

**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN  
TEKNOLOGI INSTITUT TEKNOLOGI DAN BISNIS  
PALCOMTECH**

**SKRIPSI**

**KEAMANAN JARINGAN MENGGUNAKAN TEKNIK DMZ  
DENGAN SISTEM OPERASI LINUX PADA DIAL MUSIK**



**Diajukan oleh:**

- 1. HUANITO ALFIANSYAH /011190082**
- 2. KI AGUS SOLIHIN /011190083**

**Untuk Memenuhi Sebagian dari Syarat**

**Mencapai Gelar Sarjana Komputer**

**PALEMBANG**

**2023**

**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN  
TEKNOLOGI INSTITUT TEKNOLOGI DAN BISNIS  
PALCOMTECH**

**SKRIPSI**

**KEAMANAN JARINGAN MENGGUNAKAN TEKNIK DMZ  
DENGAN SISTEM OPERASI LINUX PADA DIAL MUSIK**



**Diajukan oleh:**

- 1. HUANITO ALFIANSYAH /011190082**
- 2. KI AGUS SOLIHIN /011190083**

**Untuk Memenuhi Sebagian dari Syarat**

**Mencapai Gelar Sarjana Komputer**

**PALEMBANG**

**2023**

**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN  
TEKNOLOGI INSTITUT TEKNOLOGI DAN BISNIS  
PALCOMTECH**

---

**HALAMAN PENGESAHAN PEMBIMBING SKRIPSI**

**NAMA/NPM** : 1. HUANITO ALFIANSYAH /011190082  
2. KI AGUS SOLIHIN /011190083

**PROGRAM STUDI** : INFORMATIKA

**JENJANG PENDIDIKAN** : STRATA SATU

**JUDUL** : KEAMANAN JARINGAN  
MENGUNAKAN TEKNIK DMZ  
DENGAN SISTEM OPERASI LINUX  
PADA DIAL MUSIK

**Tanggal:**  
**Pembimbing**

**Mengetahui,**  
**Rektor**

**Eko Setiawan, S.Kom., M.Kom**  
**NIDN: 0208098703**

**Benedictus Effendi, S.T., M.T.**  
**NIP: 09.PCT.13**

**KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN  
TEKNOLOGI INSTITUT TEKNOLOGI DAN BISNIS  
PALCOMTECH**

---

**HALAMAN PENGESAHAN PENGUJI SKRIPSI**

**NAMA/NPM** : 1. **HUANITO ALFIANSYAH**  
**/011190082**

2. **KI AGUS SOLIHIN**  
**/011190083**

**PROGRAM STUDI** : **INFORMATIKA**

**JENJANG PENDIDIKAN** : **STRATA SATU**

**JUDUL** : **KEAMANAN JARINGAN**  
**MENGGUNAKAN TEKNIK DMZ**  
**DENGAN SISTEM OPERASI LINUX**  
**PADA DIAL MUSIK**

**Tanggal:**

**Penguji 1**

**Tanggal:**

**Penguji 2**

**Benedictus Effendi, S.T., M.T.**

**NIDN: 0221027002**

**Eka Prasetya Adhy Sugara, S.T., M.Kom.**

**NIDN: 0224048203**

**Menyetujui,  
Rektor**

**Benedictus Effendi, S.T., M.T.**

**NIP: 09.PCT.13**

**MOTTO:**

Sesungguhnya sesudah kesulitan itu ada kemudahan. Maka apabila kamu telah selesai (dari suatu urusan), kerjakanlah dengan sungguh-sungguh (urusan) yang lain.

(Q.S Al -Insyirah 7-8).

**Kupersembahkan kepada:**

- *Allah SWT yang telah memberikan keringan dan kemudahan dalam pekerjaan kami.*
- *Orang tua dan saudara/i yang selalu mendukung dan mendoakan kami.*
- *Kepada bapak Eko Setiawan. S.Kom., M.Kom selaku dosen pembimbing yang selalu memberikan bimbingan serta arahan yang baik sehingga skripsi ini bisa terselesaikan.*
- *Teman-teman seperjuangan yang selalu memberikan semangat dan dukungan.*

## KATA PENGANTAR

Dengan mengucapkan Alhamdulillah Puji dan syukur kehadiran Allah SWT yang telah memberikan rahmat dan hidayah-nya yang telah memberikan banyak kesempatan, sehingga dapat menyelesaikan penulisan skripsi yang berjudul **“Keamanan Jaringan Menggunakan Teknik DMZ dengan Sistem Operasi Linux Pada Dial Musik”** ini dapat diselesaikan guna memenuhi salah satu persyaratan dalam menyelesaikan program studi S1 Informatika Institut Teknologi dan Bisnis Palcomtech Palembang.

Sebagai rasa syukur melalui kesempatan ini peneliti mengucapkan banyak terima kasih kepada semua pihak yang telah membantu, serta memberikan segala saran, motivasi, dan semangat dalam proses penulisan laporan skripsi ini. Untuk itu peneliti mengucapkan terima kasih kepada orangtua tercinta, kepada bapak Rektor Institut Teknologi dan Bisnis Palcomtech Bapak Benecdictus Effendi. S.T., MT. Kepada dosen pembimbing kami Bapak Eko Setiawan. S.Kom., M.Kom yang telah banyak membantu kami dalam penyelesaian laporan skripsi ini.

Demikian kata pengantar dari peneliti, dengan harapan semoga skripsi ini berguna dan bermanfaat bagi semua pihak yang membutuhkan, dengan kesadaran peneliti bahwa penulisan skripsi masih mempunyai beberapa kekurangan sehingga membutuhkan banyak saran dan kritik yang membangun untuk menghasilkan

sesuatu yang lebih baik. Akhir kata, atas perhatiannya peneliti ucapkan terima kasih.

## DAFTAR ISI

HALAMAN JUDUL .....	i
HALAMAN PENGESAHAN PEMBIMBING SKRIPSI .....	ii
HALAMAN PENGESAHAN PENGUJI SKRIPSI .....	iii
HALAMAN MOTTO DAN PERSEMBAHAN .....	iv
KATA PENGANTAR .....	v
DAFTAR ISI .....	vi
DAFTAR GAMBAR .....	ix
DAFTAR TABEL .....	xi
DAFTAR LAMPIRAN .....	xii
ABSTRAK .....	xiii
ABSTRACT .....	xiv
<b>BAB I .....</b>	<b>1</b>
<b>PENDAHULUAN .....</b>	<b>1</b>
1.1. Latar Belakang .....	1
1.2. Rumusan Masalah Penelitian .....	2
1.3. Ruang Lingkup Penelitian .....	2
1.4. Tujuan Penelitian .....	3
1.5. Manfaat Penelitian .....	3
1.5.1. Manfaat Bagi Penulis .....	3
1.5.2. Manfaat Bagi Akademik .....	3
1.5.3. Manfaat Bagi Dial Musik .....	4
1.6. Sistematika Penulisan .....	4
<b>BAB II .....</b>	<b>6</b>
<b>GAMBARAN UMUM PERUSAHAAN .....</b>	<b>6</b>

2.1.	Profil Perusahaan .....	6
2.1.1.	Sejarah Perusahaan .....	6
2.1.2.	Visi dan Misi .....	7
2.1.3.	Struktur Organisasi .....	7
2.1.4.	Tugas dan Wewenang .....	8
<b>BAB III</b>	.....	<b>11</b>
<b>TINJAUAN PUSTAKA</b>	.....	<b>11</b>
3.1.	Landasan Teori .....	11
3.2.	Penelitian Terdahulu .....	15
3.3.	Kerangka Pemikiran .....	17
<b>BAB IV</b>	.....	<b>18</b>
<b>METODE PENELITIAN</b>	.....	<b>18</b>
4.1.	Lokasi dan Waktu Penelitian .....	18
4.2.	Teknik Pengumpulan Data .....	19
4.3.	Teknik Pengembangan Sistem .....	19
<b>BAB V</b>	.....	<b>21</b>
<b>HASIL DAN PEMBAHASAN</b>	.....	<b>21</b>
5.1.	Analisis .....	21
5.1.1.	Activity Diagram Tanpa Keamanan Demilitarized Zone (DMZ) ...	22
5.1.2.	Deployment Diagram Tanpa Keamanan Demilitarized Zone (DMZ)	23
5.1.3.	Component Diagram Tanpa DMZ .....	24
5.1.4.	Analisa Kebutuhan Hardware dan Software .....	24
5.2.	Desain .....	25
5.2.1.	Desain Activity Diagram .....	26
5.2.2.	<i>Desain Deployment Diagram</i> .....	27
5.2.3.	<i>Desain Component Diagram</i> .....	28
5.3.	Implementasi .....	28
5.3.1.	Instalasi Sistem Operasi Linux Debian 11 .....	29
5.3.2.	Konfigurasi <i>IP Address</i> .....	30
5.3.3.	Konfigurasi Packet Forwarding .....	34
5.3.4.	Konfigurasi Demilitarized Zone (DMZ) .....	36

5.4. Monitoring.....	41
5.5. Management.....	43
5.6. Pengujian.....	44
<b>BAB VI.....</b>	<b>45</b>
<b>PENUTUP.....</b>	<b>45</b>
6.1. Kesimpulan.....	45
6.2. Saran.....	45
<b>DAFTAR PUSTAKA.....</b>	<b>xii</b>

## DAFTAR GAMBAR

Gambar 2.1 Struktur Organisasi Dial Musik dan Sport. ....	8
Gambar 3.1 Kerangka Pemikiran .....	18
Gambar 4.1 Network Development Life Cycle (NDLC). ....	20
Gambar 5.1 Topologi Jaringan Tanpa Keamanan Demilitarized Zone (DMZ). ....	21
Gambar 5.2 Activity Diagram Tanpa DMZ. ....	22
Gambar 5.3 Deployment Diagram Tanpa DMZ. ....	23
Gambar 5.4 Component Diagram Tanpa DMZ. ....	24
Gambar 5.5 Topologi dengan DMZ. ....	25
Gambar 5.6 Activity Diagram Dengan DMZ. ....	26
Gambar 5.7 Deployment Diagram Dengan DMZ. ....	27
Gambar 5.8 Component Diagram Dengan DMZ. ....	28
Gambar 5.9 Instalasi Sistem Operasi Linux Debian 11. ....	29
Gambar 5.10 Tampilan Command Line Interface (CLI) Linux Debian 11. ....	30
Gambar 5.11 Konfigurasi IP Address (Bagian I). ....	31
Gambar 5.12 Konfigurasi IP Address (Bagian II). ....	32
Gambar 5.13 Konfigurasi IP Address Bagian (III). ....	33
Gambar 5.14 Konfigurasi IP Address (Bagian IV) .....	34
Gambar 5.15 Konfigurasi Packet Forwarding (Bagian I). ....	35
Gambar 5.16 Konfigurasi Packet Forwarding (Bagian II). ....	36

Gambar 5.17 Konfigurasi Demilitarized Zone (Bagian I).....	37
Gambar 5.18 Konfigurasi Demilitarized Zone (Bagian II).....	37
Gambar 5.19 Konfigurasi Demilitarized Zone (Bagian III).....	39
Gambar 5.20 Konfigurasi Demilitarized Zone (Bagian IV).....	40
Gambar 5.21 Konfigurasi Demilitarized Zone (Bagian V).....	41
Gambar 5.22 Monitoring dengan network statistic (nstat).....	42
Gambar 5.23 Monitoring dengan IPTables.....	43
Gambar 5.24 Hasil Pengujian Tanpa Demilitarized Zone (DMZ).....	44
Gambar 5.25 Hasil Pengujian Demilitarized Zone (DMZ).....	45

## DAFTAR TABEL

Tabel 3. 1 Penelitian Tedahulu .....	15
Tabel 4. 1 Waktu Penelitian .....	18

## **DAFTAR LAMPIRAN**

1. Lampiran 1. Form Topik dan Judul (Fotokopi)
2. Lampiran 2. Surat Balasan dari Perusahaan (Fotokopi)
3. Lampiran 3. Form Konsultasi (Fotokopi)
4. Lampiran 4. Surat Pernyataan (Fotokopi)
5. Lampiran 5. Form Revisi Ujian Pra Sidang (Fotokopi)
6. Lampiran 6. Form Revisi Ujian Kompre (Asli)

## ABSTRAK

HUANITO ALFIANSYAH, KI AGUS SOLIHIN: Keamanan Jaringan Menggunakan Teknik DMZ dengan Sistem Operasi Linux Pada Dial Musik.

