

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

*Implementation Honeypot using Cowrie to Detect Brute force Attack on Software Defined
Network (SDN)*

PROPOSAL PROYEK AKHIR

Diajukan sebagai syarat untuk mengikuti seminar proposal Proyek akhir

**oleh :
ARIFIAN RAMADHAN 6705184057**



**D3 TEKNOLOGI TELEKOMUNIKASI
FAKULTAS ILMU TERAPAN
UNIVERSITAS TELKOM
2021**

LEMBAR PENGESAHAN

Proposal Proyek Akhir dengan judul :

IMPLEMENTASI HONEYPOT MENGGUNAKAN COWRIE UNTUK MENDETEKSI
SERANGAN BRUTE FORCE PADA SOFTWARE DEFINED NETWORK (SDN)

*Implementation Honeypot using Cowrie to Detect Brute force Attack on Software Defined
Network (SDN)*

oleh :

ARIFIAN RAMADHAN

6705184057

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
Arifian Ramadhan

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

NIP. 06830002

Pembimbing II



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

NIP. 945700113

ABSTRAK

Software Defined Network (SDN) adalah suatu metode atau paradigma yang memisahkan antara *Control Plane* dan *Forwarding Plane*. Pada jaringan tradisional atau jaringan non-SDN, kedua fungsi diatas berada dalam satu perangkat yang sama. Dalam dunia jaringan istilah SDN sudah cukup dikenal, hal ini juga diperlukan sistem keamanan untuk jaringan SDN, seperti salah satunya yaitu serangan *bruteforce*, Jenis serangan ini bertujuan untuk membobol otentikasi sistem dengan menggunakan setiap password yang memungkinkan dengan kata lain serangan ini mencoba menggunakan password yang acak

Untuk mengatasi ancaman serangan tersebut diperlukan adanya sistem pertahanan yaitu salah satunya *Honeypot Cowrie*. *Honeypot cowrie* sendiri merupakan suatu cara membuat sistem palsu atau layanan palsu yang berfungsi untuk menjebak pengguna yang melakukan penyerangan *bruteforce* dan interaksi *shell*. Perancangan topologi SDN menggunakan *POX Controller* dan akan terhubung ke *host* melalui *switch*, kemudian pada *controller* akan diintegrasikan dengan sistem *honeypot cowrie* dan akan dihubungkan dengan grafana untuk menampilkan data yang diperoleh dari serangan *bruteforce* yang dilakukan oleh penyerang menggunakan *nmap*, *metasploit* dan *medusa* pada *kali linux*.

Pada *honeypot cowrie* akan menyimpan sebuah data serangan terhadap *port ssh* yang kemudian data tersebut akan ditampilkan melalui *grafana*, adapun data yang diharapkan yaitu; Jumlah alamat unik *IP*, periode penyerangan dan data *IP* yang menyerang.

Kata kunci: *software defined network, honeypot, cowrie, bruteforce*

DAFTAR ISI

LEMBAR PENGESAHAN	i
ABSTRAK.....	ii
DAFTAR ISI.....	iii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Tujuan dan Manfaat	3
1.3 Rumusan Masalah	3
1.4 Batasan Masalah	3
1.5 Metodologi	3
BAB II DASAR TEORI	4
2.1 <i>Software Defined Network</i>	4
2.2 <i>Honeypot</i>	5
2.3 <i>Cowrie</i>	5
2.4 <i>Brute force attack</i>	6
BAB III PERANCANGAN	7
3.1 Blok sistem	7
3.2 Spesifikasi perangkat	8
3.3 Tahapan Perancangan	8
3.4 Flowchart sistem	9
3.5 Sistem serangan	10
BAB IV BENTUK KELUARAN YANG DIHARAPKAN	11
4.1 Keluaran yang diharapkan	11
DAFTAR PUSTAKA	12

BAB I

PENDAHULUAN

1.1 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.

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.

Adapun penelitian terkait yang menjadi referensi dalam pembuatan proyek akhir ini:

1. HoneyPot Cowrie Implementation to Protect SSH Protocol in Ubuntu Server with Visualisation Using Kippo-Graph (2019)

Pada penelitian ini penerji mengimplementasikan HoneyPot Cowrie pada Ubuntu server kemudian melakukan konfigurasi menggunakan software PuTTY agar hasil serangan dapat divisualisasikan menggunakan Kippo-Graph, peneliti tidak menggunakan sistem operasi Ubuntu secara langsung melainkan menggunakan Ubuntu server. [1]

2. Implementasi Sistem Deteksi dan Mitigasi Serangan Distributed Denial of Service (DDoS) menggunakan SVM Classifier pada Arsitektur Software Defined Network (SDN) (2019)

