

**IMPLEMENTASI *HONEYPOT* PADA SISTEM KEAMANAN *SERVER*  
BERBASIS *GRAFANA* DENGAN NOTIFIKASI OTOMATIS  
MENGUNAKAN *API* TELEGRAM PADA RASPBERRY PI**

*Honeypot Implementation on Grafana Based Server Security System  
with Automatic Notification Using Telegram API on Raspberry Pi*

**PROPOSAL PROYEK AKHIR**

**Diajukan sebagai syarat untuk mengambil Mata Kuliah Proyek Akhir**

oleh :

**FITRIA FEBRIANA**

**6705184044**



**D3 TEKNOLOGI TELEKOMUNIKASI**

**FAKULTAS ILMU TERAPAN**

**UNIVERSITAS TELKOM**

**2021**

## LEMBAR PENGESAHAN

Proposal Proyek Akhir dengan judul :

IMPLEMENTASI *HONEYPOT* PADA SISTEM KEAMANAN *SERVER*  
BERBASIS *GRAFANA* DENGAN NOTIFIKASI OTOMATIS MENGGUNAKAN *API*  
TELEGRAM PADA RASPBERRY PI

*Honeypot Implementation on Grafana Based Server Security System  
with Automatic Notification Using Telegram API on Raspberry Pi*

oleh :

FITRIA FEBRIANA

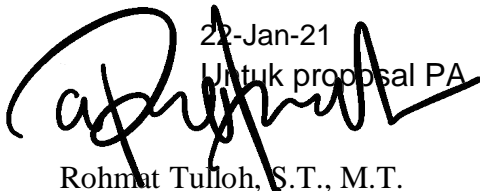
6705184044

Telah diperiksa dan disetujui untuk diajukan sebagai syarat mengambil  
Mata Kuliah Proyek Akhir  
pada Program Studi D3 Teknologi telekomunikasi Universitas Telkom

Bandung, 21 Januari 2021

Menyetujui,

Pembimbing I

22-Jan-21  
Untuk proposal PA  


Rohmat Tulloh, S.T., M.T.

NIP. 06830002

Pembimbing II



Asep Mulyana, S.T., M.T.

NIP. 945700113

## ABSTRAK

Serangan yang terjadi banyak disebabkan karna kelalaian pemilik *server* dengan memasang keamanan yang lemah maupun jarang memantau aktifitas yang janggal terjadi di servernya sendiri. Serangan yang tidak bertanggung jawab itu, tidak dapat diprediksi dan dapat mengancam seluruh data penting yang disimpan di komputer.

Berdasarkan pemaparan diatas, pada proyek akhir ini akan di implementasikan sebuah *Honeypot Kippo* untuk mengecoh penyerang dalam hal keamanan *server*. *Honeypot* akan di implementasikan pada Raspbbery Pi dengan sistem operasi Ubuntu, dan akan di terapkan pada port ssh yang ditukar sebelumnya, sehingga penyerang tidak akan menyadari bahwa dirinya dijebak. Aktifitas yang terekam oleh *Honeypot Kippo* akan di simpan ke *file* berbentuk *log*. *Log* yang terekam disimpan terlebih dahulu dalam *database* yang pada akhirnya dapat di olah dan di visualisasikan.

Segala aktifitas yang berbentuk *log* tersebut yang akan di visusalisasikan di *Dashboard Grafana* untuk memudahkan pemilik memantau seberapa sering dan seberapa bahaya *server* nya diserang. Data *log* tersebut juga dihubungkan ke Telegram, sehingga pemilik dapat mendapatkan notifikasi serangan secara *realtime*.

kata kunci : *honeypot*, serangan, *grafana*, Raspberry Pi, *server*

## DAFTAR ISI

LEMBAR PENGESAHAN.....	i
ABSTRAK .....	ii
DAFTAR ISI .....	iii
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang.....	1
1.2 Tujuan dan Manfaat .....	1
1.3 Rumusan Masalah.....	2
1.4 Batasan Masalah .....	2
1.5 Metodologi .....	2
BAB II DASAR TEORI.....	3
2.1 <i>Honeypot</i> .....	3
2.2 <i>Bruteforce</i> .....	4
2.3 <i>Database</i> .....	4
2.4 <i>Grafana</i> .....	5
2.5 <i>Telegram</i> .....	5
2.6 Raspberry Pi 3 .....	5
BAB III MODEL SISTEM .....	6
3.1 Blok Diagram Sistem.....	6
3.2 Tahapan Perancangan .....	7
3.3 Perancangan.....	8
BAB IV BENTUK KELUARAN YANG DIHARAPKAN .....	9
4.1 Keluaran yang Diharapkan.....	9
4.2 Jadwal Pelaksanaan.....	9
DAFTAR PUSTAKA .....	10