Keamanan jaringan adalah salah satu hal yang harus diperhatikan pada saat ini. Tanpa adanya suatu keamanan jaringan yang baik akan menyebabkan banyak kerugian, salah satunya kerusakan pada komputer *server*. Komputer *server* adalah salah satu komputer yang harus dilindungi dan dijaga dengan keamanan khusus diantaranya menggunakan teknik *Demilitarized Zone* (DMZ). DMZ adalah sebuah teknik keamanan yang dapat melindungi komputer *server* dengan membuat suatu zona demiliterasi untuk komputer *server* sehingga komputer *server* tidak dapat di akses secara langsung dari luar. Tujuan penelitian untuk menghasilkan keamanan jaringan dengan teknik *demilitarized zone* (DMZ) menggunakan *firewall iptables* dengan sistem operasi Linux, guna untuk mencegah dan mengatasi permasalahan keamanan jaringan yang terdapat pada *showroom* Dial Musik agar dapat memberikan keamanan bagi pengguna jaringan Dial Musik. Untuk menerapkan teknik keamanan DMZ bisa menggunakan komputer yang akan digunakan sebagai *router* dengan *firewall iptables* pada sistem operasi Linux Debian 11. DMZ menggunakan konsep *Network Address Translation* (NAT) yaitu meneruskan lalu lintas yang masuk ke alamat yang sudah ditetapkan. Metode dalam penelitian ini menggunakan metode NDLC. Pengujian dilakukan menggunakan *metode network development life cycle* (NDLC) yang menerepkan pengujian 2 kondisi, yaitu sebelum dan sesudah penerapan keamanan jaringan *server*. Hasil dari penelitian sistem operasi Linux Debian 11 bisa dijadikan sebagai sistem operasi *router*.

**Kata Kunci:** Keamanan Jaringan, DMZ, *Iptables*, Linux, Debian 11.

## ABSTRACT

*HUANITO ALFIANSYAH, KI AGUS SOLIHIN: Network Security Using DMZ Technique with Linux Operating System on Dial Musik.*

*Network security is one of the things that must be considered at present. Without good network security, there will be a lot of losses, one of which is damage to the server computer. The server computer is one of the computers that must be protected and maintained with special security, including using the Demilitarized Zone (DMZ) technique. DMZ is a security technique that can protect the server computer by creating a demilitarization zone for the server computer so that it cannot be accessed directly from the outside. The research objective is to produce network security with the DMZ technique using iptables firewall with Linux operating system, in order to prevent and solve network security problems that exist in the Dial music showroom in order to provide security for Dial music network users. To implement DMZ security technique, a computer that will be used as a router with iptables firewall on the Linux Debian 11 operating system can be used. DMZ uses the concept of Network Address Translation (NAT), which forwards incoming traffic to the predetermined address. The method used in this research is the NDLC method. Testing is done using the network development lifecycle (NDLC) method which implements 2 testing conditions, before and after the application of server network security. The results of the Linux Debian 11 operating system research can be used as a router operating system.*

**Keywords:** *Network Security, DMZ, Iptables, Linux, Debian 11*



# BAB I

## PENDAHULUAN

### 1.1. Latar Belakang

Pesatnya perkembangan dalam bidang teknologi informasi sekarang dalam bidang jaringan bukanlah sesuatu hal yang baru bagi kita karena jaringan internet ini dapat kita jumpai di setiap tempat. Dalam jaringan internet pentingnya keamanan jaringan komputer agar dapat mencegah dan menjaga keamanan data sehingga terhindar dari kerusakan dari virus maupun serangan dari penyusup, berbagai macam teknik serangan terus berkembang di era sekarang dan tidak bisa kita abaikan. Untuk itu kita perlu mempersiapkan keamanan untuk mengamankan dan meminimalisir ancaman pada jaringan.

Dial Musik merupakan suatu *showroom* alat musik dan *sport* yang bergerak di bidang penjualan contohnya seperti gitar, *sound system*, bola kaki, sepatu olahraga dan lain-lain. Dial Musik ini terbagi dalam tiga *divisi* yaitu *divisi* bagian alat musik, *audio*, dan alat olahraga, dan untuk keamanan jaringan di *showroom* Dial Musik ini belum ada sama sekali, jadi perlu adanya sistem keamanan pada jaringan untuk menjaga data, khususnya *database* dan jaringan internal pada Dial Musik, salah satu data penting yang harus diamankan yaitu *database pemrograman* stok. Karena pernah terjadi komputer *server database pemrograman* stok terkena serangan virus *ransomware* yang dimasukan oleh orang lain dari luar, sehingga membuat

komputer *server* tidak bisa di akses dan semua *file* berubah *ekstensinya* menjadi *dotmap*.

Dengan itu untuk mencegah ancaman jaringan dari luar digunakan keamanan jaringan dengan teknik *demilitarized zone* (DMZ). Dengan menggunakan DMZ ini maka akan terbentuk zona demiliterasi pada komputer *server* sehingga akses dari luar tidak bisa langsung memasuki komputer *server*, akan tetapi harus melewati zona penyangga. Hal ini membuat komputer *server* menjadi lebih aman.

Dari latar belakang diatas peneliti mengambil judul “**Keamanan Jaringan Menggunakan Teknik DMZ dengan Sistem Operasi Linux Pada Dial Musik**” akan membahas bagaimana cara mengimplementasikan keamanan jaringan menggunakan teknik *demilitarized zone* (DMZ) menggunakan *firewall iptables* pada sistem operasi Linux agar dapat memberikan keamanan bagi pengguna jaringan internet di *showroom* Dial Musik.

## 1.2. Rumusan Masalah Penelitian

Berdasarkan latar belakang diatas, maka dapat dirumuskan masalah untuk dijadikan pembahasan dalam penulisan tugas akhir ini adalah “Bagaimana mengimplementasikan keamanan jaringan dengan teknik *demilitarized zone* (DMZ) dengan menggunakan *firewall iptables* di sistem operasi Linux pada *showroom* Dial Musik”.

## 1.3. Ruang Lingkup Penelitian

Batasan masalah yang terdapat dalam penelitian ini meliputi diantaranya:

1. Menerapkan teknik *Demilitarized zone* (DMZ) dengan menggunakan *firewall iptables* sistem operasi Linux Debian 11.
2. Menerapkan teknik keamanan jaringan *Demilitarized zone* (DMZ) untuk sebagai *web server*.

#### **1.4. Tujuan Penelitian**

Dalam penelitian pada Dial Musik ini terdapat tujuan yang ingin dicapai yaitu untuk menghasilkan keamanan jaringan dengan teknik *demilitarized zone* (DMZ) menggunakan *firewall iptables* dengan sistem operasi Linux, guna untuk mencegah dan mengatasi permasalahan keamanan jaringan yang terdapat pada *showroom* Dial Musik agar dapat memberikan keamanan bagi pengguna jaringan Dial Musik.

#### **1.5. Manfaat Penelitian**

##### **1.5.1. Manfaat Bagi Penulis**

Dapat menambah ilmu pengetahuan serta wawasan mengenai implementasi keamanan jaringan menggunakan teknik *demilitarized zone* (DMZ) dengan *firewall iptables*, serta mendapatkan pengalaman di dunia pekerjaan selama penelitian sehingga dapat mempersiapkan diri masuk ke dalam dunia pekerjaan.

##### **1.5.2. Manfaat Bagi Akademik**

Penelitian ini dapat menjadi referensi untuk membantu para peneliti dalam membuat sistem keamanan jaringan yang sama di masa yang akan datang.

### **1.5.3. Manfaat Bagi Dial Musik**

Dapat meningkatkan keamanan jaringan *server* dari akses luar secara langsung dan *server* lebih aman dari akses luar dengan mengimplementasikan menggunakan teknik *demilitarized zone* (DMZ) dengan *firewall iptables*.

## **1.6. Sistematika Penulisan**

Skripsi ini ditulis dalam enam bab dan masing-masing bab terbagi dalam sub-sub bab. Sistematika penulisan skripsi disusun sebagai berikut:

### **BAB I PENDAHULUAN**

Pada bab ini Penulis akan menguraikan tentang latar belakang, perumusan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

### **BAB II GAMBARAN UMUM PERUSAHAAN**

Pada bab ini menjelaskan tentang sejarah perusahaan, struktur organisasi dan wewenang.

### **BAB III TINJAUAN PUSTAKA**

Bab ini berisi teori berdasarkan penulis yang terdiri dari landasan teori, penelitian terdahulu dan kerangka penelitian.

#### **BAB IV METODE PENELITIAN**

Dalam bab ini membahas waktu dan lokasi penelitian, jenis data, teknik pengumpulan data dan jenis penelitian.

#### **BAB V HASIL DAN PEMBAHASAN**

Dalam bab ini membahas mengenai hasil dari penelitian yang telah dilakukan dan dibahas secara detail mekanisme penelitian tersebut dilakukan.

#### **BAB VI PENUTUP**

Menguraikan beberapa kesimpulan dari pembahasan masalah dari bab-bab sebelumnya serta memberikan saran yang bisa bermanfaat bagi perusahaan.



## **BAB II**

### **GAMBARAN UMUM PERUSAHAAN**

#### **2.1. Profil Perusahaan**

##### **2.1.1. Sejarah Perusahaan**

Dial Musik dan *Sport* didirikan pada tahun 1972 berlokasi di Jalan Letkol Iskandar No.636A, Ilir Timur II, Kota Palembang. Dial Musik & *Sport* adalah salah satu toko konvensional yang bergerak di bidang penjualan alat musik dan perlengkapan olahraga. Awal mula berdirinya toko ini hanya di karenakan sekitar daerah kemuning kota Palembang tidak ada yang menjual alat musik dan perlengkapan olahraga, maka dari itulah pemilik toko ingin mendirikan toko ini sebagai peluang usaha.

Dial Musik & *Sport* merupakan toko konvensional yang menyediakan peralatan bermusik modern namun juga menyediakan perlengkapan olahraga. Dial Musik & *Sport* mampu memanjakan para konsumennya dengan koleksi alat musik dan perlengkapan olahraga terbaik mereka dan juga memberikan keistimewaan dimana konsumen yang menjadi pelanggan mereka bisa langsung mencoba alat-alat musik di toko mereka, jika merasa cocok maka bisa dilanjutkan ke tahap pembelian.

### 2.1.2. Visi dan Misi

#### 1. Visi

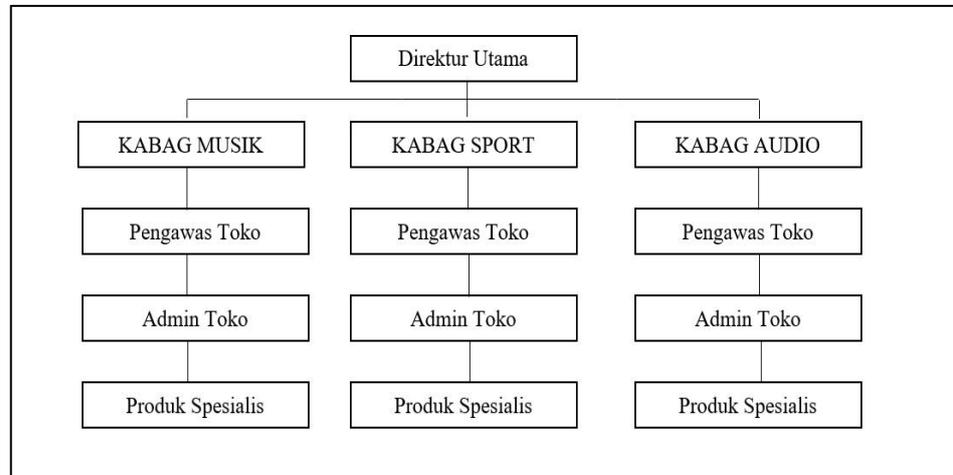
”Senantiasa memberikan spesifikasi alat serta kualitas suara yang terbaik guna memberikan kenyamanan dan keselarasan harmoni bagi para pemusik dan memberikan mutu kualitas alat olahraga terbaik”.

#### 2. Misi

- Menghasilkan keuntungan yang maksimal.
- Memberikan kepada masyarakat lapangan kerja.
- Memberikan mutu kualitas produk yang baik kepada konsumen.

### 2.1.3. Struktur Organisasi

Struktur organisasi adalah suatu bagan yang menunjukkan hubungan pada suatu organisasi atau perusahaan antara bagian yang satu dengan bagian yang lain dalam melakukan fungsi dan tugas-tugas yang dibebankan terhadap suatu posisi atau jabatan tertentu untuk menjamin kelancaran kerja. Setiap organisasi haruslah membentuk suatu struktur, dimana dengan adanya struktur organisasi ini akan tampak lebih jelas bila dituangkan dalam suatu bagan atau *skema* organisasi. Struktur organisasi pada Dial Musik & Sport dapat dilihat pada Gambar 2.1.



r: Dial Musik, 2023

**Gambar 2.1** Stuktur Organisasi Dial Musik dan *Sport*.

#### 2.1.4. Tugas dan Wewenang

Adapun tugas dan wewenang dari masing-masing yang ada pada struktur organisasi antara lain:

##### 1. **Direktur Utama**

- a. Menetapkan kebijakan sebagai pedoman unit kerja/kegiatan dalam melaksanakan tugasnya.
- b. Menyusun rencana jangka pendek dan panjang serta rencana anggaran tahunan perusahaan.
- c. Menetapkan prioritas, memonitor dan mengawasi pelaksanaan rencana kerja dan mengevaluasinya serta mengambil langkah penyelesaian apabila terjadi hambatan dan penyimpangan.
- d. Membina hubungan dengan relasi dan meningkatkan sumber daya manusia.

- e. Menegakan disiplin kerja dan memotivasi karyawan untuk meningkatkan produktivitas.

