EVALUASI *PENETRATION TESTING* TERHADAP KERENTANAN JARINGAN WLAN YANG MENGGUNAKAN WPA2

SKRIPSI

Program Studi Sarjana Teknik Elektro

Jurusan Teknik Elektro

Oleh :

NIZAM

NIM. D1021191013

FAKULTAS TEKNIK

UNIVERSITAS TANJUNGPURA

PONTIANAK

2026

HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Nizam

NIM : D1021191013

Menyatakan bahwa dalam SKRIPSI ini yang berjudul " Evaluasi *Penetration Testing* Terhadap Kerentanan Jaringan WLAN Yang Menggunakan WPA2 " tidak terdapat karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu perguruan tinggi manapun. Sepanjang pengetahuan saya, tidak terdapat karya atau pendapat yang pernah ditulis atas diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam Daftar Pustaka.

Demikian pernyataan ini dibuat dengan sebenar-benarnya. Saya sanggup menerima konsekuensi akademis dan hukum di kemudian hari apabila pernyataan yang dibuat ini tidak benar.

Pontianak, 16 April 2026



Nizam
NIM D1021191013

KEMENTERIAN PENDIDIKAN TINGGI, SAINS,
DAN TEKNOLOGI
UNIVERSITAS TANJUNGPURA
FAKULTAS TEKNIK
Jalan Prof. Dr. H. Hadari Nawawi Pontianak 78124
Telepon: (0561) 740186, WA: +6282152280907
Email: ft@untan.ac.id Website: http://teknik.untan.ac.id

SURAT KETERANGAN SELESAI PENULISAN SKRIPSI

Yang bertanda tangan di bawah ini Dosen Pembimbing Utama dan Dosen Pembimbing Pendamping pada penulisan skripsi yang berjudul **"Evaluasi *Penetration Testing* Terhadap Kerentanan Jaringan WLAN Yang Menggunakan WPA2"** yang ditulis oleh mahasiswa Fakultas Teknik Universitas Tanjungpura.

Nama : Nizam

NIM : D1021191013

Jurusan : Teknik

Prodi : Teknik Elektro

Konsentrasi : Telekomunikasi

Demikian ini menerangkan bahwa mahasiswa tersebut telah menyelesaikan penulisan skripsinya.

Pontianak, 16 April 2026

Pembimbing Utama

Leonardus Sandy Ade Putra, S.T., M.T.
NIP. 199410072020121003

Pembimbing Pendamping

Ir. H. Fitri Imansyah, S.T., M.T.,
IPU, ASEAN Eng., ACPE
NIP. 196912271997021001

KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS TANJUNGPURA
FAKULTAS TEKNIK
Jalan Prof. Dr. H. Hadari Nawawi Pontianak 78124
Telepon (0561) 740186, WA: +6282152280907
Email : ft@untan.ac.id Website : http://teknik.untan.ac.id

HALAMAN PENGESAHAN

EVALUASI *PENETRATION TESTING* TERHADAP KERENTANAN JARINGAN WLAN YANG MENGGUNAKAN WPA2

Jurusan Teknik Elektro
Program Studi Sarjana Teknik Elektro

Oleh:

Nizam
NIM D1021191013

Telah dipertahankan di depan Penguji Skripsi pada tanggal 16 April 2026
dan diterima sebagai salah satu persyaratan untuk memperoleh gelar sarjana.

Susunan Penguji Skripsi

Dosen Pembimbing Utama	: Leonardus Sandy Ade Putra, S.T., M.T NIP. 199410072020121003
Dosen Pembimbing Kedua	: Ir. H. Fitri Imansyah, S.T., M.T., IPU, ASEAN Eng., ACPE NIP. 196912271997021001
Dosen Penguji Utama	: Jannus Marpaung, S.T., M.T. IPM NIP. 197307211997021001
Dosen Penguji Kedua	: Dr. Redy Ratiandi Yacoub, S.T., M.T NIP. 197101031997021002

