

**PENGUJIAN EVIL TWIN PADA JARINGAN BERBASIS  
WIRELESS DENGAN NODEMCU ESP 8266 PADA  
PT PUPUK SRIWDJAJA PALEMBANG**



Skripsi

Diajukan sebagai syarat untuk memperoleh Gelar Sarjana Komputer pada  
Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah  
Palembang

Oleh :

**Syndi Anggriani**

**162019013**

**PROGRAM STUDI TEKNOLOGI INFORMASI  
FAKULTAS TEKNIK  
UNIVERSITAS MUHAMMADIYAH PALEMBANG  
2023**

## HALAMAN PENGESAHAN

**PENGUJIAN EVIL TWIN PADA JARINGAN BERBASIS WIRELESS DENGAN  
NODEMCU ESP 8266 PADA PT PUPUK SRIWIDJAJA PALEMBANG**

Oleh :

**Syndi Anggriani**

**162019013**

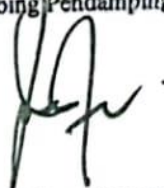
**Telah Diterima Sebagai Salah Satu Syarat Untuk Untuk Memperoleh Gelar Sarjana  
Komputer (S.Kom) Pada Program Studi Teknologi Informati**

Pembimbing Utama



**Meliyana Winda PERDANA, S.Kom., M.Kom.**  
NBM/NIDN: 1295465/0212059002

Pembimbing Pendamping



**Zulhipni Reno Saputra Elsi, S.T., M.Kom.**  
NBM/NIDN: 1338529/0205118002

Disetujui  
Dekan fakultas Teknik



**Prof Dr. Ir Kgs Ahmad Roni, S.T.M.T.IPM.ASEAN, Eng**  
NBM/NIDN: 763049/0227077004

Program Studi Teknologi Informasi  
Ketua Program Studi,



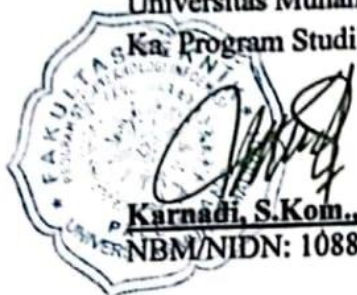
**Karnadi, S.Kom., M.Kom**  
NBM/NIDN: 1088893/0210038202

## HALAMAN PERSETUJUAN

Judul Skripsi : **PENGUJIAN EVIL TWIN PADA JARINGAN BERBASIS WIRELESS DENGAN NODEMCU ESP 8266 PADA PT PUPUK SRIWDJAJA PALEMBANG"**

Oleh Syndi Anggriani Nim 162019013 skripsi ini telah disetujui dan disahkan oleh tim penguji Program Studi Teknologi Informasi konsentrasi Manajemen Tata Kelola Teknologi Informasi, program strata I Universitas Muhammadiyah Palembang pada tanggal, 9 agustus 2023 dan dinyatakan LULUS

Mengetahui, Program Strata I  
Universitas Muhammadiyah Palembang  
Ka. Program Studi Teknologi Informasi,



**Karnadi, S.Kom., M.Kom.**  
NBM/NIDN: 1088893/0210038202

Tim Penguji :  
Ketua,

**Meilyana Winda P.S.Kom., M.Kom**  
NBM/NIDN: 1295465/0212059002  
Sekertaris

**Zulhifni Reno S E, S.T., M.Kom**  
NBM/NIDN: 340253/022204770  
Penguji I,

**Karnadi, S.Kom., M.Kom**  
NBM/NIDN: 1088893/0210038202  
Penguji II,

**Jimmie, S.Kom., M.Kom**  
NBM/NIDN: 1338529/0205118002

## HALAMAN PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Syndi Anggriani

NIM : 162019013

Dengan ini saya menyatakan bahwa :