## **2. Kepala Bagian Toko (KABAG)**

- a. Mengelola dan memantau oprasional pelayanan sehari hari.
- b. Melayani keluhan pelanggan.
- c. Melakukan pengawasan terhadap oprasional pelayanan serta pemberian solusi yang terbaik.
- d. Mengawasi pelaksanaan data pelanggan.
- e. Mengontrol pekerjaan karyawan.

## **3. Pengawas Toko**

- a. Mengelola tim.
- b. Membuat keputusan yang mempengaruhi tim.
- c. Mengembangkan potensi karyawan baru.
- d. Mengevaluasi kinerja dan memberikan umpan balik.
- e. Melapor ke HR dan manajemen senior.
- f. Membantu menyelesaikan masalah dan perselisihan karyawan.
- g. Memastikan keselamatan kerja.

## **4. Admin Toko**

- a. Merapikan data.
- b. Membuat penyimpanan arsip.
- c. Melayani pelanggan.
- d. Melakukan input atau pemasukan data penjualan.

- e. Membuat laporan mengenai persediaan di toko secara rutin.

#### **5. Produk Spesialis**

- a. Memantau dan memperkirakan tren pemasaran.
- b. Mencari tahu efektivitas program dan strategi pemasaran.
- c. Merancang dan mengevaluasi metode pengumpulan data seperti survei, kuesioner, dan *polling*.
- d. Mengumpulkan data tentang konsumen, pesaing, dan kondisi pasar.

## BAB III

### TINJAUAN PUSTAKA

#### 3.1. Landasan Teori

##### 1. *Demilitarized Zone (DMZ)*

Menurut Saputro, dkk (2022:14) *De-Militarized Zone (DMZ)* merupakan mekanisme untuk melindungi sistem *internal* dari serangan *hacker* atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. Sehingga karena DMZ dapat diakses oleh pengguna yang tidak mempunyai hak, maka DMZ tidak mengandung rule. Secara esensial, DMZ memindahkan semua layanan suatu jaringan ke jaringan lain yang berbeda. DMZ terdiri dari semua *port* terbuka, yang dapat dilihat oleh pihak luar. Sehingga jika *hacker* menyerang dan melakukan *cracking* pada *server* yang mempunyai DMZ, maka *hacker* tersebut hanya dapat mengakses *host* yang berada pada DMZ, tidak pada jaringan *internal*.

##### 2. *Firewall*

Menurut Manik dan Lubis (2021:37) *Firewall* ialah sebuah perlengkapan/aplikasi di dalam jaringan yang dapat mengerjakan pemantauan kemudian lintas jaringan, menciptakan pemisah antara jaringan yang terpercaya dan tidak terpercaya. *Firewall* menampik semua kemudian lintas yang tidak terpercaya supaya jaringan menjadi aman dari serangan dan memperbolehkan lalu lintas yang terpercaya guna masuk ke

dalam jaringan. *Firewall* adalah garis pertahanan kesatu dalam mengayomi jaringan dan data-data yang terdapat di dalamnya.

### 3. *Iptables*

Menurut Suwanto, dkk (2019:99) adalah suatu kelompok arsitektur pemrosesan paket jaringan aturan ke dalam tabel berdasarkan fungsi (filter paket, jaringan terjemahan alamat, dan paket lainnya) yang masing-masing memiliki rantai (urutan) aturan pemrosesan. Aturan terdiri dari kecocokan (digunakan untuk menentukan apa yang akan dilakukan dengan pencocokan paket).

Dapat disimpulkan bahwa *iptables* merupakan suatu *firewall* yang ada pada Linux yang berfungsi untuk menganalisis dan menyaring paket data yang masuk kedalam *firewall*, dan dibagi menjadi tiga kategori aksi yaitu:

#### a. *Drop*

membiarkan paket tersebut seolah-olah tidak pernah diterima.

#### b. *Accept*

menerima paket tersebut untuk diproses lebih lanjut.

#### c. *Reject*

menolak dan memberitahukan pengirim bahwa paket data tidak bisa diterima.

Purdy menjelaskan bahwa *IPTabless* juga sebagai alat untuk menyaring paket-paket yang masuk, keluar dan sedang berlalu lintas di dalam *Firewall* melalui *server*. *IPTabless* mendedikasikan lima

"hookpoint" di dalam jalur pemrosesan paket kernel: *Prerouting*, *Input*, *Forward*, *Postrouting* dan *Output*. Setiap aturan merupakan peluang untuk mempengaruhi atau memantau aliran paket.

#### 4. **Keamanan Jaringan**

Menurut Purba dan Efendi (2020:146) keamanan jaringan adalah konsep untuk mencegah pengguna yang tidak sah masuk ke dalam sistem jaringan komputer. Sistem harus tetap dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian oleh pihak yang tidak memiliki hak. Langkah-langkah pencegahan dapat membantu administrator untuk menghentikan pengguna yang tidak sah untuk mengakses sistem jaringan komputer.

Keamanan jaringan komputer berfungsi untuk mengantisipasi resiko-resiko yang akan terjadi pada jaringan komputer yang dapat mengganggu aktivitas yang sedang terjadi pada sistem jaringan komputer. Ada tiga hal dalam konsep keamanan jaringan, yaitu tingkat bahaya, ancaman

#### 5. **Linux**

Menurut Dwiyatno, dkk (2020:170) Linux adalah nama yang diberikan kepada sistem operasi komputer bertipe *Unix*. Linux merupakan salah satu contoh hasil pengembangan perangkat lunak bebas dan sumber terbuka utama. Seperti perangkat lunak bebas dan sumber terbuka lainnya pada umumnya, kode sumber Linux dapat dimodifikasi, digunakan dan didistribusikan kembali secara bebas oleh

siapa saja. Nama "Linux" berasal dari nama pembuatnya, yang diperkenalkan tahun 1991 oleh Linus Torvalds. Sistemnya, Peralatan sistem dan pustakanya umumnya berasal dari sistem operasi GNU, yang diumumkan tahun 1983 oleh Richard Stallman. Kontribusi GNU adalah dasar dari munculnya nama alternatif GNU/Linux.

Linux adalah sistem operasi berbasis GNU/Linux yang bersifat *Open Source* dan memiliki banyak varian seperti Debian, *Slackware*, *Open Suse*, *Archlinux*, *Redhat* dan sebagainya. Walaupun sangat banyak varian GNU/Linux hanya menyediakan aplikasi yang sudah ditentukan yang mungkin kurang bermanfaat oleh pengguna sehingga hal ini mengakibatkan banyak pengguna yang melakukan *remastering* untuk memenuhi kebutuhannya. *Remastering* adalah proses membuat sistem operasi baru dengan mengurangi atau menambahkan fitur-fiturnya dari distro GNU/Linux yang telah ada.

## 6. *Local Area Network (LAN)*

Menurut Manik dan Lubis (2021:36) *Local lokasi network* adalah jaringan lokal yang dibikin pada lokasi terbatas. Misalkan dalam satu gedung atau satu ruangan. Kadangkala jaringan lokal disebut pun jaringan *individu* atau *private*. LAN dapat di pakai pada skala kecil yang memakai sumber secara bersamaan, seperti pemakaian printer bersama, memakai media penyimpanan secara bersamaan, dan sebagainya.

## 7. *Metropolitan Area Network (MAN)*

Menurut Manik dan Lubis (2021:36) *Metropolitan* lokasi *network* memakai metode yang sama dengan LAN namun wilayah lebih luas daerah cakupan. MAN dapat satu RW kantor yang berada dalam satu kompleks yang sama, satu/beberapa desa, satu/beberapa kota. Dapat disebutkan MAN pengembangan dari LAN.

### 8. *Wide Area Network* (WAN)

Menurut Manik dan Lubis (2021:36) *Wide* lokasi *network* memakai area yang lebih luas dari pada MAN. memakai MAN mencakup satu kawasan, satu Negara, satu pulau, bahkan satu dunia, cara yang dipakai WAN sama laksana yang di pakai LAN dan MAN. Umumnya WAN terhubung dengan jaringan telepon digital. Namun media transmisi beda pun bisa digunakan.

### 3.2. Penelitian Terdahulu

Berikut adalah beberapa jurnal yang berkaitan dengan penelitian dan digunakan sebagai referensi oleh penulis dalam mengkaji penelitian yang dilakukan. Data lengkap mengenai penelitian terdahulu dapat dilihat pada Tabel 3.1.

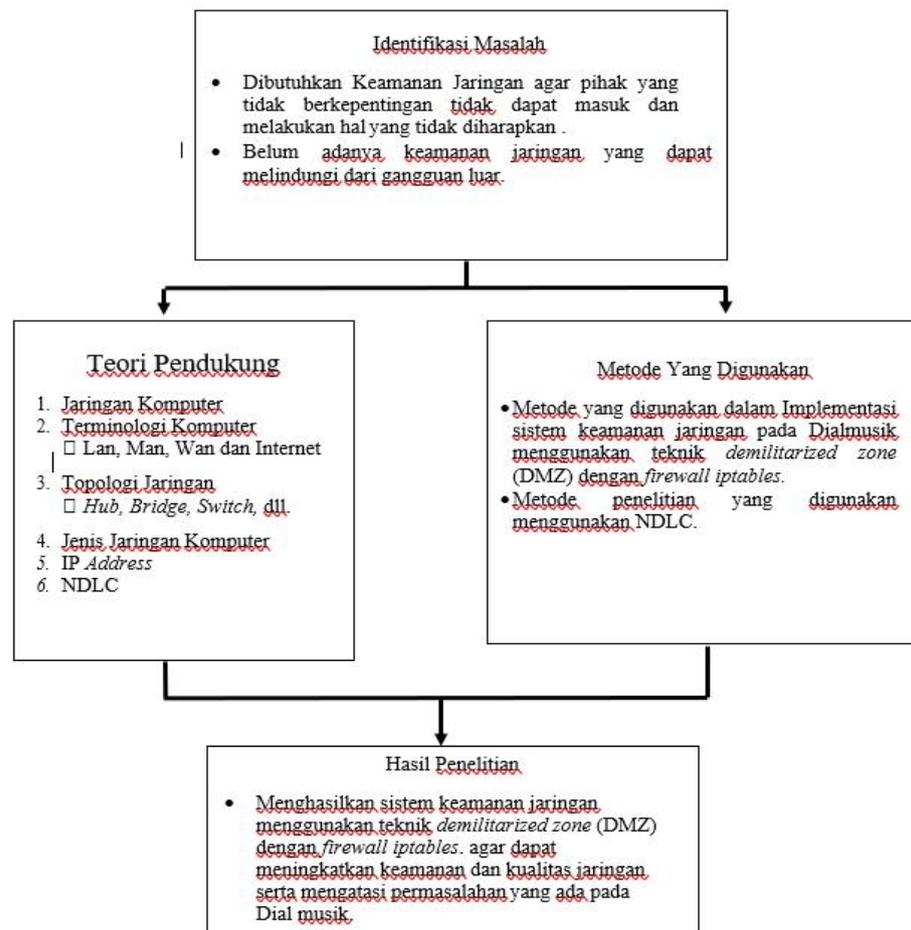
**Tabel 3. 1 Penelitian Terdahulu**

Judul	Nama Penulis	Hasil
Perancangan Sistem Keamanan Jaringan Untuk Mengurangi Kejahatan <i>Cyber</i>	Eka Suteja, Erna Kumlasari N, Suwanto Raharjo, (2021).	Setelah di terapkannya menggunakan teknik <i>Demilitarized Zone</i> (DMZ) Dan <i>firewall</i>

Menggunakan Teknik <i>Demilitarized zone</i> (DMZ) dan <i>Firewall Rules</i> .		<i>rules</i> berkurangnya penyerangan dari luar ke dalam <i>server</i> internal yang dimiliki.
Sistem Keamanan Jaringan <i>Local Area Network</i> Menggunakan Teknik <i>De-Militarized Zone</i>	Ino Nugraha, R. Hengki Rahmanto, (2017).	kesimpulannya ialah teknik keamanan jaringan DMZ pada layanan <i>server</i> jaringan LAN dapat melakukan filter terhadap serangan DOS.
Metode <i>Demilitarized Zone</i> dan <i>Port knocking</i> Untuk Keamanan Jaringan Komputer	Andik Saputro, Nanang Saputro, Hendro Wijayanto, (2020).	Teknik keamanan jaringan DMZ dan <i>Port Knocking</i> dapat diimplementasikan pada jaringan lokal maupun interlokal dimana jika suatu penyerang ingin mengexploit atau menyerang <i>server</i> utama maka yang pertama diserang

		adalah <i>server firewall</i> ( <i>router</i> ).
--	--	--

Penelitian terdahulu menjadi acuan dalam melakukan penelitian, sehingga memperkaya teori yang digunakan dalam mengkaji penelitian yang dilakukan. Dari penelitian terdahulu, peneliti akan membuat keamanan jaringan teknik *demilitarized zone* (DMZ) dengan *firewall iptables* agar akses dari luar sulit untuk masuk ke dalam jaringan pada Dial Musik.



### 3.3. Kerangka Pemikiran

Kerangka penelitian pada Keamanan Jaringan Menggunakan Teknik DMZ

Dengan Sistem Operasi Linux Pada Dial Musik, dapat dilihat pada Gambar 3.2.

