

**PENERAPAN SURICATA SNORBY BARNYARD2 SEBAGAI
PENGAMAN DARI SERANGAN DISTRIBUTED DENIAL OF
SERVICE (DDoS)**

*IMPLEMENTATION OF BARNYARD2 SNORBY SURICATA AS A SECURITY FROM
DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS*

PROPOSAL PROYEK AKHIR

Diajukan sebagai syarat untuk mengambil Mata Kuliah Proyek Akhir

oleh :

HASNATUL HUSNI

6705184106



D3 TEKNOLOGI TELEKOMUNIKASI

FAKULTAS ILMU TERAPAN

UNIVERSITAS TELKOM

2021

LEMBAR PENGESAHAN

Proposal Proyek Akhir dengan judul :

PENERAPAN SURICATA SNORBY BARNYARD2 SEBAGAI PENGAMAN DARI
SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDoS)

*IMPLEMENTATION OF BARNYARD2 SNORBY SURICATA AS A SECURITY FROM
DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS*

oleh :

HASNTUL HUSNI

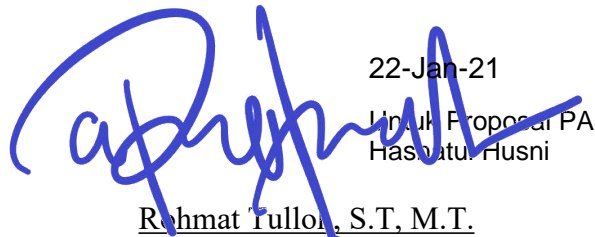
6705184106

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
Hasnutul Husni

Rohmat Tullon, S.T., M.T.

NIP. 06830002

Pembimbing II



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

NIP. 945700113

ABSTRAK

Seiring berkembangnya teknologi, khususnya keamanan jaringan yang semakin berkembang menuntut agar sistem keamanan untuk dapat mencegah terjadinya sebuah ancaman ataupun serangan terhadap suatu sistem. Seperti halnya berusaha mendapatkan suatu informasi seperti halnya username dan password, atau melakukan serangan serangan seperti DDoS (Distributed Denial of Service), Nmap, HPING3 dan lainnya.

Dalam proyek akhir ini akan dibuat sebuah sistem pencegah serangan yang dapat mengidentifikasi serangan ataupun ancaman yaitu *Intrusion Prevention System* (IPS). Dimana sistem ini merupakan perpaduan beberapa software yaitu suricata, snorby, barnyard2 yang saling terintegrasi kemudian diuji dengan DDoS (Distributed Denial of Service), Nmap, HPING3 dan lainnya. IPS dapat mencegah serangan yang akan masuk ke jaringan local dengan memeriksa dan mencatat semua paket data serta mengenali paket dengan sensor saat serangan teridentifikasi.

Pada proyek akhir ini diharapkan sistem IPS menggunakan suricata, snorby, barnyard2 dapat mengidentifikasi ancaman DDoS serta melakukan block terhadap paket-paket yang terdeteksi sebagai ancaman. Sehingga dapat memberikan keamanan jaringan dengan menggunakan sistem tersebut.

Kata kunci : *IPS, DDoS , suricata, snorby, barnyard2*

DAFTAR ISI

LEMBAR PENGESAHAN.....	i
ABSTRAK.....	ii
DAFTAR ISI.....	iii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Tujuan dan Manfaat.....	2
1.3 Rumusan Masalah.....	2
1.4 Batasan Masalah.....	2
1.5 Metodologi.....	3
BAB II DASAR TEORI.....	4
2.1 <i>Intrusion Prevention System</i>	4
2.2 <i>Suricata</i>	4
2.3 <i>Snorby</i>	5
2.4 Barnyard.....	5
2.5 Firewall.....	5
2.6 DDoS (Distributed Denial of Service).....	5
BAB III MODEL SISTEM.....	6
3.1 Blok Diagram Sistem.....	6
3.2 Tahapan Perancangan.....	6
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