1. Karya tulis saya (Skripsi) merupakan sebuah karya asli serta belum pernah diajukan untuk memperoleh gelar akademik dengan baik (Sarjana) di Program Studi Teknologi Informasi Fakultas Teknik Universitas Muhammadiyah Palembang atau perguruan tinggi lainnya.
2. Karya tulis saya (Skripsi) merupakan hasil murni memiliki gagasan, pokok, permasalahan serta hasil penilaian saya sendiri, tanpa kerja sama terhadap pihak lain melainkan dengan arahan dosen pembimbing.
3. Karya tulis saya (Skripsi) tidak terdapat karya serta pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali serta tertulis dengan jelas dicantumkan nama pengarang serta memasukkan kedalam daftar Pustaka.
4. Karya tulis saya (Skripsi) yang dihasilkan sudah melakukan pengecekan dengan keasliannya menggunakan plagirisme checker yang dipublikasikan melalui internet sehingga bisa diakses secara daring.
5. Dengan ini surat pernyataan yang saya buat secara sungguh-sungguh serta apabila terbukti terdapat penyimpangan serta ketidakbenaran dari pernyataan, maka saya bersedia menerima sanksi sesuai dengan peraturan serta perundang-undang akademik Program Studi di Fakultas Teknik Universitas Muhammadiyah Palembang.

Demikian surat pernyataan ini saya buat agar dapat dipergunakan sebagaimana mestinya.

Palembang, 29 Agustus 2023  
Yang membuat pernyataan


Syndi Anggriani  
Nim : 162019013

## **MOTTO DAN PERSEMBAHAN**

### **MOTTO**

Perbanyak bersyukur, kurangi mengeluh, buka mata, perluas hati. Nikmati  
setiap momen dalam hidup

### **PERSEMBAHAN**

Tidak bisa dipungkiri telah banyak orang yang telah membantu penulis selama menyelesaikan Skripsi penelitian ini, maka dari itu izinkan penulis untuk mempersembahkan Skripsi ini kepada orang-orang yang telah membantu penulis:

- ❖ Untuk Ibu tercinta (Nurhayati) yang selalu memberikan doa, nasihat, materi, semangat, dan motivasi kepada penulis, sehingga penulis dapat menyelesaikan skripsi ini.
- ❖ Untuk Ayah (Isnanto) yang menjadi pacuan untuk sukses.
- ❖ Untuk kakak dan adik kandung saya (Toto, Thomas, Tommy), yang selalu memberikan doa, nasihat, motivasi, dan semangat, sehingga penulis dapat menyelesaikan skripsi ini.
- ❖ Untuk dosen pembimbing penulis Ibu Meilyana Winda, S.Kom.M.Kom sebagai pembimbing I dan Bapak Zulhipni Reno, S.Kom.M.Kom sebagai pembimbing II, yang selalu mempermudah urusan penulis dan memberikan dorongan agar penulis menjadi orang yang selalu berusaha.
- ❖ Untuk sahabat-sahabatku yang telah memberikan semangat, doa, dan motivasi dalam menyelesaikan skripsi ini.

## ABSTRAK

Pengujian Evil Twin Pada Jaringan Berbasis Wireless dengan nodemcu esp 8266 Pada PT Pupuk Sriwidjaja Palembang bertujuan untuk menguji keamanan pada jaringan berbasis wireless dengan nodemcu ESP 2866 di PT Pupuk sriwidjaja. Metode pengembangan sistem yang digunakan dalam skripsi ini adalah *Network Development Life Cycle* (NDLC) Metode pengembangan system ini mencakup semua prosedur dan juga teknik penelitian serta langkah-langkah penting untuk menyelesaikan suatu masalah dengan baik. NDLC merupakan sebuah siklus proses perancangan teknik analisis terstruktur yang digunakan untuk merencanakan dan mengelola proses pengembangan sistem. Adapun tahapan siklus metodologi NDLC yakni meliputi analysis, design, simulation prototyping, implementation, monitoring dan management. Adapun hasil dari penelitian pengujian evil twin pada jaringan berbasis wireless dengan nodemcu esp 8266 pada Pt pupuk sriwdjaja Palembang yaitu pengujian evil twin pada jaringan berbasis *wireless* dengan cara mematikan akses poin dan kemudian membuat tiruan akses poin target yang telah dimatikan sebelumnya, yang dima ketika pengguna AP asli masuk ke AP palsu maka akan di arahkan ke halaman login di mana terdapat perintah memasukan kata sandi maka ketika pengguna memasukan kata sandi bisa terbaca di acses poin palsu. Maka Dapat dipastikan jaringan wireless yang menggunakan keamanan WPA2-PSK dapat dikatakan belum aman karena masih terdapat celah.