**Gambar 3.1 Kerangka Pemikiran.**

## BAB IV

### METODE PENELITIAN

#### 4.1. Lokasi dan Waktu Penelitian

##### 1. Lokasi

Penelitian ini dilakukan di Dial Musik yang beralamat di Jl. Letkol Iskandar No.636A, 18 Ilir, Kecamatan Ilir Timur 1, Kota Palembang, Sumatera Selatan 30125.

##### 2. Waktu Penelitian

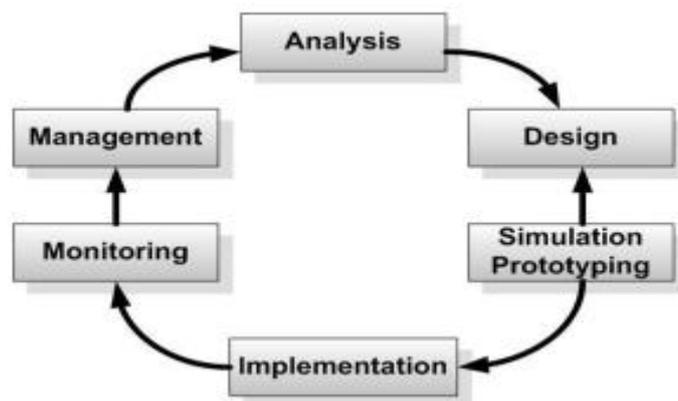
Penelitian ini dilakukan pada bulan Maret 2023 sampai dengan Juli 2023. Adapun jadwal penelitian dapat dilihat pada Tabel 4.1.

**Tabel 4. 1 Waktu Penelitian**

No	Kegiatan	Tahun 2023																			
		Maret				April				Mei				Juni				Juli			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Analisis	■	■	■																	
2	Perancangan				■	■	■	■	■	■											
3	Implementasi										■	■	■	■	■						
4	Pengujian																■	■	■	■	



perancangan jaringan komputer. Model ini mendefinisikan siklus proses pembangunan atau pengembangan sistem jaringan komputer yang dapat dilihat pada Gambar 4.1.



**Gambar 4.1** *Network Development Life Cycle (NDLC).*

1. *Analysis*

*Analysis* Tahap awal ini dilakukan analisis kebutuhan, analisis permasalahan yang muncul, analisis keinginan *user*, dan analisis Topologi/jaringan yang sudah ada.

2. *Design*

*Design* dari data-data yang didapatkan sebelumnya, tahap *design* ini akan membuat gambar *design topology* jaringan interkoneksi yang akan dibangun, diharapkan dengan gambar ini akan memberikan gambaran seutuhnya dari kebutuhan yang ada.

3. *Simulation/Prototyping*

*Simulation* Tahap membuat dalam bentuk simulasi dengan bantuan *tools* khusus di bidang *network* seperti paket *tracer*, hal ini dimaksudkan untuk melihat kinerja awal dari *network* yang akan

dibangun dan sebagai bahan presentasi dan *sharing* dengan *team work* lainnya.

#### 4. *Implementation*

*Implementasi* merupakan tahapan yang sangat menentukan dari berhasil atau gagalnya *project* yang akan dibangun dan ditahap inilah *teamwork* akan diuji di lapangan untuk menyelesaikan masalah teknis dan non teknis.

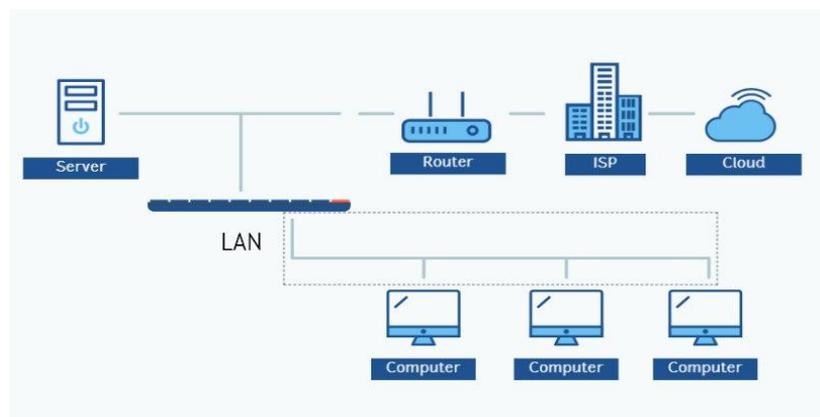
## BAB V

### HASIL DAN PEMBAHASAN

#### 5.1. Analisis

Jaringan tanpa keamanan *demilitarized zone* (DMZ) akan membuat celah keamanan komputer server semakin bertambah, dikarenakan tidak adanya zona penyangga untuk menyangga komputer *server* dari akses luar, Sehingga akses dari luar dapat dengan mudah masuk ke komputer *server*.

Sangat berbahaya jika komputer *server* langsung terhubung dengan internet tanpa ada yang melindungi. Komputer *server* akan menjadi rentan terhadap serangan serangan dari internet. Untuk menindaklanjuti hal tersebut dapat diterapkan keamanan *demilitarized zone* (DMZ) untuk melindungi komputer *server* dari akses luar. Dapat dilihat topologi jaringan tanpa keamanan jaringan menggunakan *demilitarized zone* (DMZ) pada Gambar 5.1.



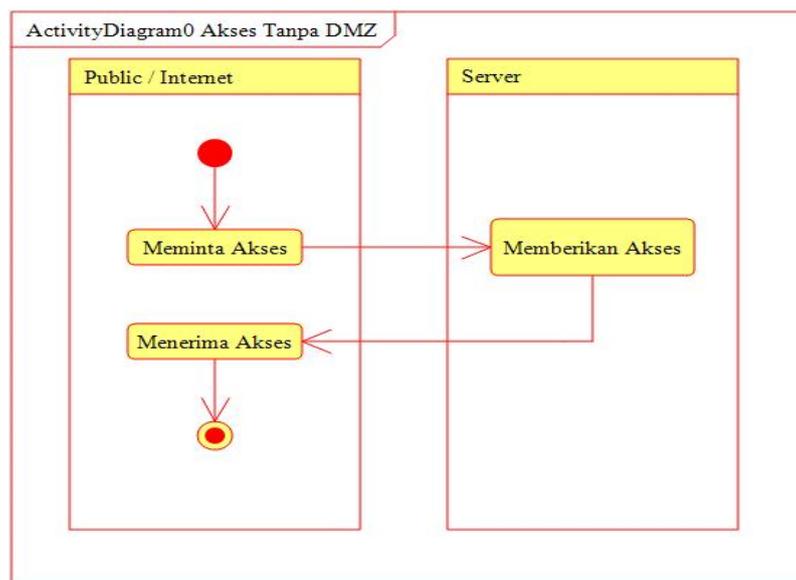
**Gambar 5.1 Topologi Jaringan Tanpa Keamanan *Demilitarized Zone* (DMZ).**

Ada beberapa permasalahan bila tidak menggunakan keamanan jaringan *demilitarized zone* (DMZ) diantaranya:

1. Komputer *server* dapat dengan mudah diserang langsung dari internet, dikarenakan tidak ada yang melindungi komputer *server* bila komputer *server* langsung terhubung ke internet.
2. Penggunaan IP publik akan bertambah, bila dalam suatu jaringan memiliki banyak *server* yang terhubung ke internet. Oleh karena itu untuk mengatasi permasalahan di atas perlu menggunakan teknik keamanan *demilitarized zone* (DMZ).

#### 5.1.1. *Activity Diagram Tanpa Keamanan Demilitarized Zone (DMZ)*

Berikut ini adalah *activity diagram* pada sebuah jaringan jika tidak menggunakan keamanan *demilitarized zone* (DMZ) dapat dilihat pada Gambar 5.2.

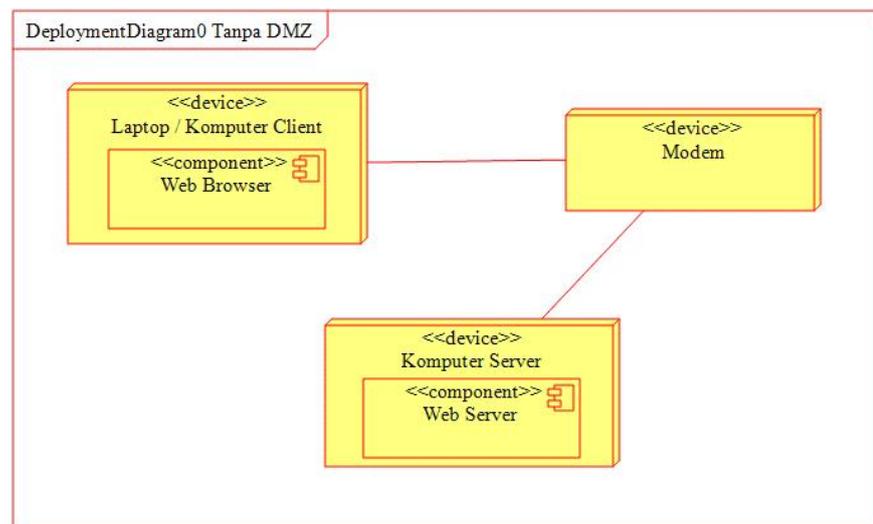


**Gambar 5.2** *Activity Diagram Tanpa DMZ.*

Pada gambar 5.2 *activity diagram* di atas dapat dilihat bahwa akses dari luar /internet atau bisa kita sebut dengan *client*, mereka dapat langsung mengakses *server*. Hal ini membuat *server* menjadi lebih rentan terhadap serangan, karena tidak ada yang melindungi.

### 5.1.2. *Deployment Diagram Tanpa Keamanan Demilitarized Zone (DMZ)*

Berikut ini adalah gambar tentang *device* apa saja yang ada dalam sebuah jaringan tanpa menggunakan keamanan *demilitarized zone* (DMZ). Digambarkan dengan *deployment diagram* dapat dilihat pada Gambar 5.3.



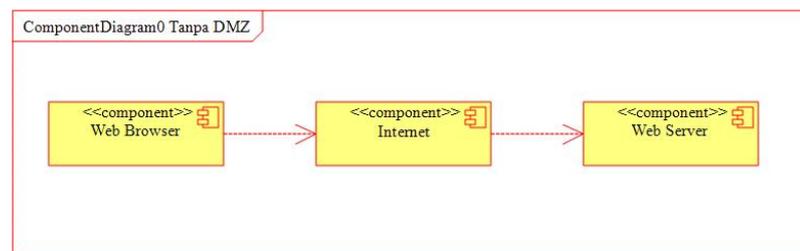
**Gambar 5.3 *Deployment Diagram Tanpa DMZ.***

*Deployment diagram* di atas adalah jaringan tanpa menggunakan keamanan *demilitarized zone* (DMZ). Terdapat tiga *device* yang berhubungan, laptop/komputer sebagai *Client*, modem sebagai media penghubung (internet) dari *client* ke *server* dan komputer *server* sebagai penyedia layanan. Pada Gambar 5.3 dapat dilihat bahwa

komputer *server* tidak dilindungi oleh apapun, dan itu membuat keamanan komputer *server* menjadi rentan terhadap serangan dari internet.

### 5.1.3. *Component Diagram Tanpa DMZ*

Berikut ini adalah beberapa komponen yang ada pada sebuah jaringan tanpa keamanan *demilitarized zone* (DMZ), komponen – komponen tersebut digambarkan dengan *component diagram* pada Gambar 5.4.



**Gambar 5.4 *Component Diagram Tanpa DMZ.***

*Diagram* di atas terdapat tiga buah komponen yang berhubungan pada sebuah jaringan tanpa keamanan *demilitarized zone* (DMZ). Terdapat *web browser* yang digunakan *client* untuk akses ke *server*, internet sebagai media penghubung antara *client* dan *server*, dan *web server* sebagai penyedia layanan. *Web browser* berhubungan langsung dengan *web server* dengan media internet.

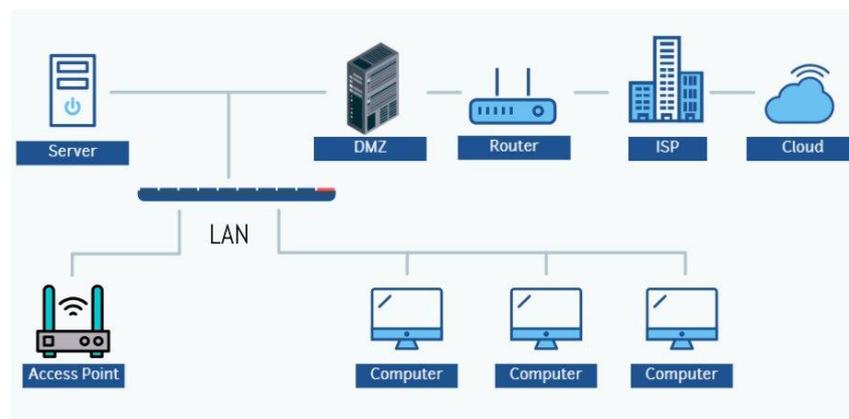
### 5.1.4. *Analisa Kebutuhan Hardware dan Software*

Untuk dapat membangun jaringan dengan keamanan *demilitarized zone* (DMZ) dibutuhkan beberapa perangkat keras/*hardware* di antaranya:

- Komputer dengan *processor* 2 GHz dan *harddisk* 512 GB
- *Ethernet Card* (Dua Buah)
- *Hub / Switch*
- Kabel jaringan
- Sistem operasi Linux Debian 11.

