

**IMPLEMENTASI MEDIUM INTERACTION HONEYPOT
MENGUNAKAN COWRIE UNTUK MENDETEKSI
SERANGAN BRUTE FORCE PADA SOFTWARE
DEFINED NETWORK (SDN)**

PRA PROPOSAL PROYEK TINGKAT

Diajukan sebagai syarat untuk mengikuti Sidang Komite Proyek tingkat

oleh :

ARIFIAN RAMADHAN

6705184057



**D3 TEKNOLOGI TELEKOMUNIKASI
FAKULTAS ILMU TERAPAN
UNIVERSITAS TELKOM**

2020

Latar Belakang

Perkembangan teknologi pada industri 4.0 sudah menunjukkan peningkatan lalu lintas jaringan internet yang signifikan, disamping fenomena tersebut serangan terhadap keamanan jaringan komputer juga meningkat, salah satu serangan yang sering terjadi atau sering dilakukan oleh peretas adalah brute force attack. Jenis serangan brute force adalah serangan yang bertujuan untuk membobol otentikasi sistem dengan menggunakan setiap password yang memungkinkan dengan kata lain serangan ini mencoba menggunakan password yang acak, metode brute force attack cukup banyak, mulai dari yang sederhana sampai melakukan crack password yang tersimpan pada database.

Software-Defined Network (SDN) adalah teknologi pada arsitektur jaringan yang memudahkan manajemen perangkat yang ada pada suatu jaringan. Dalam jaringan konvensional, router menerapkan semua algoritma routing dan memutuskan bagaimana proses forwarding suatu paket. Pada arsitektur SDN, fungsi routing dan fungsi forwarding dipisahkan.

Berdasarkan data dari F5 yang merupakan salah satu perusahaan global yang bergerak di bidang aplikasi dan keamanan, disebutkan bahwa serangan yang paling sering digunakan oleh penyerang adalah serangan brute force yang jumlah kemunculannya 2,7 kali lebih tinggi dari serangan HTTP dan tiga kali lebih tinggi dibandingkan dengan serangan terhadap layanan telnet.

Berdasarkan penelitian tersebut, diperlukan adanya sistem keamanan jaringan untuk mendeteksi dari serangan brute force, salah satunya yaitu dengan menggunakan honeypot. Honeypot sendiri adalah suatu cara membuat sistem palsu atau layanan palsu yang berfungsi untuk menjebak pengguna yang mempunyai tujuan buruk atau menangkal usaha-usaha yang dapat merugikan sistem atau layanan, honeypot sendiri terdiri dari beberapa macam yaitu; low interaction honeypot, medium interaction honeypot dan high interaction honeypot, disini menggunakan medium interaction honeypot, honeypot jenis ini memberikan ilusi dari operasi sistem palsu yang dapat berkomunikasi dengan penyerang. Kemudian melakukan pencatatan aktivitas dari si penyerang. Cowrie adalah salah satu contoh dari medium interaction honeypot. Cowrie adalah interaksi medium SSH dan Telnet honeypot yang dirancang untuk mencatat serangan brute force dan interaksi shell yang dilakukan oleh penyerang. Cowrie juga berfungsi sebagai proxy SSH dan telnet untuk mengamati perilaku penyerang ke sistem lain. SSH adalah program paket yang dapat bertindak sebagai pengganti yang

aman untuk rlogin, rsh, dan rcp. SSH menggunakan kriptografi kunci publik untuk mengenkripsi komunikasi antara dua host, dan juga digunakan untuk otentikasi pengguna.