**Kata kunci:** evil twin , jaringan *wireless*, WPA2

## **ABSTRACT**

*Evil Twin Testing on Wireless-Based Networks with nodemcu esp 8266 at PT Pupuk Sriwidjaja Palembang aims to test security on wireless-based networks with nodemcu ESP 2866 at PT Pupuk Sriwidjaja. The system development method used in this thesis is the Network Development Life Cycle (NDLC). This system development method includes all procedures and research techniques as well as important steps to solve a problem properly. NDLC is a structured analysis design process cycle used to plan and manage the system development process. The stages of the NDLC methodology cycle include analysis, design, simulation prototyping, implementation, monitoring and management. The results of the research on testing evil twins on wireless-based networks with nodemcu esp 8266 at Pt Pupuk Sriwdjaja Palembang, namely testing evil twins on wireless-based networks by turning off access points and then making clones of target access points that have been turned off before, which is when AP users the original enters the fake AP, it will be directed to the login page where there is a command to enter a password, so when the user enters the password, it can be read on the fake access points. So you can be sure that wireless networks that use WPA2-PSK security cannot be said to be secure because there are still loopholes.*

**Keywords:** *evil twin , wireless network, WPA2*

## **KATA PENGANTAR**

Dengan segala kerendahan hati, penulis mengucapkan puji dan syukur kepada Tuhan Yang Maha Esa atas rahmat dan karunia-Nya penulisan Tugas Akhir ini dapat diselesaikan. Penulisan tugas akhir ini bertujuan untuk memenuhi salah satu syarat dalam menyelesaikan mata kuliah Skripsi Penelitian. Adapun tugas akhir ini berjudul “Pengujian Evil Twin Pada Jaringan Berbasis Wireless Dengan Nodemcu Esp 8266 Pada Pt Pupuk Sriwdjaja Palembang”.

Dalam penyusunan tugas akhir ini, penulis menyadari bahwa masih banyak kekurangan. Hal ini disebabkan keterbatasan kemampuan yang penulis miliki. Namun demikian, penulis akan tetap berusaha untuk memperbaiki diri lebih baik lagi dimasa yang akan datang. Penulis ingin menyampaikan terima kasih yang sebesar-besarnya pada semua pihak, yaitu kepada

Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Bapak Dr. Abid Djazuli, S.E., M.M. selaku Rektor Universitas Muhammadiyah Palembang.
2. Bapak Prof. Dr. Ir. Kiagus Ahmad Roni, S.T, MT., IPM. ASEAN Eng. selaku Dekan Fakultas Teknik Universitas Muhammadiyah Palembang.
3. Bapak Karnadi,S.Kom.,M.Kom. selaku Kaprodi Teknologi Informasi.
4. Ibu Meilyana Winda Perdana S. Kom.,M.Kom selaku pembimbing Utama yang telah memberikan saran dan kritik yang sifatnya membangun sangat penulis



harapkan. Semoga karya Skripsi Penelitian ini bermanfaat dan dapat memberikan sumbangan yang berarti bagi pihak yang membutuhkan.

5. Bapak Zulhipni Reno, S. Kom., M.Kom selaku pembimbing Pendamping, Saran dan kritik yang sifatnya membangun sangat penulis harapkan. Semoga karya Skripsi Penelitian ini bermanfaat dan dapat memberikan sumbangan yang berarti bagi pihak yang membutuhkan.
6. Bapak Dan Ibu Kandungku selaku orang tua.

Palembang, 29 Agustus 2023



Syndi anggriani  
Nim : 162019013

## DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PENGESAHAN.....	ii
HALAMAN PERSETUJUAN.....	iii
HALAMAN PERNYATAAN.....	iv
MOTTO DAN PERSEMBAHAN.....	v
ABSTRAK.....	vi
ABSTRAK.....	vii
KATA PENGANTAR.....	viii
DAPFTAR ISI.....	ix
DAPFTAR GAMBAR.....	xii
DAPFTAR TABEL.....	xiv
<b>BAB I PENDAHULUAN.....</b>	<b>1</b>
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah .....	3
1.3 Rumusan Masalah .....	3
1.4 Batasan Masalah.....	4
1.5 Tujuan Penelitian.....	4
1.6 Manfaat Penelitian.....	4
1.6.1Bagi Mahasiswa.....	4
1.6.2 Bagi Universitas .....	4
1.6.3 Bagi Perusahaan .....	5
1.7 Sistematika Penulisan.....	5
<b>BAB II TINJAUAN PUSTAKA.....</b>	<b>Error! Bookmark not defined.</b>
2.1 Evil Twint.....	<b>Error! Bookmark not defined.</b>
2.2 Nodemcu 8266 .....	<b>Error! Bookmark not defined.</b>