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Kemajuan Ilmu dan Teknologi memunculkan lebih banyak kerugian dalam bidang teknologi. Sama halnya seperti jaringan, semakin kompleksnya jaringan dirancang, semakin kompleks juga masalah yang akan timbul dari serangan-serangan yang tidak bertanggung jawab. Serangan yang tidak dapat diprediksi kapan terjadi, terkadang membuat pemilik *server* lengah akan serangan yang terjadi saat jaringan tidak selamanya ia pantau secara *realtime*.

Dari permasalahan tersebut, pada proyek akhir ini akan dibuat sebuah perangkat bagi para penyerang yang tidak bertanggung jawab untuk direkam segala aktifitasnya dan identitas *ip* penyerang tersebut. Tidak hanya sebagai perangkat, penerapan *Honeypot* juga digunakan sebagai gerbang awal untuk mengecoh penyerang yang menganggap sebagai *server* asli yang akan diserang.

Segala aktifitas yang dilakukan saat menyerang *port ssh service* yang telah ditukar dengan *Honeypot Kippo*, akan disimpan pada *database* dan data tersebut akan diolah lalu divisualisasikan di *Grafana* untuk mempermudah pemilik *server* memantau seberapa berbahaya penyerang tersebut melakukan aktifitasnya. Dan segala bentuk tindakan yang terekam tersebut dapat dikirimkan ke pemilik *server* asli sebagai *alert* melalui Telegram secara *realtime*.

### **1.2 Tujuan dan Manfaat**

Adapun tujuan dari Proyek tingkat ini, sebagai berikut:

1. Dapat mengimplementasikan *Honeypot Kippo* pada Raspberry Pi.
2. Dapat mendeteksi adanya serangan menggunakan *Honeypot*.
3. Dapat memberikan notifikasi serangan menggunakan aplikasi Telegram.
4. Dapat memantau serangan dalam rentang waktu tertentu melalui *Grafana*.

### 1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek tingkat ini, sebagai berikut:

1. Bagaimana mengimplementasikan *Honeypot Kippo* pada Raspberry Pi?
2. Bagaimana mendeteksi adanya serangan menggunakan *Honeypot*?
3. Bagaimana cara menghubungkan notifikasi serangan ke aplikasi Telegram?
4. Bagaimana menghubungkan serangan dalam rentang waktu tertentu di *Grafana*?

### 1.4 Batasan Masalah

Dalam Proyek tingkat ini, dilakukan pembatasan masalah sebagai berikut:

1. Pengimplementasian jenis *Honeypot* di Raspberry Pi hanya *Medium Interaction*.
2. Aplikasi Telegram hanya digunakan untuk memberikan notifikasi serangan yang sedang terjadi.
3. Pemantauan serangan pada *Grafana* hanya memvisualisasikan seberapa sering dan tingkat bahaya terjadinya serangan.

### 1.5 Metodologi

Metodologi pada penelitian ini, sebagai berikut:

#### 1. Studi Literatur

Hal yang dilakukan adalah mencari informasi dan pendalaman materi-materi yang terkait melalui referensi yang tersedia di berbagai sumber.

#### 2. Riset

Hal yang dilakukan yaitu mencari informasi mengenai penerapan *Honeypot* dengan beberapa model atau versi yang berbeda, mengintegrasikan *Honeypot* dengan beberapa aplikasi yang digunakan seperti *database* dan lain-lain.

#### 3. Perancangan

Hal yang dilakukan yaitu mengimplementasikan *Honeypot* ke sebuah papan computer Raspberry Pi 3.