Keamanan jaringan merupakan salah satu proses untuk mencegah dan memonitoring penggunaan jaringan yang tidak sah dari jaringan komputer. Tujuan keamanan tersebut untuk mengantisipasi gangguan baik fisik ataupun logic. Namun tidak bisa dipungkiri bahwa semakin banyak celah keamanan jaringan internet yang ditemukan. Beberapa yang sering terjadi dan muncul ialah virus, SQL Injection, DDoS (*Distributed Denial of Service*), exploit, sniffing dan sebagainya. Sistem harus dilindungi dari berbagai ancaman keamanan dan usaha penyusupan data oleh pihak yang tidak seharusnya.

Intrusion prevention system (IPS) bertugas untuk memonitor paket-paket data (*data packets*) jaringan dari adanya aktivitas mencurigakan dan mencoba melakukan aksiaksi tertentu menggunakan kebijakan-kebijakan (*policy*) tertentu (Xinyau Zhang, 2007). Sistem IPS juga yang dapat mencegah dan memberikan tindakan saat terjadi penyusupan.

Penelitian Istiana Adesty,dkk, 2020, sistem IPS diuji menggunakan DDoS berupa HPING3, LOIC dimana menggunakan software suricata sebagai pendeteksi serangannya.

Sedangkan pada penelitian Bagas Suryo Anggoro, 2019, sistem yang digunakan IPS dengan metode SDLC (Security Development Life Cycle) dengan model waterfall menurut bassil dengan kombinasi honeypot.

Pada penelitian M. K. S. M. Alim Nuryanto tahun 2015, sistem deteksi serangan yang digunakan adalah *Network Detection System* (NIDS), yang dimana sistem ini hanya berfokus pada pengidentifikasian serangan yang terjadi menggunakan suricata. Perbedaan dari penelitian sebelumnya yaitu sistem pengidentifikasian serangan menggunakan IPS yang dimana dapat melakukan block serangan atau ancaman pada suricata.

Penelitian ini bertujuan mengimplementasikan IPS karena dengan sistem tersebut memanfaatkan *firewall* akan mendeteksi serangan yang berbasis port dan

protokol dan menolak akses, serta mencatat log yang teridentifikasi negatif. Suricata bertugas sebagai sistem pencegah serangan sejenis snort yang membutuhkan *firewall* dimana suricata akan merekam ancaman yang masuk kedalam suatu log. Snorby bertugas memonitoring sistem yang telah dibuat oleh suricata itu sendiri dalam bentuk *interface*. Serta Barnyard2 berfungsi untuk penerjemah alert dan log sistem. Sehingga dalam proyek akhir ini, hasil yang diharapkan yaitu sistem dapat mengidentifikasi serangan serta mencegah serangan berupa HPING3, Nmap, Brute Force.

1.2 Tujuan dan Manfaat

Adapun tujuan dari Proyek Akhir ini, sebagai berikut:

1. Dapat membuat sistem pendeteksi serangan *Intrusion Prevention System* (IPS) dengan suricata, snorby, barnyard2.
2. Dapat membuat sistem pencegahan paket yang terdeteksi sebagai serangan DDoS.
3. Dapat melakukan pengujian pada sistem dengan melakukan simulasi serangan DDoS.

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut:

1. Bagaimana cara membuat sistem pendeteksi serangan *Intrusion Prevention System* (IPS) dengan suricata, snorby, barnyard2?
2. Bagaimana cara membuat sistem pencegahan paket yang terdeteksi sebagai serangan DDoS?
3. Bagaimana cara pengujian pada sistem dengan melakukan simulasi serangan DDoS?

1.4 Batasan Masalah

Dalam Proyek Akhir ini, dilakukan pembatasan masalah sebagai berikut:

1. Dalam pembuatan sistem *Intrusion Prevention System* (IPS) pada ubuntu server dengan menginstall serta mengkonfigurasi suricata, snorby, barnyard2.
2. Dalam pembuatan sistem ini menggunakan sistem operasi linux, ubuntu sebagai sistem IPS dan kali linux sebagai penyerang / attacker.