2.3 Wireless fidelity.....	<b>Error! Bookmark not defined.</b>
2.4 Keamanan Jaringan WPA2-PSK.....	<b>Error! Bookmark not defined.</b>
2.5 Profil PT Pupuk Sriwidjaja Palembang.....	<b>Error! Bookmark not defined.</b>
2.6 Network Development Life Cycle (NDLC).....	<b>Error! Bookmark not defined.</b>
2.7 Penelitian sebelumnya.....	<b>Error! Bookmark not defined.</b>
<b>BAB III MOTODE PENELITIAN.....</b>	<b>Error! Bookmark not defined.</b>
3.1 Waktu Penelitian .....	<b>Error! Bookmark not defined.</b>
3.2 Tempat Penelitian.....	<b>Error! Bookmark not defined.</b>
3.3 Jadwal Penelitian.....	<b>Error! Bookmark not defined.</b>
3.4 Kerangka kerja penelitian.....	<b>Error! Bookmark not defined.</b>
3.5 Metode Pengumpulan Data .....	<b>Error! Bookmark not defined.</b>
3.6 Metode Pengembangan Sistem.....	<b>Error! Bookmark not defined.</b>
3.7 Sistem Yang Sedang Berjalan .....	<b>Error! Bookmark not defined.</b>
3.9 Rancangan topologi jaringan.....	<b>Error! Bookmark not defined.</b>
<b>BAB IV HASIL DAN PEMBAHASAN .....</b>	<b>37</b>
4.1 Analisis Kebutuhan .....	<b>37</b>
4.2 simulasi prototpe .....	<b>41</b>
4.3 implementasi .....	<b>41</b>
4.4 monitoring .....	<b>48</b>
<b>BAB V PENUTUP.....</b>	<b>55</b>
5.1 Kesimpulan.....	<b>55</b>
5.2 Saran .....	<b>55</b>
<b>DAFTAR PUSTAKA .....</b>	<b>56</b>

## DAFTAR GAMBAR

<b>Gambar 2.1</b> Ilustrasi Metode Evil .....	6
<b>Gambar 2.2</b> flowchart melakukan evil twin .....	8
<b>Gambar 2.3</b> NodeMCU .....	9
<b>Gambar 2.4</b> Topologi WPA2-PSK .....	13
<b>Gambar 2.5</b> Metode Network Development Life Cycle (NDLC) .....	16
<b>Gambar 3.1</b> kerangka penelitian .....	29
<b>Gambar 3.2</b> sistem yang sedang berjalan .....	33
<b>Gambar 3.3</b> Alur penyerangan .....	34
<b>Gambar 3.4</b> Topologi jaringan .....	35
<b>Gambar 3.5</b> Rancangan Serangan Evil Twin.....	35
<b>Gambar 3.6</b> Ilustrasi serangan evil twin .....	35
<b>Gambar 4.1</b> Nodecmu.....	38
<b>Gambar 4.2</b> Antena.....	39
<b>Gambar 4.3</b> Case Tenda .....	39
<b>Gambar 4.4</b> USB .....	40
<b>Gambar 4.5</b> Evil Twin .....	40
<b>Gambar 4.6</b> Operation .....	42
<b>Gambar 4.6</b> Config.....	42
<b>Gambar 4.8</b> Restore Default.....	43
<b>Gambar 4.9</b> Flash .....	43