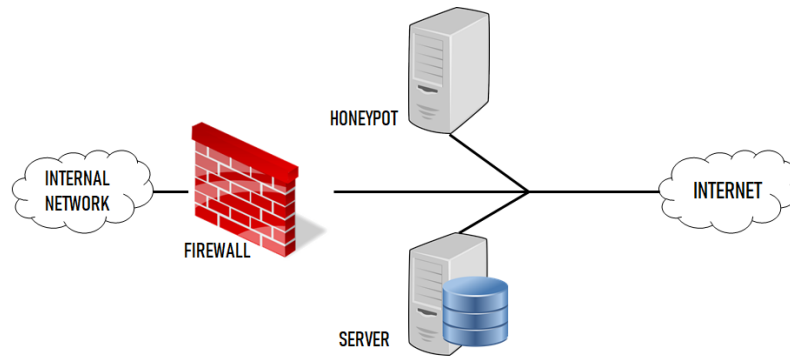
## BAB II

### DASAR TEORI

#### 2.1 *Honeypot*

*Honeypot* adalah suatu cara untuk menjebak atau menangkal usaha-usaha penggunaan tak terotorisasi dalam sebuah *system* informasi [1]. *Honeypot* merupakan *server* palsu pengalih perhatian penyerang, sehingga menganggap *server* yang diserangnya ialah *server* tujuan yang akan ia serang dengan mengambil *file-file* tidak penting sehingga membuang-buang waktunya saja. Hal tersebut selaras dengan kegunaan nya, *Honeypot* merupakan sebuah *software open source* yang digunakan untuk diserang atau di selidiki. *Honeypot* terbagi menjadi beberapa klasifikasi yaitu :

- a. *Low-Interaction Honeypot*; merupakan *honeypot* dengan tingkat interaksi *honeypot*, yang didesain untuk mengemulasikan service (layanan) seperti *server* yang asli. Penyerang hanya mampu memeriksa dan terkoneksi ke satu atau beberapa port. [2]
- b. *Medium-Interaction Honeypot*; merupakan salah satu klasifikasi *honeypot* yang service (layanan) nya lebih banyak untuk berinteraksi dengan penyerang dari pada *low-interaction*, dan lebih sedikit dari pada *high-interaction*. Salah satu jenis *Honeypot* yang satu ini hampir dapat menyerupai *server* aslinya saat penyerang melakukan interaksi, namun masih terdapat batasan layanan jika dibandingkan *high-interaction* yang tak terbatas.
- c. *High-Interaction Honeypot*; terdapat system operasi dimana penyerang dapat berinteraksi langsung dan tidak mempunyai batasan yang dapat membatasi interaksi tersebut. Dengan kata lain jenis *honeypot* ini membuat *server* palsu yang menyerupai dengan *server* asli, sehingga penyerang tidak mencurigai saat terjadi penyerang. [2]



**Gambar 2. 1 Ilustrasi Pengimplementasian Honeypot**

*Kippo* adalah salah satu jenis *Honeypot* dengan tingkat *medium-interaction* yang didesain menggunakan bahasa *python* untuk menyimpan informasi *bruteforce* dan informasi aktivitas penyusup didalam *server* [3].

## **2.2 Bruteforce**

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian permasalahan kode cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter dan panjang kode tertentu tentunya dengan banyak sekali kombinasi kode. Algoritma brute force adalah algoritma yang lempang atau apa adanya. Pengguna hanya tinggal mendefinisikan karakter set yang diinginkan dan berapa ukuran dari kodenya. Tiap kemungkinan kode akan di generate oleh algoritma ini [4].

## **2.3 Database**

Database atau pangkalan data merupakan suatu kumpulan data yang disimpan didalam sebuah perangkat komputer secara sistematis sehingga dapat diperiksa dengan menggunakan suatu program komputer agar dapat informasi dari basis data tersebut. Perangkat lunak yang digunakan untuk mengelola dan memanggil query basis data disebut dengan system manajemen basis data dalam system basis data dapat dipelajari dalam ilmu informasi.



## 2.4 Grafana

Grafana adalah perangkat lunak visualisasi dan analitik yang bersifat opensource. Grafana memungkinkan untuk memvisualisasikan, mengingatkan, dan menjelajahi metrik disimpan. Alat untuk mengubah data timeseries database (TSDB) menjadi grafik dan visualisasi yang indah [5].