Penelitian tersebut mengimplementasikan sistem deteksi serangan DDOS menggunakan Machine Learning SVM Classifier pada SDN dengan menggunakan 6 switch pada software mininet, penelitian dilakukan hanya simulasi menggunakan software mininet tidak mengimplementasikan SDN itu sendiri. [2]

3. Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack (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, penelitian tidak menggunakan sistem honeypot sehingga serangan bruteforce akan masuk ke sistem asli tidak akan terperangkap ke sistem honeypot. [3]

4. Implementasi HoneyPot Sebagai Sistem Keamanan Jaringan pada Virtual Private Server (2020)

Dalam penelitian tersebut penerji mengimplementasikan HoneyPot Cowrie pada Virtual Private Server, hasil penelitian tidak divisualisasikan sehingga data serangan hanya berupa logging pada honeypot cowrie. [4]

Perbedaan proyek akhir ini dengan penelitian diatas adalah dengan pengimplementasian SDN dan penggabungan antara sistem honeypot dengan SDN.

1.2 Tujuan dan Manfaat

Adapun tujuan dari Proyek tingkat ini, sebagai berikut:

1. Dapat merancang topologi Software Defined Network dengan menggunakan POX Controller
2. Dapat mengintegrasikan Honeypot Cowrie pada Software Defined Network
3. Mampu mengimplementasikan penyerangan bruteforce dengan kali linux pada topologi SDN
4. Dapat menampilkan data penyerangan pada Grafana

Adapun manfaat dari proyek akhir ini, sebagai berikut:

1. Sebagai penunjang keamanan pada topologi Software Defined Network
2. Sebagai penelitian terhadap sistem honeypot

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek tingkat ini, sebagai berikut:

1. Bagaimana merancang topologi Software Defined Network dengan menggunakan POX Controller
2. Bagaimana mengintegrasikan Honeypot Cowrie pada Software Defined Network
3. Bagaimana mengimplementasikan penyerangan bruteforce pada topologi Software Defined Network
4. Bagaimana menampilkan data penyerangan pada grafana

1.4 Batasan Masalah

Dalam Proyek tingkat ini, dilakukan pembatasan masalah sebagai berikut:

1. Perancangan topologi Software Defined Network dengan menggunakan POX Controller
2. Sistem penyerangan menggunakan teknik bruteforce
3. Penampilan data penyerangan menggunakan grafana

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.

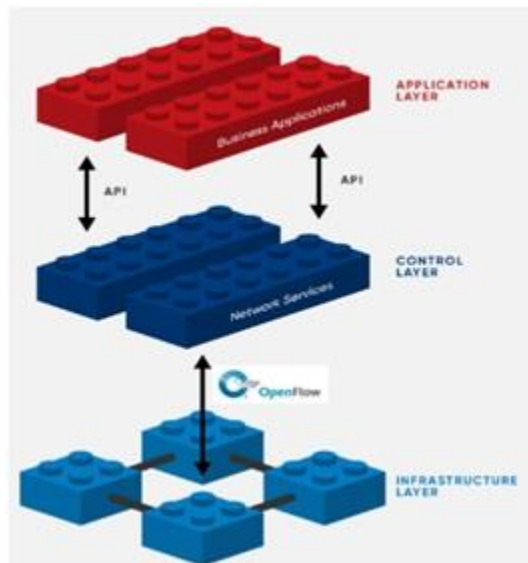
BAB II

DASAR TEORI

2.1 *Software Defined Network*

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.

Konsep dasar dari Software Defined Networking adalah melakukan pemisahan fisik antara *Control Plane* dan *Forwarding Plane*. Secara logika, control plane diletakkan secara terpusat yang membutuhkan sebuah sistem operasi jaringan yang mampu membentuk peta logika (*logical map*) dari seluruh jaringan dan kemudian memrepresentasikannya melalui sejenis API (*Application Programming Interface*).



Gambar 1 Arsitektur SDN

Arsitektur SDN (Software Defined Networking) terbagi menjadi 3 layer, yaitu:

- Application Layer

Berisi aplikasi network yang digunakan dalam sebuah perusahaan yang mencakup IDS(Intrusion Detection System), load balancing atau firewall. Apabila jaringan tradisional menggunakan alat tambahan untuk menambah fitur tersebut, maka pada SDN mengganti cara tersebut dengan sebuah aplikasi yang menggunakan controller untuk mengatur data plane.

- Control Layer

SDN Controller mentranslasikan kebutuhan antara aplikasi dan infrastruktur dengan memberikan instruksi yang sesuai dengan SDN Datapath dan relevan dengan SDN Application.