<b>Gambar 4.10</b> File Esp_code .ino.nodemcu.....	44
<b>Gambar 4.11</b> wifi atmo&power.....	44
<b>Gambar 4.12</b> Gethub .....	45
<b>Gambar 4.13</b> Scan .....	45
<b>Gambar 4.14</b> Attacks .....	46
<b>Gambar 4.15</b> Settings .....	47
<b>Gambar 4.16</b> Download Password .....	48
<b>Gambar 4.17</b> Wifi Target.....	49
<b>Gambar 4.18</b> Pengguna AP Pusri ID.....	49
<b>Gambar 4.19</b> Informasi Wifi .....	50
<b>Gambar 4.20</b> Interface Deauther .....	50
<b>Gambar 4.21</b> attacks .....	51
<b>Gambar 4.22</b> SSID Palsu Dan Asli .....	52
<b>Gambar 4.23</b> Login palsu .....	53
<b>Gambar 4.24</b> Password Masuk .....	53

## Daftar Tabel

<b>Tabel 2.4</b> Penelitian Sebelumnya .....	19
<b>Tabel 3.1</b> Jadwal Penelitian .....	28
<b>Tabel 4.1</b> Perangkat Keras yang digunakan .....	37
<b>Tabel 4.2</b> Perangkat Lunak Yang Digunakan.....	37
<b>Tabel 4.4</b> Tabel Tes login.....	54

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang**

Jaringan komputer telah mengalami perkembangan yang pesat. Seiring dengan munculnya infrastruktur jaringan nirkabel, perlahan jaringan berbasis kabel mulai ditinggalkan. Kebutuhan pengguna jaringan yang terus meningkat membuat penggunanya ingin menggunakan sebuah koneksi yang bisa digunakan dimana saja dan kapan saja. Jaringan nirkabel ini juga populer dengan istilah Wi-Fi atau Wireless Fidelity. Teknologi wireless atau biasa disebut dengan Wi-Fi merupakan fasilitas yang umum digunakan saat ini, selain menyediakan konektivitas yang mudah serta jangkauan yang cukup luas, jaringan tersebut juga menawarkan keamanan kepada penggunanya dimana hanya orang yang mempunyai autentikasi password yang dapat menggunakan fasilitas tersebut. Cakupan penggunaan Wi-Fi yang semakin bertambah luas baik di area perkantoran maupun di publik area.

Wireless Fidelity (Wi-Fi) merupakan teknologi nirkabel yang dapat menghubungkan pengguna dengan internet. Umumnya perangkat ini memancarkan gelombang radio dengan frekuensi 2,4 Ghz dan 5 Ghz tergantung jenis access point yang digunakan [1]. Fasilitas wifi banyak tersedia di beberapa tempat dan dapat dinikmati dengan menggunakan perangkat smartphone, laptop, maupun perangkat yang memiliki dukungan nirkabel lainnya. Ada beberapa tipe keamanan pada wireless sebagai protokol autentikasi yang sah. Salah satunya adalah WPA2-PSK yang menggunakan autentikasi berupa password. Dengan algoritma dua jenis enkripsi yang

dapat digunakan untuk mengamankan jaringan wifi [2]. Dengan demikian pengguna akan berfikir jaringan yang digunakan telah aman karena terdapat enkripsi yang digunakan pada jaringan tersebut.

Beberapa orang memanfaatkan wifi untuk hiburan, untuk kegiatan bisnis seperti membuka e-mail, atau bahkan melakukan transaksi online shop maupun internet banking. Namun faktanya penggunaan wifi ternyata tidak lebih aman dibandingkan dengan penggunaan kabel (Ethernet). Setiap device yang memiliki wireless adapter dapat membaca wifi yang ada di sekitar area nya [3]. Artinya wifi dapat dikatakan tidak aman apabila setiap orang dapat terkoneksi dalam jaringan tersebut hanya dengan menggunakan autentikasi berupa password. Masih ada celah pada sisi user dimana hal tersebut dapat dimanfaatkan hacker untuk masuk ke dalam wifi, dan mencuri data para pengguna yang terkoneksi ke jaringan tersebut [4]. Serangan pada wifi tentunya menjadi ancaman serius bagi para penggunanya. Sebab informasi yang di dapatkan oleh hacker dapat dimanfaatkan untuk kejahatan *cyber* lainnya, seperti pemalsuan identitas atau bahkan menyerang korban secara personal.