**Gambar 2. 2 Tampilan Dashboard Grafana**

Grafana sangat cocok untuk membuat Dashboard yang dinamis dengan berbagai menu bawaan. Grafana juga memiliki dashboard template yang bisa digunakan untuk mengumpulkan variabel data yang digunakan. Dalam paparan ini dijelaskan bahwa Grafana sangat support dalam visualisasi data dalam bentuk time series [5].

## 2.5 Telegram

Telegram merupakan salah satu aplikasi chatting yang menawarkan service chatting rahasia yang di enkripsi end-to-end sebagai keamanan tambahan. Aplikasi Telegram salah satu aplikasi gratis, ringan dan multiplatform. Telegram juga memiliki Bot API yang cukup lengkap dan makin berkembang, sehingga memungkinkan untuk membuat Bot pintar yang dapat merespon pesan dari user [6].

## 2.6 Raspberry Pi 3

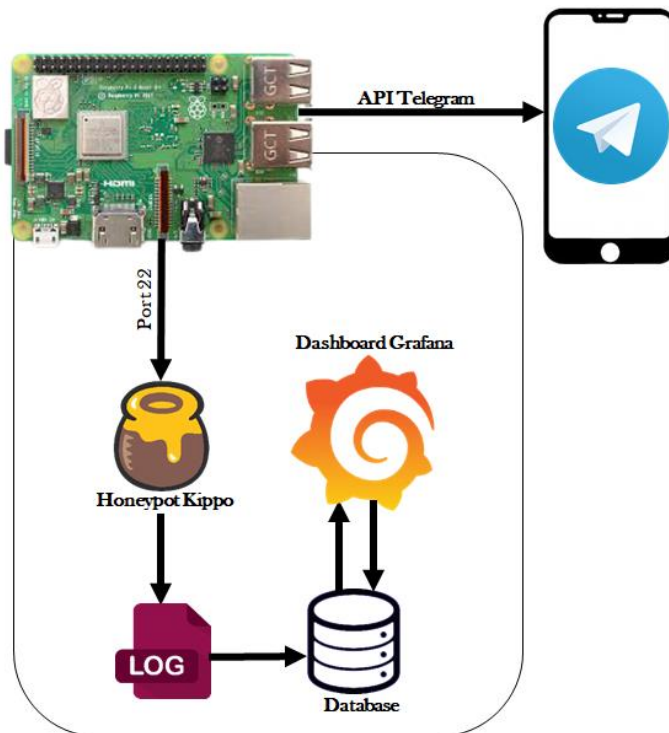
Raspberri Pi 3 merupakan komputer papan tunggal (*single-board circuit*; SBC) yang dapat digunakan untuk menjalankan program komputer hingga video beresolusi tinggi. Raspberry Pi dikembangkan oleh yayasan nirlaba, Rasberry Pi Foundation, yang digawangi sejumlah pengembang dan ahli komputer dari Universitas Cambridge, Inggris.

## BAB III

### MODEL SISTEM

#### 3.1 Blok Diagram Sistem

Pada bab ini akan dijelaskan mengenai pengimplementasian *Honeypot* pada sistem keamanan *server* berbasis *Grafana* pada *Raspberry Pi*, pengimplementasian ini juga menerapkan sebuah notifikasi otomatis serangan. *Honeypot* yang akan diterapkan pada *Raspberry Pi* dengan sistem operasi *Ubuntu*, akan menjebak para penyerang dan mencatat segala aktifitas yang dilakukan penyerang. Saat semua aktifitasnya terekam, *log* aktifitas tersebut akan di pantau melalui *Grafana* dan noifikasi di Telegram. Pengintegrasian *Honeypot* dengan *Dashboard Grafana* ini menggunakan bantuan *Database* untuk mendapatkan *log* aktifitas dan mengirimkannya untuk dapat di visualisasikan di *Grafana*. Adapun pengimplementasian dengan model sistem *monitoring* yang telah dibuat dapat dilihat pada 3.1 dibawah ini.



Gambar 3. 1 Model Sistem Implementasi Honeypot pada Rasberry Pi

*Database* digunakan untuk mengintergrasikan *log* aktifitas dengan *Dashboard Grafana* agar mempermudah pemrosesan data pada proses memvisualisasikan nya.