## 5.2. Desain

Teknik keamanan *demilitarized zone* (DMZ) dapat membuat zona penyangga untuk melindungi *server* dari akses luar. Desain topologi jaringan beserta *IP address* dengan menggunakan keamanan *demilitarized zone* (DMZ) dapat dilihat pada Gambar 5.5.



**Gambar 5.5 Topologi dengan DMZ.**

Topologi jaringan di atas adalah topologi jaringan dengan keamanan *demilitarized zone* (DMZ). Pada *desain* topologi jaringan di atas dapat dilihat *server* tidak terhubung secara langsung dengan internet. Terdapat *firewall* yang melindungi *server* dari akses internet secara langsung dengan *demilitarized zone* (DMZ).

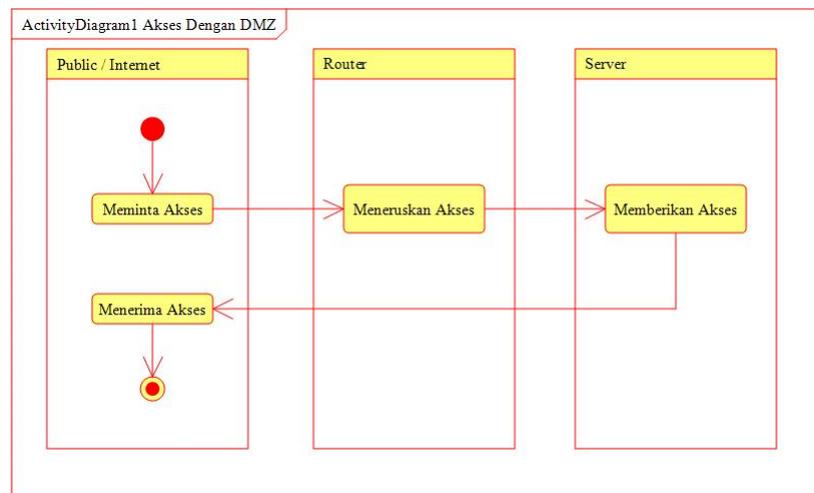
Seluruh komputer *server* tidak harus menggunakan IP publik untuk

terhubung dengan internet, cukup dengan satu buah IP publik, maka seluruh *server* dapat terhubung dengan internet. Keamanan yang didapatkan juga cukup untuk melindungi *server* dari serangan serangan internet secara langsung.

*IP address* untuk internet yaitu 10.10.10.1 akan digunakan oleh komputer *router*. Seluruh *server* akan ditempatkan pada jaringan 192.168.1.0/24. Dalam penelitian ini *web server* menggunakan *IP address* 192.168.1.1.

### 5.2.1. Desain Activity Diagram

Berikut ini adalah *desain* untuk alur proses akses jaringan dengan menggunakan keamanan *demilitarized zone* (DMZ) yang akan digambarkan dengan *activity diagram* dapat dilihat pada Gambar 5.6.



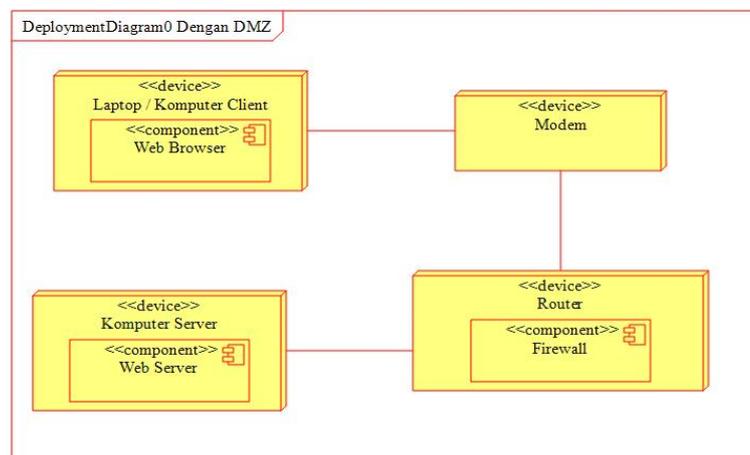
**Gambar 5.6 Activity Diagram Dengan DMZ.**

Gambar 5.6 menjelaskan bahwa pihak luar/internet meminta akses, *router* meneruskan akses ke *server*, lalu *server* memberikan akses kepada pihak luar/internet. Apabila pihak luar/internet ingin mengakses *server*, maka tidak dapat mengakses *server* secara

langsung, melainkan harus melalui *router* yang nantinya akan diteruskan ke *server*.

### 5.2.2. Desain Deployment Diagram

Beberapa perangkat atau *device* yang terdapat pada jaringan yang menggunakan keamanan *demilitarized zone* (DMZ), akan digambarkan dengan *deployment diagram* pada Gambar 5.7.

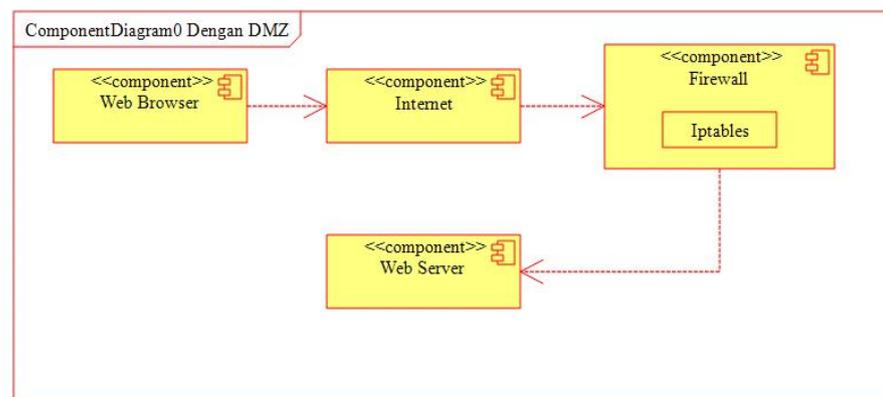


**Gambar 5.7 Deployment Diagram Dengan DMZ.**

Pada *diagram* di atas terdapat empat perangkat yaitu komputer *client*, modem, *router* dan komputer *server*. Modem digunakan sebagai media penghubung/internet yang menghubungkan antara komputer *client* dan *router*. *Router* pengatur paket data yang ingin mengakses ke *server* dan melindungi komputer *server* dari pihak luar/internet.

### 5.2.3. Desain Component Diagram

Beberapa komponen-komponen yang ada pada jaringan dengan keamanan *demilitarized zone* (DMZ), akan digambar dengan *component diagram* pada Gambar 5.8.



**Gambar 5.8 Component Diagram Dengan DMZ.**

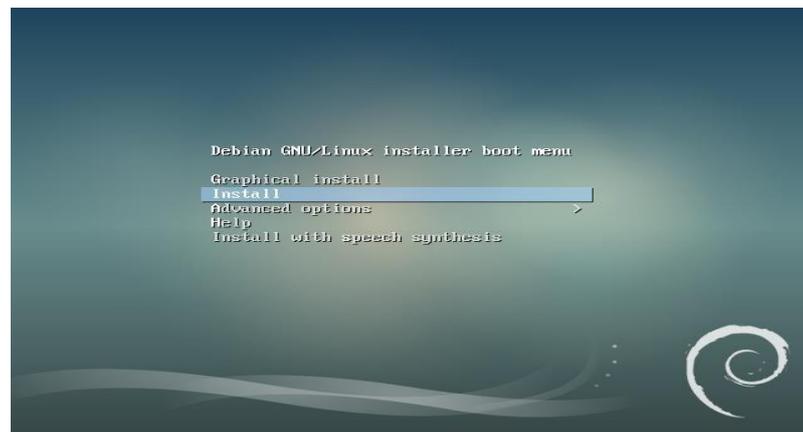
Terdapat empat buah komponen yang ada pada jaringan dengan keamanan *demilitarized zone* (DMZ). *Web browser* adalah komponen yang ingin mengakses *web server*. *Internet* adalah penghubung antara *web browser* dengan *web server*. *Firewall* untuk melindungi *web server*.

### 5.3. Implementasi

Setelah melakukan beberapa tahap sebelumnya, selanjutnya masuk ke tahap *implementasi*, dimana nantinya akan mengimplementasikan teknik keamanan *demilitarized zone* (DMZ) ke dalam sebuah jaringan komputer.

### 5.3.1. Instalasi Sistem Operasi Linux Debian 11

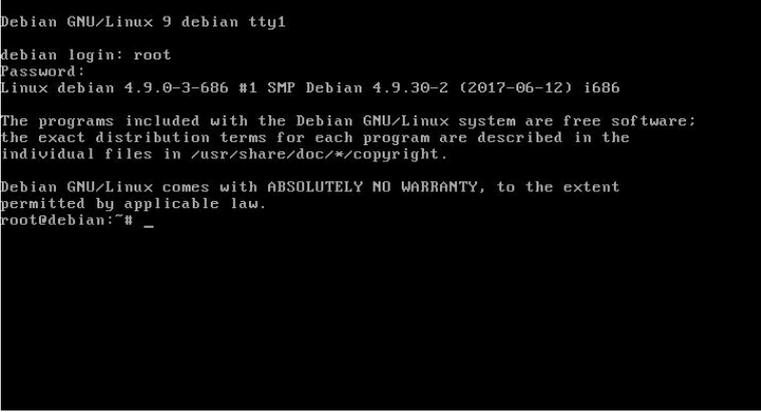
*Implementasi* awal yang dilakukan untuk membangun jaringan dengan keamanan *demilitarized zone* (DMZ) yaitu dengan menginstall sistem operasi Linux Debian 11 ke dalam komputer *router* yang nantinya akan dikonfigurasi untuk membangun jaringan dengan keamanan *demilitarized zone* (DMZ) dapat dilihat pada Gambar 5.9.



**Gambar 5.9 Instalasi Sistem Operasi Linux Debian 11.**

*Instalasi* sistem operasi Linux Debian 11 ini bisa menggunakan *Command Line Interface* (CLI) maupun *Graphical Install*. Perbedaannya ada pada tampilan saat *instalasi*, bila menggunakan *Command Line Interface* (CLI) akan minim sekali grafik yang ditampilkan, namun bila ingin mudah dalam menginstall, gunakan *Graphical Install*.

Setelah selesai *instalasi*, masuk kedalam sistem Debian 11 dengan *user root*. *Root* adalah *superuser*, *user* dengan tingkatan yang paling tinggi dan bisa melakukan apapun terhadap sistem operasi Linux.



```
Debian GNU/Linux 9 debian tty1
debian login: root
Password:
Linux debian 4.9.0-3-686 #1 SMP Debian 4.9.30-2 (2017-06-12) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@debian:~# _
```

**Gambar 5.10** Tampilan *Command Line Interface (CLI) Linux Debian 11*.

Gambar di atas merupakan *Command Line Interface (CLI)* dari Linux Debian 11, tidak ada *grafis* untuk konfigurasi Linux Debian 11 ini. Konfigurasi seluruhnya menggunakan *command*. *Command Line Interface (CLI)* merupakan tempat kita untuk mengoperasikan *linux debian* dengan mengetikkan *command* atau perintah yang nantinya akan dieksekusi oleh sistem operasi Linux Debian.

### 5.3.2. Konfigurasi *IP Address*

Setelah dilakukan *instalasi system* operasi Linux Debian. Konfigurasi pertama yang dilakukan adalah konfigurasi *IP Address*. Konfigurasi *IP Address* dilakukan dengan menggunakan *Command Line Interface (CLI)*. Cara konfigurasinya dengan mengedit *file*

konfigurasi untuk jaringan menggunakan *nano* sebagai *file editor*.

Konfigurasi *IP address* bagian satu dapat dilihat pada Gambar 5.11.