Evil Twin merupakan salah satu teknik yang digunakan oleh hacker untuk masuk ke dalam jaringan, dan mendapatkan informasi yang dimiliki korban (Information Harvesting) [5]. Mengakses internet dengan memutus dan mengirimkan SSID (nama Wi-Fi) palsu agar dapat terhubung pada Wi-Fi yg dituju . Evil Twin adalah Service Set Identifier (SSID) palsu yang meniru jaringan Wi-Fi asli . Tiruan ini benar-benar sangat mirip dengan nama jaringan aslinya. kekuatan sinyal, hingga frekuensinya. Pengguna bisa saja menyambungkan perangkatnya ke Wi-Fi Evil Twin



ini karena mengira itu adalah Wi-Fi yang asli. Evil Twin ini bekerja dengan menggunakan teknik penyerangan bernama man-in-the-middle (MITM). Teknik ini memungkinkan pembuat Evil Twin untuk menyuntikkan Malware atau Backdoor. Salah satu praktek Evil Twin terpopuler kepada perangkat pengguna tanpa terdeteksi sama sekali.

Berdasarkan uraian yang telah disampaikan pada latar belakang diatas maka penulis bermaksud melakukan penelitian dengan judul “**Pengujian Evil Twin Pada Jaringan Berbasis Wireless dengan nodemcu esp 8266 Pada PT Pupuk Sriwidjaja Palembang**”

## **1.2 Identifikasi Masalah**

Berdasarkan uraian latar belakang masalah diatas maka dapat di identifikasikan beberapa pokok permasalahan yaitu :

1. Jaringan wireless (Wi-Fi) rentan terhadap serangan kejahatan seperti serangan evil twint
2. Keamanan WPA2-PSK pada Wi-Fi yang menggunakan autentikasi hanya berupa password masih kurang aman, dan memiliki potensi untuk diretas.

## **1.3 Rumusan Masalah**

Berdasarkan pada identifikasi masalah di atas maka dapat dirumuskan beberapa pokok permasalahan yaitu : **Bagaimana pengujian evil twin pada Jaringan Berbasis Wireless dengan nodemcu di PT Pusri ?**

## **1.4 Batasan Masalah**

Adapun batasan masalah yang terdapat pada penelitian ini sebagai berikut :

1. Alat yang digunakan menggunakan nodmcu esp8266
2. Hanya digunakan untuk menyerang *wireless fidelity*

## **1.5 Tujuan Penelitian**

Tujuan yang terdapat pada penelitian ini adalah untuk melakukan pengujian keamanan pada jaringan berbasis wireless dengan nodemcu ESP 2866 di PT Pupuk sriwidjaja.

## **1.6 Manfaat Penelitian**

### **1.6.1 Bagi Mahasiswa**

Manfaat penelitian yang di dapat pada laporan penelitian rancang bangun evil twin portable dengan nodmcu esp8266 untuk melakukan pengujian jaringan berbasis wireless dengan keamanan wpa2-psk

1. Meningkatkan hasil belajar dan Mengembangkan wawasan dalam mengetahui serangan evil twin .
2. Bagi calon peneliti dapat dijadikan bahan referensi untuk penelitian selanjutnya.

### **1.6.2 Bagi Universitas**

1. Sebagai bahan masukan bagi perguruan tinggi untuk menambah referensi sebagai bahan penelitian lanjutan yang lebih mendalam pada masa yang akan datang.
2. Penelitian ini diharapkan dapat memberikan kontribusi penambah ilmu pengetahuan khususnya mahasiswa Universitas Muhammadiyah Palembang.

### **1.6.3 Bagi Perusahaan**

1. Dengan adanya evil twin yang akan di uji di PT. PT tersebut dapat meningkatkan keamanan jaringan agar terhindar dari serangan evil twint.
2. Memahami cara kerja serangan evil twint pengguna WLAN

## **1.7 SISTEMATIKA PENELITIAN**

### **BAB I PENDAHULUAN**

Berisi tentang latar belakang, identifikasi masalah, batasan masalah, perumusan masalah tujuan manfaat penelitian, Wireless fidelity dan sistematika penelitian.

### **BAB II TINJAUAN PUSTAKA**

Bab ini berisikan tinjauan pustaka yang menjelaskan evil twin, Nodemcu 8266, Keamanan Jaringan WPA2-PSK dan penelitian sebelumnya.

