	1	500 159	3						Port	: any			₹ ▲		
P IPV6 P	w ethero	Bhenet	1	500 155	2						VLAN Id	: any			¥ 🔺		
MPLS N	ether10	Ethernet	1	500 159	3						DSCP	anv			Ŧ ▲		
Routing 🗅	•										500						
🛱 System 🛛 🗅	11 items			-		Eth / Pr	otocol Src			Dst.		VL	AN Id DSCP	Tx Rate	Rx Rate	Tx Pack F	Rx P
Queues	1					800 (ip)	6 (tcp) 193	217.148.8:445	(smb)	192.168.1	2:54216			0 bps	0 bps	0	
Files						800 (p) 200 (n)	6 (tcp) 50.2	20.18.96:445 (st 249.57.77-445	mb) (omb)	192.168.1	2:54217			0 bps	Obps	0	
	France					800 (p)	17 (udp) 1/3	243.57.77.445	(smb) 3 (https)	192 168 1	2.34243 2.40867			0 bps	Obps	0	
P RADIUS	1 110020																
	# Time	Buffer Topic	s I	lessage	1 10 10 7 105 6	•											•
N 100IS	984 Jul/24/2023 15:29:1	o memory uncp. 1 memory dhop	info d	hon 1 assigne	d 10.10.7.10510f d 10.10.7.92for 8	2 125 items	Total 1	fx: 46.2 kbps	Total R	bc: 13.3 kbps	Total Tx	Packet: 34	ļ.	Total R	x Packet: 1	6	
au new remnal	985 Jul/24/2023 15:30:0	8 memory dhcp.	info d	hcp1 deassig	ned 10.10.0.16												-
Dot1X	986 Jul/24/2023 15:30:0	8 memory dhcp.	info d	hcp1 assigne	d 10.10.0.1621	rewall											
LCD	987 Jul/24/2023 15:30:1	4 memory dhcp.	info d	hcp1 assigne	d 10.10.7.106	Filter Rules N	AT Mangle	Raw Servi	ice Ports (Connections	Address Lists	Layer7 F	Protocols				
MetaROUTER	988 Jul/24/2023 15:32:5	4 memory dhop.	info d	hcp1 deassig	ned 10.10.7.10				Countern	C Runt M	Counterer						
Partition	990 Jul/24/2023 15:39:1	2 memory drup, 1 memory drup,	info d	hon 1 deassig	ned 10.10.7.30			I TO Hese	Counters	to neset A	Courters						
Make Supout if	991 Jul/24/2023 15:40:1	4 memory dhcp.	info d	hcp1 deassic	ned 10.10.7.10	# Action	Chain	Src. Addre	ss Dst. Adv	dress Proto.	Src. Port	Ost. Port	In. Inter 0	.t. int in. in	ter Out. I	nt Src. Ad.	D
New WinBox	992 Jul/24/2023 15:40:2	9 memory dhcp.	info d	hcp1 assigne	d 10.10.7.92 fc	PORT KNO	K TAHAP 1			14.							
ZI For	993 Jul/24/2023 15:42:1	3 memory dhcp.	info d	hcp1 deassig	ned 10.10.0.16	- PORT KNO	CK VERIEK	121		1 (C							
	994 Jul/24/2023 15:42:1	3 memory dhcp.	into d	hcp1 assigne	d 10.10.0.1621	1 📑 adi	d input			6 (top)		111					
	996 Jul/24/2023 15:45:0	0 memory system 0 memory dbco	info, account u	ser sidik logg bon 1 deassio	red 10 10 3 23	BLOKIR W	NBOX UNTU	JK KNOCK									
Windows P	997 Jul/24/2023 15:47:0	2 memory dhco.	info d	hcp1 assigne	d 10.10.7.1071	2 🗱 dro	p input			6 (tcp)		21,22,23				IVERIV.	
	998 Jul/24/2023 15:48:4	0 memory dhcp.	info d	hcp1 deassig	ned 10.10.7.92												
	000 LU(04/0000 1E.49.4	memory dhon	info d	hon1 assigns	d 10 10 7 926												