Studi Literatur Penelitian Terkait

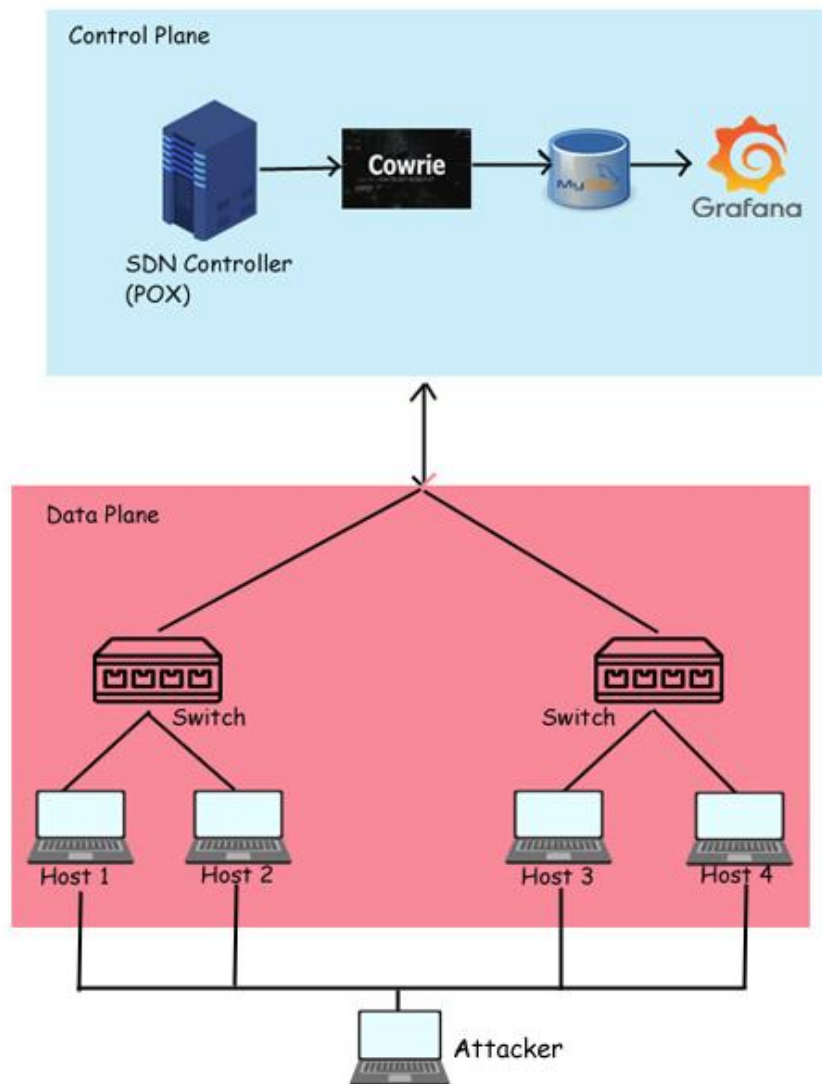
Tabel 1 Merupakan hasil studi literature terhadap penelitian yang terkait dengan judul yang diangkat.

No	Judul Penelitian / Karya Ilmiah	Tahun	Keterangan
1	Honeypot Cowrie Implementation to Protect SSH Protocol in Ubuntu Server with Visualisation Using Kippo-Graph [1]	2019	Pada penelitian ini pemateri mengimplementasikan Honeypot Cowrie pada Ubuntu server kemudian melakukan konfigurasi menggunakan software PuTTY agar hasil serangan dapat divisualisasikan menggunakan Kippo-Graph
2	Implementasi Honeypot Sebagai Sistem Keamanan Jaringan pada Virtual Private Server [2]	2020	Dalam penelitian tersebut pemateri mengimplementasikan Honeypot Cowrie pada Virtual Private Server
3	Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack [3]	2016	Pada penelitian tersebut proses brute force menggunakan program Aplikasi Scanning, maka dengan cara ini dapat dilihat secara jelas proses yang terjadi ketika sebuah website di serang dengan proses brute force .
4	Implementasi Sistem Monitoring Menggunakan Prometheus dan Grafana [4]	2020	Penelitian tersebut mengimplementasikan Grafana untuk melakukan monitoring server
5	Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur SoftwareDefined Network (SDN) [5]	2019	Penelitian tersebut mengimplementasikan sistem deteksi serangan DDOS menggunakan Machine Learning SVM Classifier pada SDN dengan menggunakan 6 switch pada software mininet

6	Perancangan Simulasi Jaringan Virtual Berbasis Software-Define Networking [6]	2016	Pada artikel tersebut dilakukan simulasi jaringan virtual berbasis SDN dengan menggunakan 2, 4, 8, 16 switch dan menganalisis parameter QOS (Quality Of service) yang diperoleh
---	---	------	---

Sistem Perancangan

Pada bab ini akan dijelaskan mengenai perancangan medium interaction Honeypot menggunakan Cowrie untuk mendeteksi dan mencegah serangan bruteforce pada jaringan SDN. Adapun model sistem yang telah dibuat dapat dilihat pada gambar dibawah ini.