Pontianak, 16 April 2026

Dekan,

Pembimbing Utama

Dr. -Ing. Ir. Slamet Widodo, M.T., IPM
NIP. 196712231992031002

Leonardus Sandy Ade Putra, S.T., M.T.
NIP. 199410072020121003

ABSTRAK

Perkembangan teknologi nirkabel menghadirkan kemudahan akses informasi, namun juga menimbulkan tantangan serius terkait keamanan jaringan. Penelitian ini bertujuan untuk menganalisis tingkat kerentanan *Wireless Local Area Network* (WLAN) dengan menggunakan metode *penetration testing*. Pengujian difokuskan pada protokol keamanan WPA2 yang umum digunakan, dengan skenario serangan berupa *Cracking the Encryption* dan *Man in the Middle Attack* (MITM). Metode penelitian dilakukan melalui serangkaian tahapan mulai dari *network monitoring*, *packet capture*, *deauthentication attack*, hingga upaya *encryption key cracking* menggunakan *Aircrack-ng*. Selain itu, simulasi serangan MITM dilaksanakan dengan memanfaatkan *Ettercap* melalui teknik *ARP poisoning* untuk mengintersepsi komunikasi jaringan. Hasil penelitian menunjukkan bahwa upaya cracking terhadap SSID target tidak berhasil dikarenakan keterbatasan *wordlist*, sedangkan simulasi serangan MITM berhasil memperoleh data sensitif pada jaringan terbuka. Berdasarkan hasil tersebut, dapat disimpulkan bahwa meskipun jaringan WLAN dengan WPA2 memiliki tingkat keamanan lebih baik dibandingkan metode enkripsi sebelumnya, potensi kerentanan masih dapat dimanfaatkan apabila konfigurasi dan kontrol keamanan tidak diperkuat. Oleh karena itu, diperlukan implementasi strategi keamanan tambahan seperti penggunaan kata sandi yang kuat, pembaruan konfigurasi perangkat, serta peningkatan pengawasan jaringan untuk meminimalisasi risiko ancaman siber.

Kata Kunci: *Penetration Testing*, *Cracking the Encryption*, Keamanan Jaringan

ABSTRACT

The rapid development of wireless technology provides convenience in accessing information, yet also raises significant challenges related to network security. This research aims to analyze the vulnerability level of Wireless Local Area Network (WLAN) by applying the penetration testing method. The study focuses on the WPA2 security protocol, with two main attack scenarios: Cracking the Encryption and Man in the Middle Attack (MITM). The methodology involves several stages, including network monitoring, packet capture, deauthentication attack, and encryption key cracking using Aircrack-ng. Additionally, a MITM attack simulation was carried out using Ettercap through ARP poisoning techniques to intercept network communications. The results indicate that the encryption cracking attempt on the target SSID failed due to wordlist limitations, while the MITM simulation successfully intercepted sensitive data on an open network. Based on the findings, it can be concluded that although WPA2 offers stronger protection compared to its predecessors, vulnerabilities may still be exploited if network configuration and security controls are not properly reinforced. Therefore, additional security strategies such as the use of strong passwords, regular device configuration updates, and enhanced network monitoring are recommended to minimize cybersecurity risks.

Keywords: *Penetration Testing, Cracking the Encryption, Network Security*

KATA PENGANTAR

Puji syukur penulis panjatkan kepada Allah Subhanahu Wa Ta'ala, atas berkat rahmat dan kuasa-Nya lah penulis diberikan kesanggupan dan kemudahan sehingga mampu menyusun tugas akhir yang berjudul "Evaluasi *Penetration Testing* Terhadap Kerentanan Jaringan WLAN Yang Menggunakan WPA2" ini dengan baik. Shalawat dan salam semoga tercurahkan kepada nabi Muhammad Shallallahu'Alaihi Wassalam dan kepada keluarganya, Tabi'in, Tabiut Tabi'in serta pengikutnya yang mengikuti beliau hingga akhir zaman.

Dalam penyusunan tugas akhir ini penulis mengalami berbagai hambatan. Namun, semua hal itu dapat dilalui dengan pertolongan Allah Subhanahu Wa Ta'ala melalui bantuan dan bimbingan serta pengarahan dari berbagai pihak sehingga penulis dapat menyelesaikan tugas akhir ini. Pada kesempatan ini penulis ingin mengucapkan terima kasih yang sebesarnya kepada:

1. Dr. Ing. Ir. Slamet Widodo, M.T., IPM selaku Dekan Fakultas Teknik Universitas Tanjungpura Pontianak.
2. Prof. Dr. -Ing. Seno Darmawan Panjaitan, S.T., M.T. IPM selaku Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Tanjungpura.
3. Jannus Marpaung, S.T., M.T. IPM selaku Ketua Program Studi Teknik Elektro Fakultas Teknik Universitas Tanjungpura.
4. Leonardus Sandy Ade Putra, S.T., M.T., selaku Pembimbing Utama yang telah banyak memberikan pengarahan dan bimbingan selama penulisan tugas akhir ini.
5. Ir. H. Fitri Imansyah, S.T., M.T., IPU, ASEAN Eng., ACPE., selaku Pembimbing Pendamping yang telah banyak memberikan pengarahan dan bimbingan selama penulisan tugas akhir ini.
6. Jannus Marpaung, S.T., M.T. IPM selaku Dosen Penguji Utama yang telah memberikan masukan dan kritikan yang membangun untuk menyelesaikan tugas akhir ini.
7. Dr. Redy Ratiandi Yacoub, S.T., M.T., selaku Dosen Penguji Pendamping yang telah memberikan masukan dan kritikan yang membangun untuk menyelesaikan tugas akhir ini.

8. Comdev & Outreaching Universitas Tanjungpura yang telah membiayai kuliah saya melalui program beasiswa Bidikmisi.
9. Kedua orang tua tercinta yang selalu mendoakan dan mendukung dalam segala hal, memberikan motivasi dan nasihat.
10. Sahabat, orang terdekat serta teman-teman yang telah memberikan dukungan, masukan, saran, serta solusi dalam penyelesaian tugas akhir ini yang tidak dapat penulis sebutkan satu per satu.

Penulis menyadari bahwa pada penyusunan tugas akhir ini masih terdapat kekurangan-kekurangan karena keterbatasan kemampuan yang penulis miliki, untuk itu penulis masih mengharapkan kritik dan saran demi perbaikan pada masa yang akan datang

Akhir kata, semoga Tugas Akhir ini dapat memberikan manfaat dalam menambah wawasan serta pengetahuan.

Pontianak, April 2026

Penulis

Nizam
NIM.D1021191013

DAFTAR ISI

ABSTRAK i
ABSTRACT v
KATA PENGANTAR vi
DAFTAR ISI viii
DAFTAR GAMBAR xi
DAFTAR TABEL xii
DAFTAR LAMPIRAN xiii
DARTAR ISTILAH xiv
DAFTAR SINGKATAN xvi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Pembataan Masalah 3
1.5 Sistematika Penulisan 3
BAB II LANDASAN TEORI 5
2.1 Penelitian Terdahulu 5
2.2 Landasan Teori 7
2.2.1 Jaringan Komputer 7
2.2.2 Jaringan *Wireless Local Area Network* (WLAN) 8
2.2.3 Keamanan Wireless LAN 9
2.2.4 Serangan *Wireless* LAN 11
2.2.5 *Protokol Wireless Protected Access* 2 (WPA2) 12
2.2.6 Router 13
2.2.7 *Web Proxy* 14
2.2.8 *Penetration Testing* 15
2.2.9 *Kali Linux* 15
BAB III METODOLOGI PENELITIAN 17
3.1 Diagram Alir Penelitian 17
3.2 Bahan Penelitian 18

3.2 Waktu dan Tempat Penelitian 20
3.3 Metode Penelitian 20
3.3.1 *Cracking The Encryption* 21
3.3.2 *Man In The Middle Attack* (MITM) 23
3.4 Variabel atau Data 25
3.5 Analisa Hasil 26
3.5.1 Analisis Pengujian *Cracking The Encryption* 26
3.5.2 Analisis Pengujian *Man-In-The-Middle* (MITM) *Attack* 27
BAB IV HASIL DAN PEMBAHASAN 28
4.1 Deskripsi Umum Hasil Pengujian 28
4.2 Proses Pengujian *Cracking The Encryption* Terhadap *Access Point ftuntan* Menggunakan *aircrack-ng* 29
4.2.1 *Network Monitoring* 29
4.2.2 *Target Selection* 31
4.2.3 *Packet Capture* 31
4.2.4 Deauthentication Attack 32
4.2.5 *Encryption Key Cracking* 33
4.3 Hasil dan Analisa Pengujian *Cracking The Encryption* Terhadap *Access Point ftuntan* Menggunakan *aircrack-ng* 33
4.3.1 Analisis Pengujian Terkontrol 36
4.4 Proses Pengujian *Man In The Middle Attack* Terhadap Tingkat Keamanan Website 38
4.4.1 *Enable IP Forwarding* 38
4.4.2 Pilih *Target* 39
4.4.3 *ARP Poisoning* 39
4.5 Analisa Pengujian *Man In The Middle Attack* Terhadap Website Kategori HTTP 40
4.6 Analisa Pengujian *Man In The Middle Attack* Terhadap Website Kategori HTTPS 41
4.7 Hasil Pengujian *Penetration Testing* 42
4.7.1 Analisis *Cracking The Encryption* 43
4.7.2 Analisis *Man-In-The-Middle* (MITM) *Attack* 43
BAB V PENUTUP 44