### 3.2 Tahapan Perancangan

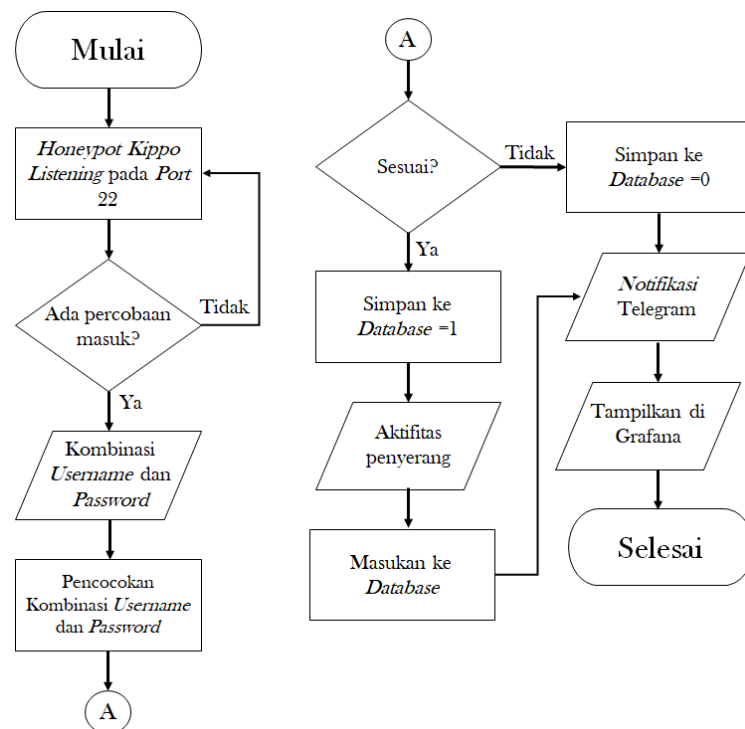
Proses pengimplementasian *Honeypot Kippo* ini dilakukan dengan melakukan pertukaran *port* dan proses implementasi tersebut dapat dilihat pada Gambar 3.2, tahapan pengimplementasiannya ialah sebagai berikut:

1. Penukaran port

Langkah awal dalam mengimplementasikan *Honeypot* adalah dengan menukar *port ssh service* yang akan digunakan oleh *Honeypot* nantinya sebagai *server* palsu.

2. Pengimplementasian Honeypot

Pengimplementasian dilakukan untuk menerapkan *server* palsu pada Raspberry Pi pada port 22 yang nantinya akan di perkirakan oleh penyerang sebagai *server ssh service* yang asli, adapun beberapa tahapan dalam bentuk flowchart sebagai berikut :



Gambar 3. 2 Diagram Alir Perancangan

### 3.3 Perancangan

Pada Proyek Akhir ini akan diimplementasikan sebuah *Honeypot Kippo* dengan *level medium-interaction* yang diambil dari jurnal komputer dan aplikasi Fakultas MIPA Universitas Tanjungpura dengan judul “Implementasi *Honeypot Kippo* pada Sistem Keamanan Server Berbasis *Web Monitoring* dengan Notifikasi Otomatis menggunakan *API Telegram*”. Pada jurnal yang ditulis oleh Fathuzzikri dkk ini, pengimplementasian *Honeypot Kippo* sederhana nya hanya dikomputer dengan sistem operasi linux dan pantauan *log* aktifitasnya melalui *web monitoring* yang dibuat menggunakan *Framework Laravel*. Namun pada Proyek Akhir ini, implementasi akan di pantau melalui *software open source Grafana*, dan *Honeypot* tersebut akan diimplementasikan pada Raspberry Pi.

## BAB IV

### BENTUK KELUARAN YANG DIHARAPKAN

#### 4.1 Keluaran yang Diharapkan

Perancangan pada Proyek Akhir akan mengimplementasikan *Honeypot Kippo* di Raspberry Pi. Adapun hasil yang diharapkan ialah :

1. *Honeypot Kippo* dapat mendeteksi serangan *bruteforce* yang mungkin terjadi pada keamanan server.
2. Segala aktifitas penyerang termasuk serangan *bruteforce* dapat terekam didalam *log*, dan akan tersimpan di dalam *database* sesuai dengan tingkatan serangan yang dilakukan.
3. Data yang berada di dalam database akan visualisasikan di *Dashboard Grafana* dan serangannya pun akan di notifikasikan secara realtime melalui aplikasi Telegram.