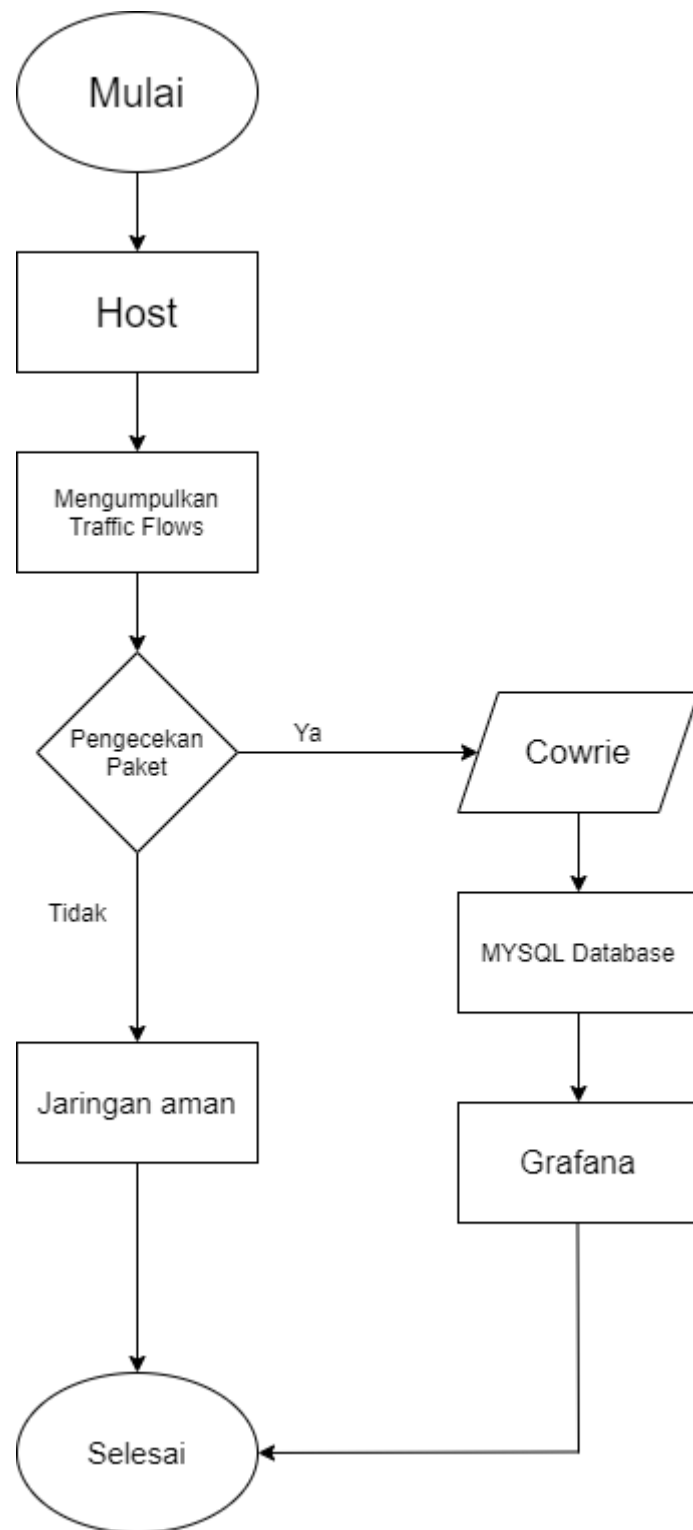
Gambar 1. Model sistem perancangan

Skenario pengujian akan dilakukan dengan melakukan serangan dari komputer attacker kepada komputer korban atau host.