# *nano /etc/network/interfaces*

```

GNU nano 2.7.4      File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface

# Interface Local
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    network 192.168.1.0

# Interface Public
auto enp0s8

```

**Gambar 5.11 Konfigurasi IP Address (Bagian I).**

Konfigurasi dapat disesuaikan dengan masing masing kondisi pada jaringan. Namun kali ini konfigurasi sesuai dengan tahap desain yang telah kita lakukan pada tahap sebelumnya. Terdapat tiga buah *network card* atau bisa disebut dengan *interface*. Pertama ada *lo* sebagai *interface loopback*, *enp0s3* sebagai *interface* lokal yang menghubungkan komputer *router* dengan komputer *server* dan *enp0s8* sebagai *interface* publik yang terhubung ke internet. Ketiganya adalah *interface* yang digunakan dalam jaringan dengan keamanan *demilitarized zone* (DMZ). Konfigurasi *IP address* bagian dua dapat dilihat pada Gambar 5.12.

```

GNU nano 2.7.4      File: /etc/network/interfaces
# Interface Local
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    network 192.168.1.0

# Interface Public
auto enp0s8
iface enp0s8 inet static
    address 10.10.10.1
    netmask 255.0.0.0
    network 10.0.0.0

^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^M Replace   ^U Uncut Text ^I To Spell   ^_ Go To Line

```

**Gambar 5.12 Konfigurasi IP Address (Bagian II).**

Terdapat beberapa istilah – istilah dalam konfigurasi tersebut, antara lain:

1. *Auto* <interface> adalah konfigurasi yang digunakan agar *interface* otomatis dihidupkan pada saat komputer dihidupkan.
2. *Iface* <interface> *inet static* adalah konfigurasi yang digunakan untuk membuat *interface* menjadi *mode statis* dan mengisi *ip address* secara manual.
3. *Address* <ip\_address> adalah konfigurasi yang digunakan untuk menetapkan *ip address*.
4. *Subnet* <subnet mask> adalah konfigurasi yang digunakan untuk menetapkan *subnet mask* pada jaringan.
5. *Network* <network> adalah konfigurasi yang digunakan untuk menetapkan identitas jaringan atau *network*.

Beberapa konfigurasi dapat berubah dan dapat disesuaikan dengan kondisi jaringan. Setelah selesai konfigurasi tekan “Ctrl + X” dan “Y” untuk *save* konfigurasi dan keluar dari *file editor*.

*Restart* layanan jaringan di sistem Linux untuk mengaktifkan konfigurasi yang telah kita lakukan. Hal ini terus dilakukan setelah kita selesai konfigurasi, agar sistem menjalankan apa yang telah dikonfigurasi tadi. Konfigurasi *IP address* bagian tiga dapat dilihat pada Gambar 5.13.

```
# Interface Local
auto enp0s3
iface enp0s3 inet static
    address 192.168.1.100
    netmask 255.255.255.0
    network 192.168.1.0

# Interface Public
auto enp0s8
iface enp0s8 inet static
    address 10.10.10.1
    netmask 255.0.0.0
    network 10.0.0.0

root@debian:~# /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
root@debian:~# _
```

**# *etc/init.d/networking restart***

### **Gambar 5.13 Konfigurasi IP Address Bagian (III).**

Setelah muncul [ok] berarti layanan jaringan tidak terdapat *error* atau kesalahan dan sudah berhasil dijalankan. Hasil konfigurasi dapat diperiksa apakah sudah sesuai atau belum dapat dilihat pada Gambar 5.14.

```

root@debian:~# /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
root@debian:~# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe52:8854 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:52:88:54 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 1506 (1.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.1 netmask 255.0.0.0 broadcast 10.255.255.255
    inet6 fe80::a00:27ff:febd:1236 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bd:12:36 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 648 (648.0 B)

```

**# ifconfig**

### Gambar 5.14 Konfigurasi IP Address (Bagian IV)

Bila muncul *enp0s3*, *enp0s8* atau *interface* yang telah dikonfigurasi tadi beserta *ip address* telah muncul, berarti *interface* kita sudah menyala dan sudah tersambung ke jaringan. Tahap konfigurasi *ip address* selesai sampai disini.

#### 5.3.3. Konfigurasi Packet Forwarding

Setelah dilakukannya konfigurasi *IP Address* dilanjutkan dengan konfigurasi *Packet Forwarding* yang digunakan untuk *memforward* paket yang keluar dan masuk kedalam jaringan menuju *host* yang dituju. Konfigurasi ini juga membuat komputer dapat digunakan sebagai *router* dan dapat mengatur lalu lintas jaringan yang keluar masuk, dapat dilihat pada Gambar 5.15.

### # nano/etc/sysctl.conf

```

GNU nano 2.7.4      File: /etc/sysctl.conf      Modified
#####3
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
#
^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit      ^R Read File  ^_ Replace   ^U Uncut Text^T To Spell   ^_ Go To Line

```

**Gambar 5.15 Konfigurasi *Packet Forwarding* (Bagian I).**

*sysctl.conf* adalah *file* konfigurasi untuk mengontrol sistem dalam sistem operasi Linux Debian 11 itu sendiri. Hilangkan tanda pagar pada “*net.ipv4.ip forward=1*” untuk mengaktifkan *packet forwarding*. Angka “1” merupakan *yes / hidup / on*, sebaliknya angka “0” merupakan *mati / off*. *Save file* konfigurasi lalu keluar dari *file editor*. Untuk memeriksa apakah sistem telah menghidupkan *packet forwarding* dapat dilakukan pada Gambar 5.16.

```
root@debian:~# sysctl -p
net.ipv4.ip_forward = 1
root@debian:~# _
```

```
# sysctl -p
```

**Gambar 5.16 Konfigurasi *Packet Forwarding* (Bagian II).**

“*net.ipv4.ip\_forward = 1*” menandakan bahwa *Packet forwarding* telah diaktifkan dan komputer ini telah bisa difungsikan sebagai *router*. Konfigurasi untuk *packet forwarding* telah selesai sampai disini.

#### 5.3.4. Konfigurasi *Demilitarized Zone* (DMZ)

Konfigurasi dilanjutkan dengan konfigurasi *iptables* untuk mengaktifkan *demilitarized zone* (DMZ). *demilitarized zone* (DMZ) dapat dibangun oleh *firewall iptables* pada sistem operasi Linux secara manual. Langkah awal yaitu dengan membuat *file* konfigurasi di dalam folder konfigurasi jaringan, yaitu folder */etc/network/if-up.d/*. karena dalam folder tersebut *file* konfigurasi yang dibuat dapat berjalan otomatis setelah jaringan dihidupkan, dapat dilihat pada Gambar 5.17.

```
# touch /etc/network/if-up.d/dmz
```

```
# chmod +x /etc/network/if-up.d/dmz
```

```
root@debian:~# touch /etc/network/if-up.d/dmz
root@debian:~# chmod +x /etc/network/if-up.d/dmz
root@debian:~# _
```

### Gambar 5.17 Konfigurasi *Demilitarized Zone* (Bagian I)

*Touch* digunakan untuk membuat *file* baru, *chmod* digunakan untuk mengubah mode dari suatu *file* dan “+x” membuat *file* menjadi *executable* dan bisa di eksekusi. Setelah itu konfigurasi *file* *dmz* untuk membangun keamanan *demilitarized zone* (DMZ) dapat dilihat pada Gambar 5.18.

```

GNU nano 2.7.4      File: /etc/network/if-up.d/dmz      Modified
#?bin/sh_
# REFRESH KONFIGURASI
iptables -F
iptables -X

# DROP SELURUH KONEKSI YANG MASUK
iptables -P INPUT DROP

# IZINKAN AKSES PING DENGAN PANJANG DATA 86 BYTE, LIMIT 1/s, 1 AKSES
iptables -A INPUT -p icmp --icmp-type echo-request -m length --length 1:86
-m limit --limit 1/s --limit-burst 1 -j ACCEPT

# MENGINZINKAN AKSES FORWARD DAN KELUAR JARINGAN
iptables -A FORWARD -j ACCEPT
iptables -A OUTPUT -j ACCEPT
iptables -t nat -A POSTROUTING -j MASQUERADE

# MENGINZINKAN LOOPBACK
iptables -A INPUT -i lo -j ACCEPT

```

# nano /etc/network/if-up.d/dmz

### Gambar 5.18 Konfigurasi *Demilitarized Zone* (Bagian II).

*File* konfigurasi ini berisikan *rules* atau perintah *iptables* yang di konfigurasi untuk membangun keamanan *demilitarized zone* (DMZ). Ada beberapa tahap untuk konfigurasi *firewall iptables* ini.

Tahap pertama yaitu *refresh* konfigurasi untuk membersihkan konfigurasi yang dilakukan sebelumnya sebelum memulai konfigurasi baru untuk *iptables*. #*iptables -F* dan #*iptables -X* yaitu perintah untuk menghapus seluruh konfigurasi yang ada pada *iptables* sebelumnya tanpa tersisa. Ini harus dilakukan agar konfigurasi *iptables* tidak bertumpuk dengan konfigurasi-konfigurasi lama.

Tahap kedua yaitu memblokir seluruh paket dan koneksi yang akan masuk ke komputer *router* agar komputer *router* dapat memilih mana koneksi yang diizinkan masuk dan mana yang tidak diizinkan. Konfigurasi dengan perintah *iptables -P INPUT DROP*.

Tahap ketiga yaitu mengizinkan akses *ping* ke komputer *router* agar pihak luar dapat memastikan *server* hidup atau tidak. Konfigurasi sebagai berikut: *iptables -A INPUT -p icmp -icmp-type echo-request -m length --length 1:86 -m limit --limit 1/s --limit-burst 1 -j ACCEPT*.

*-A INPUT* mendefinisikan *rule* untuk koneksi yang masuk. *-p icmp* mendefinisikan *port*, dalam hal ini *ping* menggunakan *port icmp*. *-icmp-type echo-request* mendefinisikan *type* untuk *ping* dan membolehkan *client* melakukan *ping*. *--length 1:86* mendefinisikan besaran data yang akan diterima, dalam hal ini maksimal besaran data yang boleh masuk yaitu *86 byte*. *--limit 1/s* mendefinisikan batasan waktu melakukan *ping*, dalam hal ini akses *ping* hanya boleh 1 buah per detik. *--limit-burst 1* mendefinisikan satu *client* hanya boleh melakukan 1 koneksi *ping*.

Dalam tahap ini akses *ping* telah di tingkatkan keamanannya untuk menghindari serangan *denial of service* (DOS) dari luar. Akses *ping* hanya diizinkan masuk kedalam komputer *router* apabila ukuran data tidak lebih dari *86byte* dengan batasan satu kali *ping* per detik dan satu buah koneksi. Hal itu memungkinkan apabila besar data *ping* lebih

besar dari 86 *byte*, maka akses *ping* akan ditolak dan menunjukkan *request time out* dan juga apabila sebuah komputer melakukan lebih dari satu koneksi *ping*, maka akses juga akan ditolak dan menunjukkan *request time out*. Dan konfigurasi tahap keempat dapat dilihat pada Gambar 5.19.

```

GNU nano 2.7.4      File: /etc/network/if-up.d/dmz      Modified
-m limit --limit 1/s --limit-burst 1 -j ACCEPT

# MENGINZINKAN AKSES FORWARD DAN KELUAR JARINGAN
iptables -A FORWARD -j ACCEPT
iptables -A OUTPUT -j ACCEPT
iptables -t nat -A POSTROUTING -j MASQUERADE

# MENGINZINKAN LOOPBACK
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# DMZ WEB SERVER
iptables -A INPUT -p tcp -d 10.10.10.1 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.1.1 --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d 10.10.10.1 --dport 80
-j DNAT --to 192.168.1.1:80

exit 0

```

**Gambar 5.19 Konfigurasi *Demilitarized Zone* (Bagian III).**

Tahap keempat yaitu mengizinkan seluruh paket untuk di *forward* / diteruskan ke *IP address* lain (*iptables -A FORWARD -j ACCEPT*). Mengizinkan seluruh paket untuk keluar dari jaringan (*iptables -A OUTPUT -j ACCEPT*). Mengizinkan seluruh koneksi untuk di translasikan atau dialihkan ke *IP address* lain (*iptables -t nat -A POSTROUTING -j MASQUERADE*).

Tahap kelima yaitu keamanan *demilitarized zone* (DMZ) untuk *web server*. Pada tahap ini ada beberapa perintah yang dilakukan yaitu:

1. *Firewall iptables* akan membuka *port* mengizinkan akses pada komputer *router* melalui *ip address* 10.10.10.1

dan port 80. `iptables -A INPUT -p tcp -d 10.10.10.1 --dport 80 -jACCEPT.`

2. Firewall `iptables` mengizinkan *forward* paket atau paket diteruskan ke alamat *ip address server* yakni 192.168.1.1 pada port 80. `Iptables -A FORWARD -p tcp -d 192.168.1.1 -- dport 80-j ACCEPT.`
3. Firewall `iptables` akan mengarahkan koneksi yang masuk ke komputer *router* pada *ip address* 10.10.10.1 port 80 ke komputer *server* dengan *ip address* 192.168.1.1 port 80 untuk mengakses *web server*. `Iptables -t nat -A PREROUTING -p tcp -d 10.10.10.1 -- dport 80 -j DNAT --to 192.168.1.1:80.`

Konfigurasi *demilitarized zone* (DMZ) disini hanya sebatas untuk *web server*, namun dapat dikonfigurasi sesuai dengan kebutuhan jaringan. Setelah konfigurasi selesai, simpan *file* konfigurasi dan keluar lalu lakukan *restart* layanan jaringan, dapat dilihat pada Gambar 5.20.

```
root@debian:~# /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
root@debian:~# _
# /etc/init.d/networking restart
```

#### **Gambar 5.20 Konfigurasi *Demilitarized Zone* (Bagian IV).**

Setelah muncul [ok] berarti layanan jaringan telah berhasil dihidupkan kembali. Untuk memeriksa konfigurasi apakah sudah benar, lakukan perintah yang dapat dilihat pada Gambar 5.21.

```

root@debian:~# /etc/init.d/networking restart
[ ok ] Restarting networking (via systemctl): networking.service.
root@debian:~# iptables -nL
Chain INPUT (policy DROP)
target     prot opt source                destination           icmptype 0 length
ACCEPT    icmp -- 0.0.0.0/0             0.0.0.0/0
1:86 limit: avg 1/sec burst 1
ACCEPT    all  -- 0.0.0.0/0             0.0.0.0/0
ACCEPT    tcp  -- 0.0.0.0/0             10.10.10.1            tcp dpt:80

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination           tcp dpt:80
ACCEPT    all  -- 0.0.0.0/0             0.0.0.0/0
ACCEPT    tcp  -- 0.0.0.0/0             192.168.1.1

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    all  -- 0.0.0.0/0             0.0.0.0/0
ACCEPT    all  -- 0.0.0.0/0             0.0.0.0/0
root@debian:~#

```

**# iptables -nL**

### **Gambar 5.21 Konfigurasi *Demilitarized Zone* (Bagian V).**

Dapat dilihat pada Gambar 5.21, konfigurasi untuk *iptables* sudah ditetapkan dan *demilitarized zone* (DMZ) sudah berjalan. Terdapat beberapa *rule* dalam *chain input*, *forward* dan *output*. Di dalam *chain input* terdapat *rule* atau kebijakan untuk paket yang masuk ke dalam komputer *router*. *Chain forward* terdapat *rule* untuk *forwarding* / paket yang masuk ke dalam komputer *router* akan diteruskan ke alamat yang dituju. *Chain output* terdapat *rule* untuk paket yang keluar dari jaringan.