3. Sistem IPS dapat mendeteksi serangan serta memblock serangan pada suricata, sedangkan snorby digunakan sebagai interface monitoring namun tidak dapat melakukan block serangan.
4. Serangan yang dilakukan HPING3, Nmap, BruteForce.

1.5 Metodologi

Metodologi pada proyek akhir ini, sebagai berikut:

1. Studi Literatur

Studi literatur yang dilakukan adalah mempelajari hal-hal yang berkaitan dengan IPS, suricata, snorby, barnyard dan DDoS, serta cara kerja sistem tersebut.

2. Analisis Kebutuhan Perangkat

Tahapan selanjutnya adalah menyiapkan perangkat dari persiapan alat yang dibutuhkan dalam pengkonfigurasian sistem sampai pengujian sistem.

3. Perancangan Ilustrasi Jaringan.

Perancangan ilustrasi jaringan dilakukan untuk meletakkan posisi suricata pada sebuah jaringan yang sudah ada.

4. Pembuatan Sistem

Melakukan konfigurasi suricata, snorby, barnyard2, DDoS pada linux sebagai sistem yang akan berjalan.

5. Pengujian Sistem

Melakukan pengujian terhadap sistem yang telah dirancang sebelumnya.

Diantaranya suricata, snorby, barnyard2 dan DDoS sebagai penyerang.

6. Pengujian Keamanan Sistem

Pada tahap ini dilakukan penyerangan oleh DDoS terhadap sistem IPS yang telah di konfigurasi sebelumnya.

7. Analisis

Pada tahap ini dapat menganalisis hasil dari serangan DDoS terhadap sistem IPS suricata, snorby, barnyard2.

BAB II

DASAR TEORI

2.1 Intrusion Prevention System

Sistem Intrusion Prevention System (IPS) merupakan sistem untuk mencegah sebuah serangan terjadi dengan memanfaatkan firewall yang ada, sistem IPS juga yang dapat mencegah dan memberikan tindakan saat terjadi penyusupan. Ada beberapa metode IPS (Intrusion Prevention System) melakukan kebijakan apakah paket data yang lewat layak masuk atau keluar dalam jaringan tersebut :

1. Signature-based Intrusion Detection System

Pada metode ini, telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data signature yang ada harus tetap ter-update.

2. Anomaly-based Intrusion Detection System

Pada metode ini, terlebih dahulu harus melakukan konfigurasi terhadap IDS dan IPS, sehingga IDS dan IPS dapat mengetahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau akan menolak paket tersebut untuk diteruskan (IPS). Untuk metode ini, pengelola jaringan harus terusmenerus memberi tahu IDS dan IPS bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian oleh IDS (Intrusion Detection System) atau IPS (Intrusion Prevention System).

2.2 Suricata

Suricata merupakan IDS yang dapat mendeteksi aktifitas ancaman serangan pada jaringan yang dibantu dengan rules yang telah ada. Cara kerja dari suricata adalah ketika adanya penyerangan suricata akan melakukan pengecekan paket/serangan yang ada melalui rules yang dibuat. Ketika serangan terdeteksi maka suricata akan membuat log serangan yang dilakukan. [4]

2.3 Snorby

Snorby merupakan web interface yang digunakan untuk memonitoring suatu keamanan jaringan komputer dengan tampilan berbasis GUI (Graphical User Interface) yang terintegrasi dengan suricata. Fitur dari snorby adalah dapat menampilkan data kejadian/event serangan dari suricata dalam tampilan grafis. Cara kerja snorby adalah ketika adanya serangan suricata akan membuat file berupa log penyerangan yang terhubung dengan barnyard2. File tersebut adalah file undified2 adalah file notifikasi yang dibuat oleh barnyard2. Setelah log terbuat barnyard2 akan memasukan log tersebut ke dalam database, lalu snorby akan menampilkan log penyerangan pada web interface snorby. [4]

2.4 Barnyard

Barnyard2 adalah aplikasi yang melakukan perekaman data hasil dari serangan pada suricata dan menyimpannya dalam bentuk database yang ditentukan dengan format tersendiri [4].