Sesuai pada gambar terdapat 2 bagian pada jaringan SDN yaitu control plane dan data plane. Control plane berfungsi sebagai otak jaringan, dimana terdapat controller yang akan bertanggung jawab atas perilaku keseluruhan jaringan seperti

mekanisme routing, manajemen flow, mengatur prioritas paket, dan sebagainya. Dalam penelitian ini, controller yang digunakan yaitu POX yang merupakan controller berbasis bahasa pemrograman python. Lalu ada data plane yang terdapat komponen openflow switch, yang terhubung dengan controller. Controller akan memberi perintah kepada switch dalam melakukan forwarding. Masing-masing switch akan terhubung dengan host yang diantaranya terdapat host.

Kemudian pada control plane akan melakukan konfigurasi honeypot cowrie. Konsep pada cowrie adalah pengalihan, yaitu setelah openssh diserang, cowrie akan mengarahkan attacker untuk masuk pada layanan palsu honeypot, sehingga attacker akan mengira bahwa penyerangan tersebut telah berhasil, padahal attacker hanya masuk dalam perangkap honeypot. Pada fitur cowrie terdapat log dan logging. Logging adalah suatu proses untuk mencatat semua kegiatan yang dilakukan attacker yang terjadi pada sistem honeypot. Fitur Logging inilah yang akan digunakan sebagai output cowrie yang akan dikirim ke MYSQL database melalui konfigurasi pada Ubuntu, kemudian hasil output yang sudah tersimpan pada MYSQL database akan divisualisasikan menggunakan Grafana, pada grafana akan menampilkan sesuai dengan output dari cowrie, untuk mengkonfigurasi MYSQL database dengan Grafana menggunakan Ubuntu dan pada saat sudah masuk ke dashboard Grafana terdapat Data source MYSQL yang dapat menampilkan data dari database.



Gambar 2. Flowchart Sistem Penyerangan

Tools untuk Pengukuran

- Honeypot Cowrie

Cowrie adalah interaksi medium SSH dan Telnet honeypot yang dirancang untuk mencatat serangan brute force dan interaksi shell yang dilakukan oleh penyerang.

- MYSQL Database

MySQL adalah sistem manajemen database relasional open source (RDBMS) dengan client-server model. Sedangkan **RDBMS** merupakan software untuk membuat dan mengelola database berdasarkan pada model relasional.

- Grafana

Grafana adalah analitik sumber terbuka multi-platform dan aplikasi web visualisasi interaktif. Ini menyediakan bagan, grafik, dan peringatan untuk web saat terhubung ke sumber data yang didukung.

- Ubuntu

Ubuntu merupakan salah satu distribusi Linux yang berbasis Debian dan didistribusikan sebagai perangkat lunak bebas. Ubuntu ditawarkan dalam tiga edisi resmi: Ubuntu Desktop untuk komputer pribadi, Ubuntu Server untuk server dan komputasi awan, dan Ubuntu Core untuk "Internet untuk Segala", perangkat kecil dan robot.

- Kali Linux

Kali Linux adalah distro turunan Debian dan juga penerus BackTrack yang digunakan untuk melakukan penetrasi pada jaringan. Kali Linux memiliki lebih dari 300 perkakas yang ada di dalamnya dengan fungsi masing-masing.

- Mininet

Mininet adalah emulator berbasis CLI yang digunakan untuk membuat topologi jaringan Software Defined Network (SDN).

- POX Controller

POX adalah sebuah platform pengembangan perangkat lunak SDN Controller berbasis bahasa pemrograman Python. POX memiliki beberapa komponen yang dapat digunakan dan digabung untuk membentuk SDN Controller sesuai kebutuhan pengguna.

Referensi

- [1] A. R. Devi Afriyantari Puspa Putri, "Honeypot Cowrie Implementation to Protect SSH Protocol in Ubuntu Server with Visualisation Using Kippo-Graph," *International Journal of Advanced Trends in Computer Science and Engineering*, 2019.
- [2] W. A. Sulaksono, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *Jurnal Nasional Informatika dan Teknologi Jaringan*, 2020.
- [3] H. S. Pratita, "Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack," Repository UKSW, Salatiga, 2016.
- [4] R. M. Febriana, "IMPLEMENTASI SISTEM MONITORING MENGGUNAKAN PROMETHEUS DAN GRAFANA," 2020.
- [5] Izzatul Ummah, Desianto Abdillah, "Perancangan Simulasi Jaringan Virtual Berbasis Software-Define Networking," *Ind. Journal on Computing*, 2016.
- [6] Jodi Chris Jordan Sihombing, Dany Primanita Kartikasari, Adhitya Bhawiyuga, "Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur SoftwareDefined Network (SDN)," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2019.