5.1 Kesimpulan 44
5.2 Saran..... 45
DARTAR PUSTAKA 46
LAMPIRAN A PROSES PENGAMBILAN DATA..... A-1
LAMPIRAN B DARTAR WORDLIST YANG DIGUNAKAN..... B-1

DAFTAR GAMBAR

Gambar 2. 1 Konfigurasi WLAN 9
Gambar 2. 2 Tampilan Kali Linux 16
Gambar 3. 1 Diagram Alir Penelitian 17
Gambar 3. 2 Logo Virtual Box 19
Gambar 3. 3 USB TP-Link TL-WN722N 20
Gambar 3. 4 Labolatorium Telekomunikasi Fakultas Teknik 20
Gambar 3. 5 Gambaran Alur Kerja *Cracking The Encryption* 21
Gambar 3. 6 Gambaran Alur Kerja *Man In The Middle* Attack 23
Gambar 4. 1 *Command Network Monitoring* 29
Gambar 4. 2 Hasil *Network Monitoring* 29
Gambar 4. 3 *Command Packet Capture* 31
Gambar 4. 4 Hasil *Packet Capture* 32
Gambar 4. 5 *Command Deauthentication Attack* 32
Gambar 4. 6 Hasil WPA *Handshake* 33
Gambar 4. 7 *Command Encryption Key Cracking* 33
Gambar 4. 8 Hasil *Encryption Key Cracking* 34
Gambar 4. 9 *Four-Way Handshake* WPA/WPA2 36
Gambar 4. 10 Kunci WPA2 *Handshake* dengan Status "KEY FOUND" 37
Gambar 4. 11 *Command Enable IP Forwarding* 38
Gambar 4. 12 Proses *ARP Poisoning* 39
Gambar 4. 13 Hasil *ARP Poisoning* 40
Gambar 4. 14 Tampilan Login Techpanda.org 41

DAFTAR TABEL

Tabel 2. 1 Tabel Penelitian Terdahulu 5
Tabel 2. 2 Konsep Keamanan 10
Tabel 2. 3 Syarat Keamanan 11
Tabel 3. 1 Variabel dan Kebutuhan Data Spesifikasi Pengujian 25
Tabel 4. 1 Hasil *Network Monitoring* 30
Tabel 4. 2 100 Sampel *Wordlist* 35
Tabel 4. 3 *Wordlist* dalam Skenario Pengujian Terkontrol 37
Tabel 4. 4 Hasil *Ettercap* 40
Tabel 4. 5 Hasil *Penetration Testing* 42

DAFTAR LAMPIRAN

LAMPIRAN A PROSES PENGAMBILAN DATA..... A-1
LAMPIRAN B DARTAR WORDLIST YANG DIGUNAKAN..... B-1

DARTAR ISTILAH

Cracking	:	Upaya membobol sistem keamanan untuk merusak, mengambil, atau mencuri data.
Enkripsi	:	Proses teknis mengubah data atau informasi menjadi kode rahasia agar tidak dapat dibaca oleh pihak yang tidak berwenang.
Flowchart	:	Diagram alir yang menggambarkan langkah-langkah suatu proses atau sistem secara visual menggunakan simbol-simbol standar.
Hacking	:	Kegiatan memanfaatkan kelemahan dalam sistem komputer atau jaringan untuk mendapatkan akses tidak sah.
Handshake	:	Proses pertukaran paket data antara perangkat pengguna dan *Access Point* untuk memvalidasi kunci enkripsi sebelum koneksi terjalin.
Monitoring	:	Proses pengawasan aktivitas dan lalu lintas data yang terjadi di dalam suatu jaringan.
Packet Capture	:	Tahap pengambilan atau akuisisi paket data yang melintasi jaringan untuk keperluan analisis.
Penetration Testing	:	Metode evaluasi keamanan siber yang dilakukan dengan mensimulasikan serangan nyata untuk menemukan celah keamanan.
Phishing	:	Teknik penipuan untuk mendapatkan informasi sensitif pengguna seperti kata sandi atau data pribadi.
Sniffing	:	Praktik menyadap atau memantau lalu lintas data yang mengalir melalui jaringan komputer.
Spoofing/Poisoning	:	Teknik pemalsuan identitas atau data (seperti alamat MAC atau IP) dalam jaringan untuk mengalihkan lalu lintas data.