- Infrastructure Layer

Mengatur SDN Datapath sesuai dengan instruksi yang diberikan melalui Control-Data-Plane Interface (CDPI). [5]

2.2 *Honeypot*



Gambar 2 Honeypot

Honeypot 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. [1]

2.3 *Cowrie*



Gambar 3 Cowrie

Cowrie adalah interaksi medium SSH dan Telnet honeypot yang dirancang untuk mencatat serangan brute force dan interaksi shell yang dilakukan oleh penyerang. Pertama, cowrie perlu memanipulasi port server SSH dengan mengkonfigurasi port asli

yang digunakan 22 menjadi 8975. Kemudian, perlu redirect server SSH dari port 22 ke sistem cowrie di port 2222. [1]

2.4 *Brute force attack*



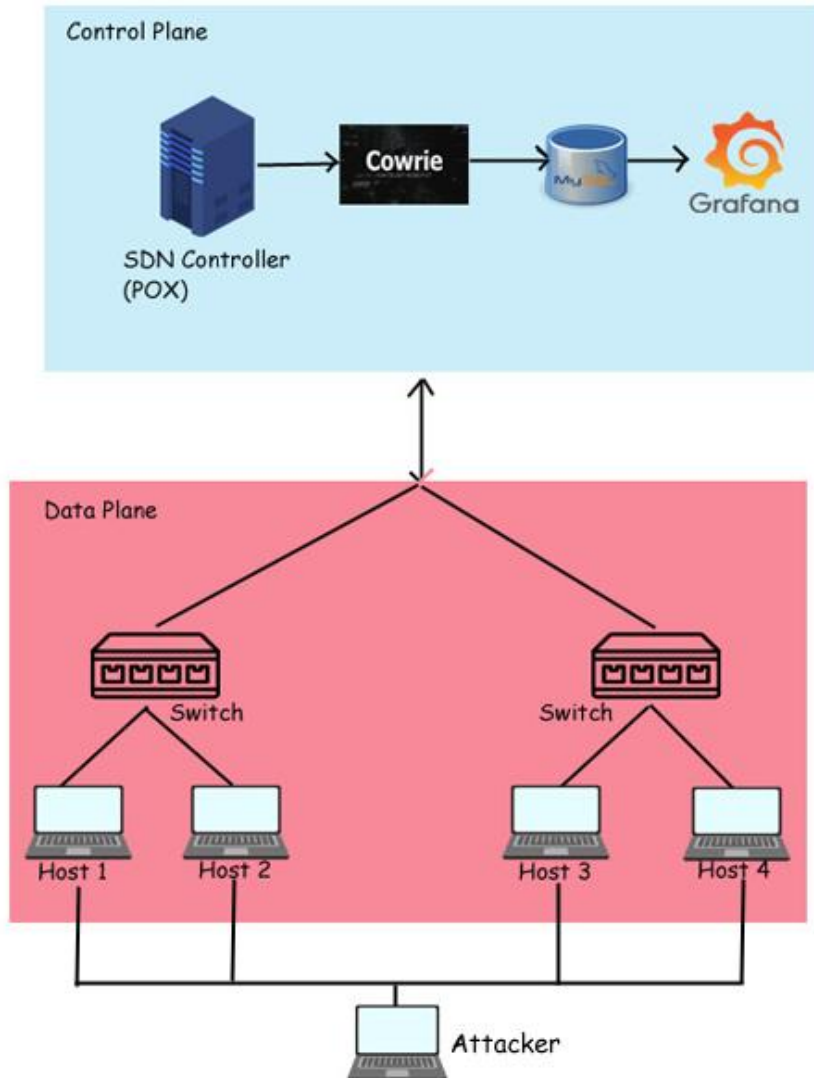
Gambar 4 Brute force attack

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. [3]

BAB III

PERANCANGAN

3.1 Blok sistem



Gambar 5 Blok sistem implementasi honeypot cowrie pada SDN

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.

3.2 Spesifikasi perangkat

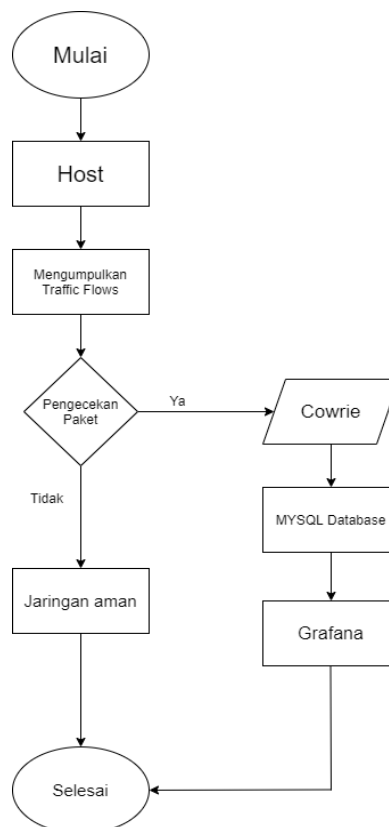
- 2 Switch
- 1 laptop/PC sebagai controller
- 5 laptop/PC sebagai host dan penyerang
- POX Controller
- Ubuntu 18.04
- Kali linux 2019.2
- Honeypot cowrie
- Grafana
- Nmap
- Metasploit
- Medusa