#### 4.2 Jadwal Pelaksanaan

Adapun jadwal pengerjaan Proyek Akhir bisa dilihat pada tabel 4.1 sebagai berikut:

**Tabel 4. 1 Jadwal Pelaksanaan**

Judul Kegiatan	Waktu							
	Nov	Des	Jan	Feb	Mar	Apr	Mei	Jun
Studi Literatur								
Implementasi dan Simulasi								
Pengujian								
Analisa								
Pembuatan Laporan								

## DAFTAR PUSTAKA

- [1] L. Spitzner, *Honeypots: Tracking Hackers*. 2002.
- [2] D. D. Laksana, S. J. I. Ismail, and N. Hendrarini, "Implementation Honeypot With Modern Honey Network," *e-Proceeding Appl. Sci.*, vol. 3, no. 3, p. 1816, 2017.
- [3] Fathuzzikri, I. Ruslianto, and U. Ristian, "Implementasi Honeypot Kippo pada Sistem Keamanan Server Berbasis Web Monitoring dengan Notifikasi Otomatis menggunakan API Telegram," *J. Komput. dan Apl.*, vol. 07, no. 03, p. 55, 2019.
- [4] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *J. Nas. Inform. dan Teknol. Jar.*, vol. 1, no. 1, p. 52, 2016, doi: 10.30743/infotekjar.v1i1.48.
- [5] D. Rahman, H. Amnur, and I. Rahmayuni, "Monitoring Server dengan Prometheus dan Grafana serta Notifikasi Telegram," *J. Ilm. Teknol. istem Inf.*, vol. 1, no. 4, p. 135, 2020.
- [6] G. Sastrawangsa, "Pemanfaatan Telegram Bot Untuk Automatisasi Layanan Dan Informasi Mahasiswa Dalam Konsep Smart Campus," *Konf. Nas. Sist. Inform.*, p. 773, 2017.



UNIVERSITAS TELKOM  
FAKULTAS ILMU TERAPAN  
KARTU KONSULTASI  
SEMINAR PROPOSAL PROYEK AKHIR

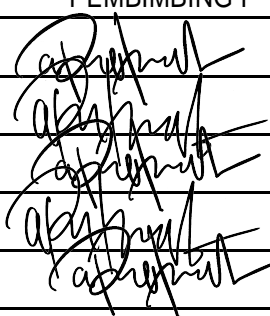
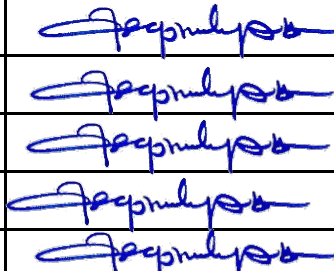
NAMA / PRODI : FITRIA FEBRIANA / D3 Teknologi Telekomunikasi NIM : 6705184044

JUDUL PROYEK TINGKAT :

IMPLEMENTASI HONEYPOT PADA SISTEM KEAMANAN SERVER BERBASIS GRAFANA DENGAN NOTIFIKASI OTOMATIS MENGGUNAKAN API TELEGRAM PADA RASPBERRY PI

CALON PEMBIMBING : I. Rohmat Tulloh, S.T., M.T.

II. Asep Mulyana, S.T., M.T.

NO	TANGGAL	CATATAN HASIL KONSULTASI	TANDA TANGAN CALON PEMBIMBING I
1		BAB 1 (SELESAI)	
2		BAB 2 (SELESAI)	
3		BAB 3 (SELESAI)	
4		BAB 4 (SELESAI)	
5		FINALISASI PROPOSAL	
6			
7			
8			
9			
10			
NO	TANGGAL	CATATAN HASIL KONSULTASI	TANDA TANGAN CALON PEMBIMBING II
1		BAB 1 (SELESAI)	
2		BAB 2 (SELESAI)	
3		BAB 3 (SELESAI)	
4		BAB 4 (SELESAI)	
5		FINALISASI PROPOSAL	
6			
7			
8			
9			
10			