## **5.4. Monitoring**

Tahap *monitoring* yaitu untuk memantau, apakah konfigurasi jaringan yang dilakukan sudah berjalan sesuai dengan semestinya. *Monitoring* dapat dilakukan untuk memantau dan melihat paket yang keluar, paket yang di

teruskan, maupun paket yang masuk dalam sebuah jaringan. *Monitoring* dapat menggunakan beberapa aplikasi, salah satunya *network statistic (netstat)* yang sudah menjadi aplikasi bawaan sistem operasi *linux* dan juga menjadi aplikasi dasar *networking* yang wajib, sama seperti *ping*, *ifconfig*, *traceroute*. *network statistic (netstat)*. Untuk melakukan *monitoring* dapat dilakukan perintah pada Gambar 5.22.

```
Every 1.0s: netstat -ntua                debian: Fri Jul 7 02:50:20 2017
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6      0      0  :::80                  :::*                    LISTEN
udp       0      0  192.168.1.100:44517    192.168.1.1:53        ESTABLISHED
udp       0      0  0.0.0.0:68             0.0.0.0:*
```

# watch -n 1 "netstat -ntua"

**Gambar 5.22** *Monitoring* dengan *network statistic (netstat)*.

*network statistic (netstat)* dapat digunakan untuk *memonitoring* seluruh aktifitas jaringan pada komputer *router*. Aktifitas itu dapat berupa paket yang masuk, paket yang diteruskan maupun paket yang keluar. Untuk menghentikan

*monitoring* bisa menekan tombol "*CTRL + C*". *Iptables* juga bisa digunakan untuk *monitoring* jaringan suatu komputer, dapat dilakukan dengan perintah pada Gambar 5.23.

```

Every 1.0s: iptables -nL -v                                debian: Sun Jul 30 04:12:33 2017
Chain INPUT (policy DROP 4 packets, 1312 bytes)
pkts bytes target      prot opt in      out     source      destination
  33   312 ACCEPT      icmp -- *       *       0.0.0.0/0   0.0.0.0/0
      0     0 ACCEPT      all  -- lo     *       0.0.0.0/0   0.0.0.0/0
  824 9248 ACCEPT      tcp  -- *       *       0.0.0.0/0   10.10.10.1
      tcp dpt:80
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination
  824 9248 ACCEPT      all  -- *       *       0.0.0.0/0   0.0.0.0/0
  824 9248 ACCEPT      tcp  -- *       *       0.0.0.0/0   192.168.1.1
      tcp dpt:80
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination
  44  2948 ACCEPT      all  -- *       *       0.0.0.0/0   0.0.0.0/0
# watch -n 1 "iptables -nL -v

```

**Gambar 5.23 Monitoring dengan IPTables.**

Dengan *iptables* dapat melihat paket yang keluar, masuk maupun data yang di *forward* oleh *demilitarized zone* (DMZ). Untuk menghentikan *monitoring* tekan tombol “CTRL + C”.

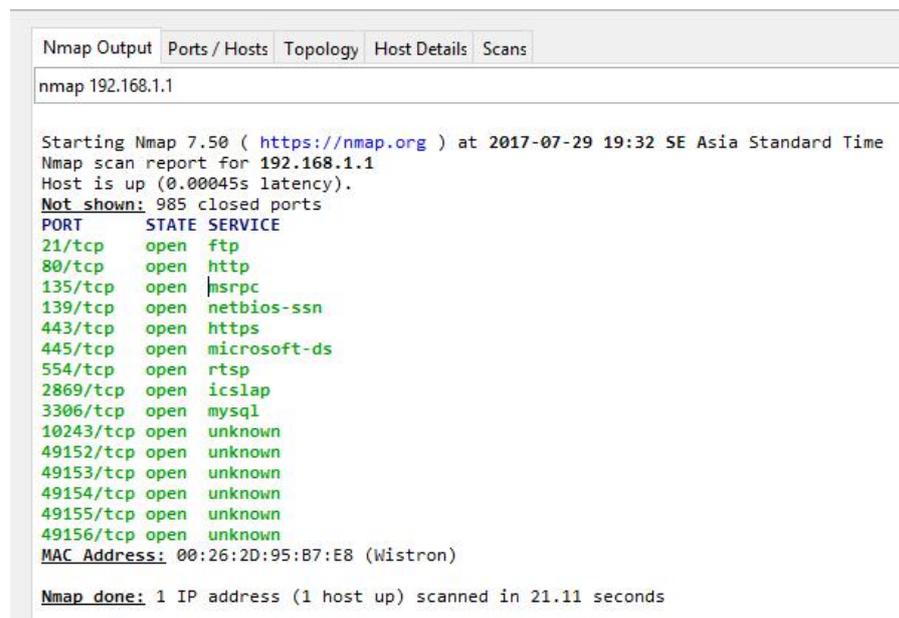
Tahap *monitorng* telah selesai sampai disini. Untuk melakukan *monitoring* yang lebih baik lagi, bisa dilakukan dengan *instalasi software* seperti *mrtg*, dll. Namun untuk tingkat dasar, bisa gunakan *netstat* dan *iptables*.

## 5.5. Management

Tahap *management* merupakan tahap akhir dari *network development life cycle* (NDLC). Tahap ini dimana dilakukannya *manajemen* terhadap jaringan yang telah dibangun. Dibutuhkan seorang *Administrator* yang dapat memajemen *server* dan jaringan. Manajemen sangat diperlukan agar jaringan yang telah dibangun dapat bertahan lama dan terus diperbaharui. Tahap manajemen dilakukan secara terus menerus agar jaringan dapat selalu di kontrol.

## 5.6. Pengujian

Berikut ini pengujian *scanning port* sebelum diterapkan teknik keamanan *demilitarized zone* (DMZ) ke sebuah *server website* dengan menggunakan



```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
-----
nmap 192.168.1.1

Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-29 19:32 SE Asia Standard Time
Nmap scan report for 192.168.1.1
Host is up (0.00045s latency).
Not shown: 985 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  iclslap
3306/tcp  open  mysql
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:26:2D:95:B7:E8 (Wistron)

Nmap done: 1 IP address (1 host up) scanned in 21.11 seconds

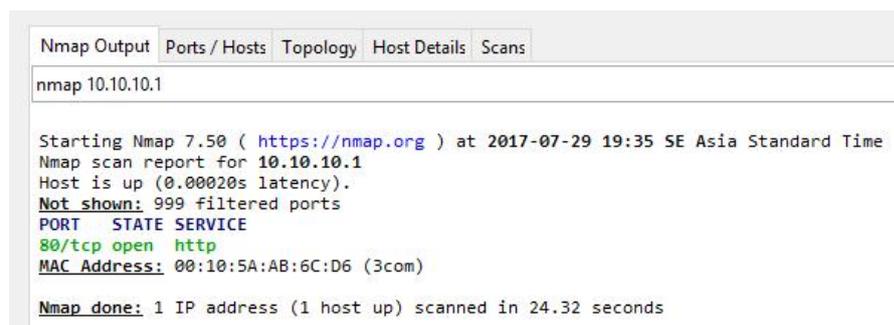
```

aplikasi *NMAP* dapat dilihat pada Gambar 5.24.

### Gambar 5.24 Hasil Pengujian Tanpa *Demilitarized Zone* (DMZ).

Hasil *scan* diatas menunjukkan banyak sekali *port* yang terbuka, hal itu menyebabkan banyaknya celah keamanan di dalam komputer *server* tersebut.

Bandingkan jika sudah diterapkan keamanan *demilitarized zone* (DMZ) dapat



```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
-----
nmap 10.10.10.1

Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-29 19:35 SE Asia Standard Time
Nmap scan report for 10.10.10.1
Host is up (0.00020s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:10:5A:AB:6C:D6 (3com)

Nmap done: 1 IP address (1 host up) scanned in 24.32 seconds

```

dilihat pada Gambar 5.25.

**Gambar 5.25 Hasil Pengujian *Demilitarized Zone (DMZ)*.**

Dengan menggunakan *demilitarized zone (DMZ) port* yang tadinya terbuka menjadi tertutup, hanya *port 80* yang tersedia untuk di akses secara publik. Dengan adanya keamanan *demilitarized zone (DMZ)* ini komputer *server* akan terlindungi dan menjadi lebih aman dari akses luar.

## BAB VI

### PENUTUP

#### 6.1. Kesimpulan

Berdasarkan penelitian pada Dial Musik setelah dibangunnya sistem keamanan jaringan, maka penulis menarik kesimpulan sebagai berikut:

1. Sistem operasi *linux debian 11* bisa dijadikan sebagai sistem operasi *router*. Terbukti dari hasil pengujian sistem operasi Linux Debian dapat diandalkan.
2. *Demilitarized Zone (DMZ)* menerapkan fungsi *Network Address Translation (NAT)* dan *Port Address Translation (PAT)* yang digunakan untuk *memforward* dan mengalihkan paket data ke *network* dan *port* lainnya. Terbukti berjalan dengan baik dan berhasil.

#### 6.2. Saran

Berdasarkan uraian dan kesimpulan yang telah dijelaskan dalam skripsi mengenai implementasi *demilitarized zone (DMZ)* penulis memberikan beberapa saran berikut:

1. Untuk meningkatkan keamanan, lakukan *update* aplikasi secara rutin dengan perintah *apt-get upgrade*.
2. Gunakanlah *ethernet card* yang berkualitas pada *router*, agar *router* dapat menangani paket yang keluar masuk secara cepat, kalau bisa gunakan *Gigabyte Ethernet Card*.

3. Selain itu gunakanlah *processor* pada komputer *router* yang berkecepatan tinggi, misalnya 3 GHz. Agar kecepatan proses untuk *routing* dapat dilakukan dengan cepat.
4. Selalu memantau *log* dari sistem untuk melihat kondisi sistem yang berjalan.

## DAFTAR PUSTAKA

- Agitya, N. A. P. (2022). **Perancangan Sistem Informasi Peminjaman Bus Sekolah Dinas Perhubungan Unit Pengelola Angkutan Sekolah DKI Jakarta Berbasis *Java***. *METHODIKA: Jurnal Teknik Informatika dan Sistem Informasi*, 8(2), 14-18.
- Anugrah, I., & Rahmanto, R. H. (2017). **Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone**. *PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic*, 5(2), 91-106.
- Aris, A., Perawati, P., & Komalasari, N. (2017). **Sistem Aplikasi HRD Berbasis *Web* untuk Penilaian Kinerja Staf pada Pengadilan Negeri Tangerang**. *SEMNASSTEKNOMEDIA ONLINE*, 5(1), 1-2.
- Dwiyatno, S., Rachmat, E., Sari, A. P., & Gustiawan, O. (2020). **Implementasi virtualisasi server berbasis docker container**. *PROSISKO: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, 7(2), 165-175.
- Hidayah, I., Ariefiantoro, T., Nugroho, D. W. P. S., & Suryawardana, E. (2021). **Analisis Strategi Bauran Pemasaran Dalam Meningkatkan Volume Penjualan (Studi Kasus Pada Pudanis Di Kaliwungu)**. *Solusi*, 19(1).
- Manik, B. M., & Lubis, I. (2021). **Perbandingan Kinerja Ipcop dengan Honeypot dalam Mengamankan Server Linux dari Serangan Hacker**. *Jurnal Ilmu Komputer dan Sistem Komputer Terapan (JIKSTRA)*, 3(1), 34-41.