3.3 Tahapan Perancangan

Tahapan perancangan diawali dengan membuat topologi Software Defined Network (SDN), lalu mengintegrasikan Honeypot Cowrie pada SDN tersebut

1. Perancangan Topologi Software Defined Network
Pada proyek akhir ini akan dirancang topologi Software Defined Network dengan menggunakan 2 buah switch dan 1 buah laptop/PC sebagai controller dan juga 4 laptop/PC sebagai host yang akan terhubung pada switch, controller yang digunakan yaitu POX Controller
2. Penginstallan Honeypot Cowrie pada Controller di Topologi SDN
Penginstallan Honeypot Cowrie dilakukan pada controller SDN, yang kemudian akan terintegrasi dengan setiap host yang terhubung pada switch
3. Visualisasi data serangan menggunakan Grafana
Setelah Honeypot Cowrie terintegrasi, kemudian akan dilakukan pengaturan agar data serangan dapat ditampilkan pada grafana. Pada cowrie, hasil output akan dikirim ke database MYSQL lalu database tersebut akan ditampilkan pada grafana.

3.4 Flowchart sistem



Gambar 6 Flowchart sistem

3.5 Sistem serangan

Skenario serangan yaitu dengan bruteforce attack, pada laptop/PC penyerang menggunakan nmap, metasploit dan medusa pada kali linux untuk melakukan bruteforce attack. Nmap, Metasploit, dan medusa merupakan framework yang dapat digunakan untuk melakukan skenario serangan brute force. Kerangka tersebut secara otomatis dipasang di sistem operasi linux. Pada nmap akan dilakukan port scanning kemudian akan dilakukan serangan bruteforce pada port ssh menggunakan metasploit dan medusa.

BAB IV

BENTUK KELUARAN YANG DIHARAPKAN

4.1 Keluaran yang diharapkan

Bentuk keluaran yang diharapkan adalah output data yang akan ditampilkan pada grafana, yaitu:

1. Jumlah alamat unik IP
Alamat IP penyerang akan terakumulasikan dan ditampilkan pada grafana
2. Periode penyerangan
Pada grafana akan terlihat periode penyerangan, misalnya dalam 7 hari terakhir terdapat serangan
3. Data IP yang menyerang
IP penyerang akan terbaca pada cowrie dan dapat ditampilkan pada grafana

DAFTAR PUSTAKA

- [1] A. R. Devi Afriyanti Puspita 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] Jodi Chris Jordan Sihombing, Dany Pramanita 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.
- [3] H. S. Pratita, "Analisa Brute Force Attack menggunakan Scanning Aplikasi pada HTTP Attack," Repository UKSW, Salatiga, 2016.
- [4] W. A. Sulaksono, "Implementasi Honeypot Sebagai Sistem Keamanan Jaringan Pada Virtual Private Server," *Jurnal Nasional Informatika dan Teknologi Jaringan*, 2020.
- [5] Christan, E. Wijaya and B. Kanigoro, "Bina Nusantara University School of Science," Bina Nusantara, [Online]. Available: <https://socs.binus.ac.id/2018/12/10/software-defined-networking-sdn/>. [Accessed 5 12 2020].



UNIVERSITAS TELKOM
FAKULTAS ILMU TERAPAN
KARTU KONSULTASI
SEMINAR PROPOSAL PROYEK AKHIR

NAMA / PRODI : ARIFIAN RAMADHAN / D3TT



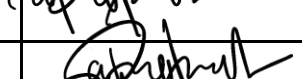
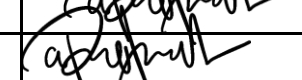
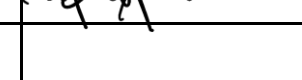

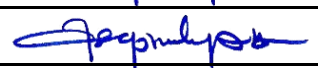
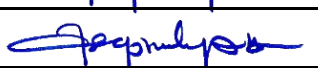
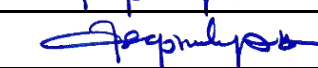
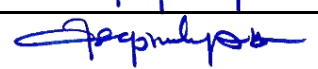
NIM : 6705184057

JUDUL PROYEK AKHIR :

IMPLEMENTASI HONEYPOT MENGGUNAKAN COWRIE UNTUK MENDETEKSI SERANGAN
BRUTE FORCE PADA SOFTWARE DEFINED NETWORK (SDN)

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			