Form Kesiediaan Membimbing Proyek Tingkat


PROYEK TINGKAT SEMESTER GANJIL|GENAP* TA 2020/2021




Tanggal	: 11 Desember 2020	
Kami yang bertanda tangan dibawah ini:		
CALON PEMBIMBING 1		
Kode	: RMT	
Nama	: Rohmat Tulloh, S.T., M.T.	
CALON PEMBIMBING 2		
Kode	: ASM	
Nama	: Asep Mulyana, S.T.,M.T.	
Menyatakan bersedia menjadi dosen pembimbing Proyek Tingkat bagi mahasiswa berikut,		
NIM		: 6705184057
Nama		: Arifian Ramadhan
Prodi / Peminatan		: TT/Keamanan Jaringan
Calon Judul PA		:
		IMPLEMENTASI MEDIUM INTERACTION HONEYPOT MENGGUNAKAN COWRIE UNTUK MENDETEKSI SERANGAN BRUTE FORCE PADA SOFTWARE DEFINED NETWORK (SDN)

Dengan ini akan memenuhi segala hak dan kewajiban sebagai dosen pembimbing sesuai dengan Aturan Proyek Tingkat yang berlaku.

Calon Pembimbing 1

11-Dec-20

(Rohmat Tulloh, S.T.,M.T.)
NIP: 06830002

Calon Pembimbing 2


(Asep Mulyana, S.T.,M.T.)
NIP: 945700113

CATATAN:

1. Aturan Proyek Akhir versi terbaru dapat diunduh dari : <http://dte.telkomuniversity.ac.id/panduan-proyek-akhir/>
2. Keputusan akhir penentuan pembimbing berada di tangan Ketua Kelompok Keahlian dengan memperhatikan aturan yang berlaku.
3. Pengajuan pembimbing boleh untuk kedua pembimbing sekaligus atau untuk salah satu pembimbing saja



Telkom University
 Jl. Telekomunikasi No.1, Terusan Buah Batu
 Bandung 40257
 Indonesia

DAFTAR NILAI HASIL STUDI MAHASISWA

NIM (Nomor Induk Mahasiswa) : 6705184057
 Nama : ARIFIAN RAMADHAN

Dosen Wali : TAR / TENGKU AHMAD RIZA
 Program Studi : D3 Teknologi Telekomunikasi

Mata Kuliah yang Lulus

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
1	DTH1F3	DASAR SISTEM TELEKOMUNIKASI	BASIC TELECOMMUNICATIONS SYSTEM	3	C
1	DTH1C3	DASAR TEKNIK KOMPUTER DAN PEMROGRAMAN	BASIC COMPUTER ENGINEERING AND PROGRAMMING	3	AB
1	DTH1A2	K3 DAN LINGKUNGAN HIDUP	K3 AND ENVIRONMENT	2	AB
1	DUH1A2	LITERASI TIK	ICT LITERACY	2	AB
1	DTH1B3	MATEMATIKA TELEKOMUNIKASI I	MATHEMATICS TELECOMMUNICATIONS I	3	C
1	HUH1A2	PENDIDIKAN AGAMA DAN ETIKA - ISLAM	RELIGIOUS EDUCATION AND ETHICS - ISLAM	2	AB
1	DTH1D3	RANGKAIAN LISTRIK	ELECTRICAL CIRCUITS	3	AB
1	DTH1E2	BENGKEL MEKANIKAL DAN ELEKTRIKAL	MECHANICAL AND ELECTRICAL WORKSHOP	2	B
2	LUH1B2	BAHASA INGGRIS I	ENGLISH I	2	AB
2	DMH1A2	OLAH RAGA	SPORT	2	A
2	DTH1G3	MATEMATIKA TELEKOMUNIKASI II	MATHEMATICS TELECOMMUNICATIONS II	3	B
2	DTH1H3	TEKNIK DIGITAL	DIGITAL TECHNIQUES	3	B
2	DTH1I3	ELEKTRONIKA ANALOG	ANALOG ELECTRONIC	3	BC
2	DTH1J2	BENGKEL ELEKTRONIKA	ELECTRONICS WORKSHOP	2	B
2	DTH1K3	ELEKTROMAGNETIKA	ELECTROMAGNETIC	3	C
2	HUH1G3	PANCASILA DAN KEWARGANEGARAAN	PANCASILA AND CITIZENSHIP	3	AB
Jumlah SKS				78	3.11