- Mulyanto, Y., & Prakoso, S. B. (2020). **Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (Ndlc): Rancang Bangun Jaringan Komputer Menggunakan Sistem Manajemen Omada Controller Pada Inspektorat Kabupaten Sumbawadengan Metode Network Development Life Cycle (NDLC).** Jurnal Informatika Teknologi dan Sains, 2(4), 223-233
- Purba, W. W., & Efendi, R. (2020). **Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT.** AITI, 17(2), 143-158.
- Saputro, A., Saputro, D. T., & Remawat, D. (2022). **Implementasi Port Knocking Untuk Keamanan Jaringan Komputer Dengan Metode Demilitarized Zone.** Jurnal Informa: Jurnal Penelitian dan Pengabdian Masyarakat, 8(2), 13-18.
- Saputro, A., Saputro, N., & Wijayanto, H. (2020). **Metode Demilitarized Zone dan Port Knocking Untuk Keamanan Jaringan Komputer.** CybeSecurity dan Forensik Digital Col, 3.
- Suteja, E., Kumalasari, E., & Raharjo, S. (2021). **Perancangan Sistem Keamanan Jaringan Untuk Mengurangi Kejahatan Cyber Menggunakan Teknik *Demilitarized Zone (DMZ)* dan *Firewall Rules* (Studi Kasus: Laboratorium Basis Data IST AKPRIND).** Jurnal Jarkom, 9(1), 71-80.

Suwanto, R., Ruslianto, I., & Diponegoro, M. (2019). **Implementasi Intrusion Prevention System (IPS) Menggunakan Snort Dan IPTable Pada Monitoring Jaringan Lokal Berbasis Website.** Coding Jurnal Komputer dan Aplikasi, 7(01).



 PalComTech	<b>FORMULIR</b> <b>SURAT PERSETUJUAN TOPIK &amp; JUDUL SKRIPSI</b>
Kode Formulir : <b>FM-IPCT-BAAK-PSB-043</b>	Institusi : INSTITUT TEKNOLOGI DAN BISNIS PALCOMTECH

Kepada Yth. Palembang, .....  
 Ka.Prodi .....  
 di tempat.

Dengan hormat,  
 Saya yang Bertanda tangan di bawah ini :

Program Studi : Informatika Program Sarjana

No	NPM	Nama	IPK	Semester	Sesi Belajar*	No.HP
1.	011190083	KI AGUS SOLIHIN	3,41	8	Malam	08987532868
2.	011190082	HUANITO ALFIANSYAH	3,10	8	Malam	082180003198
3.						

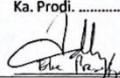
\* Pilih Salah Satu :Pagi/Siang/Malam

Mengajukan Skripsi dengan topik :  
 ..... Keamanan Jaringan .....

Dengan melampirkan deskripsi awal penelitian yang terdiri dari :

- Objek Penelitian
- Apa yang akan diteliti dari objek
- Metode Pengembangan/analisis yang digunakan
- Tujuan / hasil yang diharapkan dari penelitian

Rekomendasi Nama Pembimbing : .....

Menyetujui, Wakil Rektor 1, 	Mengetahui, Ka. Prodi ..... 
---	--

Judul Skripsi (dalam bahasa Indonesia dan Inggris):

- Keamanan Jaringan Menggunakan Teknik DMZ ZONE dengan Sistem Operasi Linux Pada Dialmisik
- Network Security Using the DMZ ZONE Technique with the Linux Operating System on Dialmisik

Diusulkan judul nomor : .....

Pemohon, Mahasiswa 1,  <u>KI AGUS SOLIHIN</u>	Mahasiswa 2,  <u>HUANITO ALFIANSYAH</u>	Mahasiswa 3, _____
Menyetujui, Pembimbing  <u>Agus S.</u>	Mengetahui, Ka. Prodi ..... 	Mengesahkan Wakil Rektor 1 

- Diperbanyak 1 kali : Asli diserahkan ke BAAK dan copy diarsip Mahasiswa
- Form ini wajib dikembalikan ke BAAK pada saat pengumpulan berkas untuk pengajuan ujian

**DIAL** musik

Jl.Letkol Iskandar No. 636 A, Telp. 351723, Fax 356004  
PALEMBANG

Lampiran : -

Hal : Izin Riset Penelitian Skripsi

Kepada Yth.

Ka.Prodi Informatika Palcomtech

Jln. Basuki Rahmat No.05 Palembang

Di-

Tempat

Dengan hormat,

Perihal Permohonan Riset Penelitian Skripsi, yang akan dilakukan. Bersama surat ini kami memberikan izin Riset Penelitian Skripsi di **Toko Dial Musik** kepada saudara :

Nama : Ki Agus Solihin & Huanito Alfiansyah

NPM : 011190083 & 011190082

Prodi : Informatika

Demikianlah surat izin Riset Penelitian Skripsi ini dibuat, untuk dipergunakan semestinya. Atas perhatian kerjasamanya kami ucapkan terima kasih.

Palembang, 4 Agustus 2023

Hormat kami,

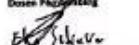
(Dial Musik)

  
**DIAL** MUSIC & CO.  
(Riset Musik)  
Jl. Letkol Iskandar No. 636 A  
Telp. 0711 351723  
Fax. 0711 356004  
PALEMBANG 30132

	FORMULIR			
	KONSULTASI LAPORAN SKRIPSI INSTITUT TEKNOLOGI DAN BISNIS PALCOMTECH			
	Kode Formlir FM-IPCT-BAJK-PSB-045	Institusi Tahun Akademik	: INSTITUT TEKNOLOGI DAN BISNIS PALCOMTECH :	
NO	NPM	Nama	Prodi	Semester
1	011190062	Huzaini AlFarasyah	Informatika	8 (Delapan)
2	011190063	Ki Agus Solihin	Informatika	8 (Delapan)

Judul Laporan Skripsi : Keamanan Jaringan Menggunakan Teknik DMZ Dengan Sistem Operasi Linux Pada Dns Munk

Pertemuan Ke -	Tanggal Konsultasi	Batas Waktu Perbaikan	Materi yang Dibahas / Catatan Perbaikan	Paraf Pembimbing
1	13 Maret 2023	16 Maret 2023	-Pengkajuan Judul	
2	16 Maret 2023	16 Maret 2023	-Acc Judul	
3	17 Maret 2023	18 April 2023	-Progres Laporan Skripsi	
4	18 April 2023	02 Mei 2023	-Revisi Latar Belakang -Revisi Rumusan Masalah -Revisi Kesimpulan Pembicaraan	
5	02 Mei 2023	09 Mei 2023	-Acc Bab I, II, III	
6	09 Mei 2023	11 Mei 2023	-Pengumpulan Proposal	
7	11 Mei 2023	03 Juni 2023	-Acc Ujian Proposal	
8	03 Juni 2023	07 Juli 2023	-Progres Laporan Skripsi Bab IV, V	
9	07 Juli 2023	14 Juli 2023	-Revisi Tata Tulis -Pembuatan Project	
10	14 Juli 2023	21 Juli 2023	-Implementasi DMZ	
11	21 Juli 2023	27 Juli 2023	-Revisi Bab V	
12	27 Juli 2023	01 Agustus 2023	-Revisi Tata Tulis dan Kesimpulan -Demo Project	
13	01 Agustus 2023	04 Agustus 2023	-Review Laporan Keseluruhan	
14	04 Agustus 2023	-	-Acc Bab IV dan V -Acc Ujian Kompro	
15				

Palembang,  
Dosen Pembimbing  


## SURAT PERNYATAAN UJIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Huanito Alfiansyah  
Tempat/Tanggal Lahir : Palembang/10 Juni 2001  
Prodi : Informatika  
NPM : 011190082  
Semester : 8 (Delapan)  
No.Telp/Hp : 082180009198  
Alamat : Komp Kehutanan 1 Jln melati blok b8 no13

Menyatakan dengan sesungguhnya bahwa :

1. Laporan ini saya buat dengan sebenarnya dan berdasarkan sumber yang benar.
2. Objek tempat saya melaksanakan laporan berbentuk CV/PT/Pemerintahan/SMA sederajat dan dinyatakan masih aktif beroperasi hingga saat ini
3. Data perusahaan dalam laporan skripsi ini benar adanya dan bersifat valid.
4. Laporan ini bukan merupakan hasil plagiat/menjiplak karya ilmiah orang lain
5. Laporan ini merupakan hasil kerja saya sendiri (bukan buatan/dibuatkan orang lain)
6. Buku referensi yang saya gunakan untuk laporan skripsi ini merupakan buku yang terbit dalam 5 (lima) tahun terakhir ini.
7. Semua dokumen baik berupa dokumen asli maupun salinan yang saya serahkan sebagai syarat untuk mengikuti ujian skripsi adalah dokumen yang sah dan benar.
8. Hasil karya saya yang merupakan hasil dari skripsi berupa karya tulis, program, aplikasi atau alat, setelah melalui ujian komprehensif dan revisi, bersedia untuk saya serahkan kepada lembaga melalui Kaprodi untuk dokumentasi dan kepentingan pengembangan ilmu pengetahuan dan teknologi.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari pihak manapun dan apabila di kemudian hari ternyata saya terbukti secara sah melanggar salah satu dari pernyataan ini, saya bersedia untuk menerima sanksi sesuai dengan peraturan dan hukum berlaku di negara Republik Indonesia, dan gelar akademik yang saya peroleh dari Perguruan Tinggi ini dapat dibatalkan.

Palembang,  
Menyatakan,  
  
Huanito Alfiansyah

## SURAT PERNYATAAN UJIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Ica Agus Salihin  
Tempat/Tanggal Lahir : Paimbung, 10-Maret-2023  
Prodi : INFORMATIKA  
NPM : 011190083  
Semester : 8  
No.Telp/Hp : 08987532868  
Alamat : Jl. Misa No. 26, Rt. 12 RW. 03

Menyatakan dengan sesungguhnya bahwa :

1. Laporan ini saya buat dengan sebenarnya dan berdasarkan sumber yang benar.
2. Objek tempat saya melaksanakan laporan berbentuk CV/PT/Pemerintahan/SMA sederajat dan dinyatakan masih aktif beroperasi hingga saat ini
3. Data perusahaan dalam laporan skripsi ini benar adanya dan bersifat valid.
4. Laporan ini bukan merupakan hasil plagiat/menjiplak karya ilmiah orang lain
5. Laporan ini merupakan hasil kerja saya sendiri (bukan buatan/dibuatkan orang lain)
6. Buku referensi yang saya gunakan untuk laporan skripsi ini merupakan buku yang terbit dalam 5 (lima) tahun terakhir ini.
7. Semua dokumen baik berupa dokumen asli maupun salinan yang saya serahkan sebagai syarat untuk mengikuti ujian skripsi adalah dokumen yang sah dan benar.
8. Hasil karya saya yang merupakan hasil dari skripsi berupa karya tulis, program, aplikasi atau alat, setelah melalui ujian komprehensif dan revisi, bersedia untuk saya serahkan kepada lembaga melalui Kaprodi untuk dokumentasi dan kepentingan pengembangan ilmu pengetahuan dan teknologi.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tanpa paksaan dari pihak manapun dan apabila di kemudian hari ternyata saya terbukti secara sah melanggar salah satu dari pernyataan ini, saya bersedia untuk menerima sanksi sesuai dengan peraturan dan hukum berlaku di negara Republik Indonesia, dan gelar akademik yang saya peroleh dari Perguruan Tinggi ini dapat dibatalkan.

Paimbung, 7-Agustus-2023

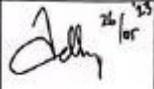
/atakan,  
  
SALIHIN

	<b>FORMULIR REVISI UJIAN PROPOSAL INSTITUT TEKNOLOGI DAN BISNIS PALCOMTECH</b>
	Kode Formulir : FM-PCT-BAAK-PSB-127 Instansi : INSTITUT TEKNOLOGI DAN BISNIS PALCOMTECH

**Revisi Ujian Proposal Skripsi  
Mahasiswa Institut Teknologi dan Bisnis PalComTech**

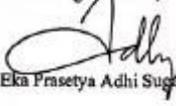
Program Studi : Informatika Program Sarjana  
 Tanggal Pelaksanaan : 17 Mei 2023  
 Judul Proposal Skripsi : Keamanan Jaringan Menggunakan Teknik DMZ Zone dengan Sistem Operasi Linux pada Dialmusik

No	NPM	Nama	Semester
1	011190082	Huanito Alfiansyah	8
2	011190083	Ki Agus Solihin	8

No	Revisi	Nama Penguji	Tanda Tangan
1.	parafasi parafisa		Benediktus Effendi
1.	latar belakang - Identifikasi masalah	Eka Prasetya A.S.	
2.	Landasan teori: - teori NOL - uraian penelitian terdahulu		
3.	Metode Penelitian - apakah sampai ke bahas monitoring & management		
1.	Laporan proposal	Eko Sitomara	

Perubahan Judul Skripsi : Keamanan Jaringan Menggunakan Teknik DMZ dengan Sistem Operasi Linux pada Dialmusik

Palembang, 17 Mei 2023  
 Ketua Program Studi,

  
 Eka Prasetya Adhi Sugara, S.T., M.Kom.

\*Fotokopi Form Revisi dikumpulkan ke BAAK setelah ditandatangani Kaprodi