2.5 Firewall

Firewall adalah suatu aturan yang diterapkan baik terhadap perangkat keras, perangkat lunak ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan filterisasi, membatasi, ataupun menolak suatu koneksi pada jaringan yang dilindunginya dengan jaringan luar lainnya seperti internet (Muammar, 2004).

2.6 DDoS (Distributed Denial of Service)

Dalam serangan DDOS penyerang mengirim paket secara langsung dari komputernya ke target namun alamat pengirim mungkin saja dipalsukan. Ada banyak tools yang tersedia untuk menjalankan serangan ini dengan berbagai macam protocol seperti ICMP, UDP, dan TCP.

BAB III

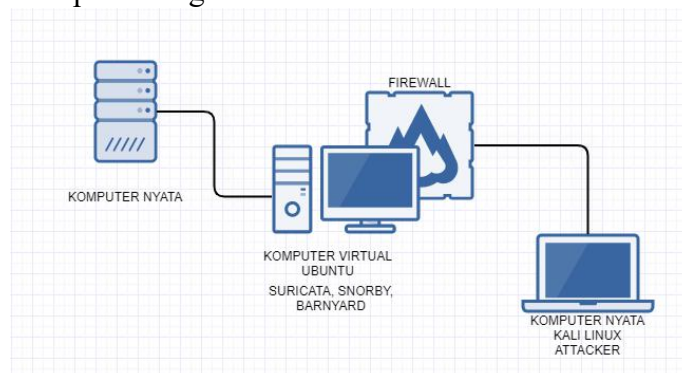
MODEL SISTEM

3.1 Blok Diagram Sistem

Pada bab ini akan dijelaskan mengenai implementasi suricata, snorby barnyard2 terhadap serangan DDoS (*Distributed Denial of Service*). untuk implementasi tersebut dilakukan dengan menggunakan teknologi IPS (*Intrusion Prevention System*) dimana dapat mendeteksi serangan DDoS serta dapat memblock serangan tersebut. Berbeda halnya IDS (*Intrusion Detection System*) yang hanya dapat mendeteksi serangan tanpa memblock serangan yang terdeteksi.

Sistem IPS menggunakan suricata snorby barnyard2 ini diuji menggunakan serangan DDoS dengan bantuan tools HPING3 dan LOIC. IPS (*Intrusion Prevention System*) tersebut akan mendeteksi serangan kedalam sebuah log. Serta memblock serangan ketika rules serangan diaktifkan.

Berikut perancangan skema :



Gambar 3.1. Perancangan IPS

Secara garis besar attacker akan melakukan penyerangan terhadap server yang dimana sudah terinstall suricata snorby barnyard yang sudah di setting sedemikian rupa sehingga dapat mendeteksi serangan. Suricata akan merekam semua kegiatan attacker sedangkan snorby akan memonitoring sistem yang telah dibuat oleh suricata itu sendiri. Log serangan disimpan pada fast.log pada suricata. Untuk barnyard berfungsi sebagai penerjemah alert dan log sistem itu sendiri. Serangan DDoS akan disajikan pada Snorby dalam bentuk grafik.

3.2 Tahapan Perancangan

Proses perancangan dilakukan dengan metode studi literatur dan prosesnya bisa dilihat pada Gambar 3.2 , tahapan pembuatanya adalah sebagai berikut:

1. Studi Literatur

Langkah awal dalam perancangan ini adalah melakukan studi literatur mengenai IPS, DDoS, suricata, snorby, barnyrd2 dan data pendukung lainnya.