### **BAB III METODOLOGI PENELITIAN**

Bab ini membahas tentang manajemen penelitian,waktu penelitian,tempat penelitian, jadwal penelitian ,kerangka penelitian, mtode pengumpulan data, dan metode pengembangan sistem

### **BAB IV HASIL DAN PEMBAHASAN**

Bab ini membahas tentang analisis kebutuhan, simulasi prototype , implementasi, dan monitoring.

### **BAB V PENUTUP**

Bab ini membahas tentang kesimpulan dan saran.

### DAFTAR PUSTAKA

- [1] j. D. A. A. B. amewuda, f. A. katsriku, “implementasi dan evaluasi wlan 802.11ac untuk jaringan perumahan di ns-3 j. komputer. komunitas jaringan,” 2018.
- [2] r. S. G. v. vipin poddar dan jaipur, “analisis perbandingan protokol keamanan nirkabel (wep dan wpa2),” *int. J. jaringan ad hoc. syst.*,” vol. 4, tidak. 3, 2014.
- [3] P. D. v.r. G. v. v. nanavare, “survei tentang teknik deteksi titik akses kembar jahat ,” *int.j. innov. res. komputer. komuni. eng*”, 2016.
- [4] v.:pparek. C. modi, "deteksi titik akses nakal untuk mencegah serangan kembar jahat di jaringan nirkabel," *int. J. eng. res. teknologi.*,” vol. 6, tidak. 4, 2014.
- [5] l. B. A. singh, t. e. kelompok, "peretasan etis (alat, teknik, dan pendekatan)".
- [6] v. wuwung, “mitigasi serangan mitma – evil twin pada jaringan wireless lan (wlan),” vol. volume 10.
- [7] peniarsih, “penerapan evil twin detektor dalam pendeteksian pengganggu jaringan nirkabel pada user,” 2017.
- [8] r. baloch, “ethical hacking and penetration testing guide. new york: auebarch publications. <https://doi.org/10.1201/b17225>,” 2015.
- [9] d. j. afif khairullah, agung susilo yuda irawan, “alat pengacau sinyal wi-fi dengan nodemcu (board v.3 lolin) esp8266 deauther berbasis microcontroller,” *j. ilm. wahana pendidik. 8(10)*, 231-237, no. p-issn: 2622-8327 e-issn: 2089-5364, 2022.

- [10] n. hidayati, "prototype smart home dengan modul nodemcu esp8266 berbasis internet of things(iot)," 2019.
- [11] y. yanti dan z. baihaqi, "implementasi sistem keamanan wpa2 pada jaringan wi-fi," 2018.
- [12] widyanto dan taqrim ibadi hamza alfan suri, "analisis fluxion sebagai program uji keamanan wpa2 pada perangkat wireless," 2016.
- [13] j. t. e. s. m. g. h. wibowo, "eamanan jaringan wlan terhadap serangan wireless hacking pada dinas komunikasi & informatika diy," in prosiding sense," vol. vol 1 no 1, 2017.
- [14] r. p. r.w. ismail, "etode penetration testing pada keamanan jaringan wireless wardriving pt . puma makmur aneka engineering bekas," *j. mhs. bina insa. vol 5 no 1, pp. 53-62*, 2020.
- [15] antoni, "analisis dan pengujian kemanan kelemahan jaringan nirkabel dengan metode evil twin attack pada kali linux," 2012.
- [16] r. r. m. sadikin, "analisa dan pengujian serangan evil twin pada jaringan berbasis wireless dengan keamanan wpa2-psk," 2019.
- [17] a. w. muhammad iqbal nugraha, "rancang bangun sistem keamanan anti evil twin (anet) berbasis raspberry pi," 2021.
- [18] Ayu Tiara Sunja , Meilyana Winda Perdana," Pengembangan jaringan area lokal (LAN) di SMK 1 belitang madang raya"INTERNATIONAL JOURNAL CISTER," VOL. 01 NO. 02 (2022).

- [19]. Karnadi, Taqrim Ibadi "PERANCANGAN JARINGAN LOAD BALANCING DAN MANAJEMEN BANDWIDTH MENGGUNAKAN MIKROTIK DI PT.TASPEN (PERSERO) PALEMBANG"ISSN: 2654-5438.