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
3	DTH2G3	SISTEM KOMUNIKASI OPTIK	OPTICAL COMMUNICATION SYSTEMS	3	C
3	DTH2B3	KOMUNIKASI DATA BROADBAND	BROADBAND DATA COMMUNICATIONS	3	AB
3	DTH2C2	BENGKEL INTERNET OF THINGS	INTERNET OF THINGS WORKSHOP	2	AB
3	DTH2A2	BAHASA INGGRIS TEKNIK I	ENGLISH TECHNIQUE I	2	AB
3	DTH2D3	APLIKASI MIKROKONTROLER DAN ANTARMUKA	MICROCONTROLLER APPLICATIONS AND INTERFACES	3	AB
3	DTH2F3	TEKNIK TRANSMISI RADIO	RADIO TRANSMISSION TECHNIQUES	3	C
4	DMH1B2	PENGEMBANGAN PROFESIONALISME	PROFESSIONAL DEVELOPMENT	2	A
4	DTH2M3	SISTEM KOMUNIKASI SELULER	CELLULAR COMMUNICATION SYSTEMS	3	AB
4	DTH2L3	TEKNIK ANTENNA DAN PROPAGASI	ANTENNA TECHNIQUES AND PROPAGATION	3	B
4	DTH2K3	ELEKTRONIKA TELEKOMUNIKASI	ELECTRONICS TELECOMMUNICATIONS	3	AB
4	DTH2J2	TEKNIK TRAFIK	TRAFFIC ENGINEERING	2	AB
4	DTH2I3	DASAR KOMUNIKASI MULTIMEDIA	BASIC COMMUNICATION MULTIMEDIA	3	AB
4	DTH2H3	JARINGAN DATA BROADBAND	BROADBAND DATA NETWORK	3	B
4	DMH2A2	KERJA PRAKTEK	INTERSHIP	2	A
Jumlah SKS				78	3.11

Mata Kuliah yang Belum Lulus

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
3	VTI2G3	PENGOLAHAN SINYAL INFORMASI	INFORMATION SIGNAL PROCESSING	2	
3	VTI2C3	PERANGKAT TELEKOMUNIKASI BROADBAND	BROADBAND TELECOMMUNICATION DEVICES	3	
3	DTH2E3	SISTEM KOMUNIKASI	COMMUNICATIONS SYSTEMS	3	E
4	UKI2C2	BAHASA INDONESIA	INDONESIAN LANGUAGE	2	
Jumlah SKS				23	

Semester	Kode Mata Kuliah	Mata Kuliah	Nama Mata Kuliah B. Inggris	SKS	Nilai
4	VTI2H2	BAHASA INGGRIS TEKNIK II	ENGLISH TECHNIQUES II	2	
4	VTI2K3	JARINGAN TELEKOMUNIKASI BROADBAND	BROADBAND DATA NETWORKS	3	
5	VTI3D3	KEAMANAN JARINGAN	NETWORK SECURITY	3	
5	UWI3E1	HEI	HEI	1	
5	VTI3E2	CLOUD COMPUTING	CLOUD COMPUTING	2	
5	UWI3A2	KEWIRAUSAHAAN	ENTREPRENEURSHIP	2	
Jumlah SKS				23	

Tingkat I	: 41 SKS	Belum Lulus	IPK : 3
Tingkat II	: 81 SKS	Belum Lulus	IPK : 2.99
Tingkat III	: 81 SKS	Belum Lulus	IPK : 2.99
Jumlah SKS	: 78 SKS		IPK : 2.99

Total SKS dan IPK dihitung dari mata kuliah lulus dan mata kuliah belum lulus. Nilai kosong dan T tidak diikutkan dalam perhitungan IPK.

Pencetakan daftar nilai pada tanggal 10 Desember 2020 23:16:46 oleh ARIFIAN RAMADHAN