2. Penentuan spesifikasi

Langkah selanjutnya yaitu menentukan spesifikasi sistem baik hardware ataupun software. Serta melakukan instalasi sesuai spesifikasi yang dibutuhkan. Berikut spesifikasi *hardware* dan *software* :

Tabel 1. Spesifikasi *hardware*

<i>Hardware</i>	Keterangan
ASUS X441U	Sistem Operasi : Windows 10 Home 64 bit Prosesor : Intel Core i3-6006U 2.0 GHz RAM : 4GB DDR3L

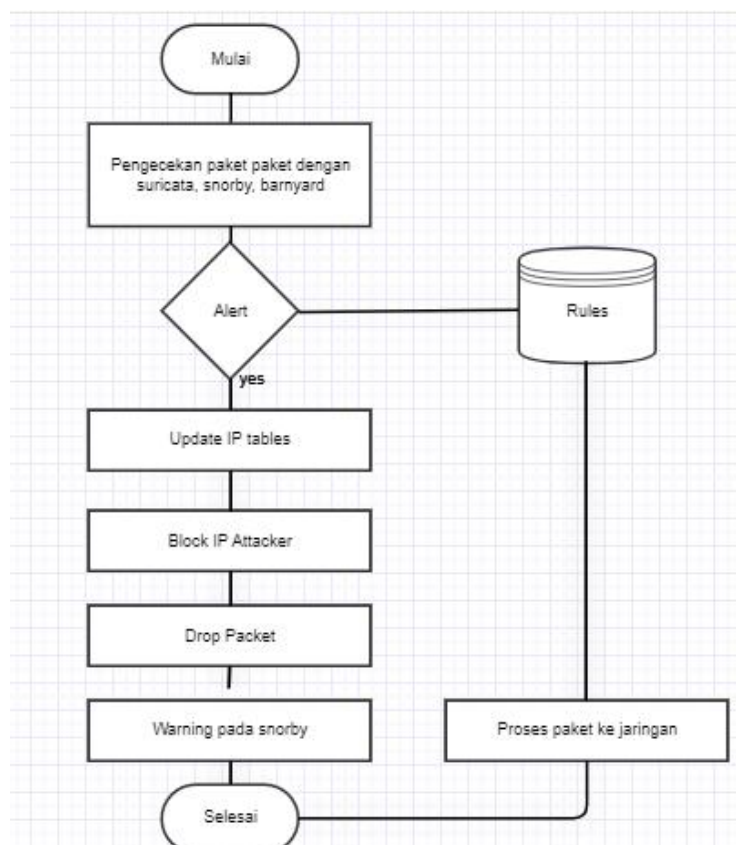
<i>Software</i>	Keterangan
Ubuntu 18.04	Sistem Operasi yang digunakan untuk IPS
Kali linux	Sistem Operasi yang digunakan untuk sebagai penyerang / <i>attacker</i>
Suricata	Perangkat lunak yang digunakan untuk mendeteksi serangan
Snorby	Perangkat lunak yang digunakan untuk menampilkan notifikasi melalui web interface

Barnyard	Perangkat lunak yang digunakan untuk membuat alert menjadi database dan dimasukkan kedalam database Snorby
HPING3	Sebagai jenis serangan yang digunakan.
Nmap	Perangkat lunak yang digunakan untuk melakukan port scanning pada server target.
Brute force	Sebagai jenis serangan yang digunakan

3. Perancangan sistem

Pada perancangan ini dilakukan dari awal pengecekan paket sampai memblokir paket yang teridentifikasi sebagai ancaman.

Dari tahapan utama diatas, ada beberapa tahapan pendukung dan jika dibuat *flowchart* adalah sebagai berikut:



Gambar 3.2 Perancangan Sistem

Pada perancangan sistem ini, dimulai dari instalasi suricata, snorby, barnyard2 sebagai sistem pengaman dari DDoS. Tahap selanjutnya yaitu mengkonfigurasi suricata, snorby, barnyard2 dengan rules yang telah ditentukan. Jika suatu paket terdeteksi sebagai ancaman, maka paket tersebut akan terupdate dalam IP Tables lalu akan d block melalui snorby. Jika paket yang diterima bukan ancaman, maka lalu lintas paket lancar. Paket yang terdeteksi ancaman tersebut akan teridentifikasi oleh snorby pada interface. Dan dapat di analisis paket yang masuk termasuk dalam ancaman sedang atau ancaman berat.

BAB IV

BENTUK KELUARAN YANG DIHARAPKAN

4.1 Keluaran yang Diharapkan

Perancangan pada Proyek Akhir akan dibuat dengan spesifikasi sebagai berikut :

1. Dapat menginstall serta konfigurasi sistem pendeteksi serangan *Intrusion Prevention System* (IPS) dengan suricata, snorby, barnyard2.
2. Sistem dapat melakukan pencegahan terhadap paket yang terdeteksi sebagai serangan DDoS.
3. Pengujian pada sistem dengan melakukan simulasi serangan DDoS.

4.2 Jadwal Pelaksanaan

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

Tabel 4.1 Jadwal Pelaksanaan

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

DAFTAR PUSTAKA

- [1] Istiana Adesty, "Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service (DDoS)," 2020.
- [2] Bagas Suryo Anggoro, "Implementasi Intrusion Prevention System Suricata dengan Anomaly-Based untuk Keamanan Jaringan PT. Grahamedia Informasi," 2019.
- [3] Satri Bagus Pribadi, "IMPLEMENTASI SURICATA UNTUK MENINGKATKAN KEAMANAN PADA CLOUD COMPUTING," 2019.
- [4] Sofyan Hadi, Periyadi, S.T., M.T., "Implementasi Network Intrusion Detection System pada Sistem Smart Identification," 2016.
- [5] M. K. S. M. Alim Nuryanto, "ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2," 2015.

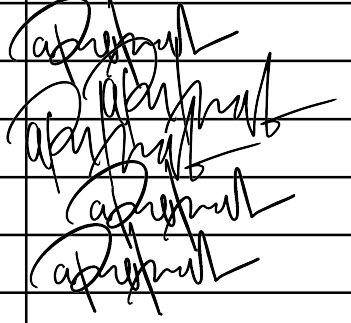
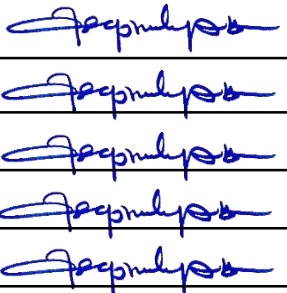


UNIVERSITAS TELKOM
FAKULTAS ILMU TERAPAN
KARTU KONSULTASI
SEMINAR PROPOSAL PROYEK AKHIR

NAMA / PRODI : HASNATUL HUSNI / D3 TEKNOLOGI
TELEKOMUNIKASI NIM : 6705184106
JUDUL PROYEK AKHIR : PENERAPAN SURICATA SNORBY BARNYARD2 SEBAGAI PENGAMAN DARI
SERANGAN DISTRIBUTED DENIAL OF SERVICE (DDoS)

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	22/01/2021	BAB 1 (SELESAI)	
2	22/01/2021	BAB 2 (SELESAI)	
3	22/01/2021	BAB 3 (SELESAI)	
4	22/01/2021	BAB 4 (SELESAI)	
5	22/01/2021	FINALISASI PROPOSAL	
6			
7			
8			
9			
10			
NO	TANGGAL	CATATAN HASIL KONSULTASI	TANDA TANGAN CALON PEMBIMBING II
1	21/01/2021	BAB 1 (SELESAI)	
2	21/01/2021	BAB 2 (SELESAI)	
3	21/01/2021	BAB 3 (SELESAI)	
4	21/01/2021	BAB 4 (SELESAI)	
5	21/01/2021	FINALISASI PROPOSAL	
6			
7			
8			
9			
10			