Wordlist/Dictionary	:	Daftar kumpulan kata sandi umum atau kustom yang digunakan sebagai database referensi dalam serangan brute-force.

DAFTAR SINGKATAN

AP (*Access Point*)	:	Perangkat keras yang bertindak sebagai jembatan untuk menghubungkan perangkat nirkabel ke jaringan lokal.
ARP (*Address Resolution Protocol*)	:	Protokol yang digunakan untuk memetakan alamat IP ke alamat fisik (MAC address) dalam jaringan lokal.
BSSID (*Basic Service Set Identifier*)	:	Identitas fisik unik (MAC Address) dari sebuah *Access Point*.
ESSID (*Extended Service Set Identifier*)	:	Nama identitas dari jaringan nirkabel yang biasa dikenal oleh pengguna sebagai nama WiFi.
HTTP (*Hypertext Transfer Protocol*)	:	Protokol pengiriman data antara browser dan server yang tidak terenkripsi (teks biasa).
HTTPS (*Hypertext Transfer Protocol Secure*)	:	Protokol pengiriman data yang telah dilengkapi keamanan enkripsi TLS/SSL.
IEEE (*Institute of Electrical and Electronics Engineers*)	:	Organisasi internasional yang menetapkan standar teknis, termasuk standar 802.11 untuk WiFi.
IP (*Internet Protocol*)	:	Address Alamat logis unik yang diberikan kepada setiap perangkat dalam jaringan komputer.
MITM (*Man-In-The-Middle*)	:	Jenis serangan di mana penyerang memposisikan diri di tengah-tengah komunikasi antara dua pihak.
OS (*Operating System*)	:	Sistem operasi yang mengelola perangkat keras dan perangkat lunak pada komputer.
OSCP (*Offensive Security Certified Professional*)	:	Sertifikasi profesional internasional di bidang pengujian penetrasi keamanan siber.
WLAN (*Wireless Local Area Network*)	:	Jaringan komputer lokal yang menggunakan teknologi nirkabel untuk berkomunikasi.

WPA2 (*Wi-Fi Protected Access 2*)	:	Standar keamanan jaringan nirkabel yang menggunakan enkripsi AES untuk melindungi data.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi semakin lama semakin maju dengan pesat mendorong manusia untuk menciptakan teknologi baru yang dapat lebih bermanfaat dan mempermudah pekerjaan manusia. Tentunya perkembangan teknologi tersebut akan membuat laju informasi di dunia ini semakin cepat. Laju informasi yang begitu cepatnya membuat manusia harus mampu mengolah berbagai informasi yang ada untuk memperoleh suatu hasil data yang diinginkan. Perkembangan teknologi komunikasi ini juga didukung dengan semakin meningkatnya kemajuan infrastruktur dan teknologi komunikasi dan informasi ini adalah komunikasi menggunakan *wireless*. Ini ditandai dengan perkembangan munculnya peralatan nirkabel yang telah menggunakan standar protokol *Wireless Fidelity* (WiFi) yang berbasiskan standar IEEE 802.11.[1] Penggunaan jaringan yang semakin luas di dunia bisnis dan pertumbuhan kebutuhan penggunaan internet online services yang semakin cepat mendorong untuk memperoleh keuntungan dari *shared data* dan *shared resources*. [2]

Pengguna di seluruh dunia memanfaatkan *Wifi* untuk beragam tujuan, mencakup sektor pendidikan, bisnis, dan perdagangan, bahkan adopsinya telah meluas hingga ke kalangan anak-anak. Namun, penggunaan *Wifi* tidak lepas dari berbagai risiko keamanan, seperti *phishing, sniffing, hacking, cracking*, dan bentuk kejahatan siber lainnya. [3] Ancaman-ancaman ini dapat muncul baik untuk tujuan pengujian sistem maupun untuk tindakan tidak bertanggung jawab, seperti pencurian data atau penyalahgunaan hak akses. Potensi serangan terhadap sistem, data, dan jaringan kapan saja menimbulkan rasa ketidakamanan bagi pengguna. Oleh karena itu, implementasi keamanan jaringan yang efektif menjadi krusial untuk mencegah dan menanggulangi berbagai ancaman tersebut.

Universitas Tanjungpura sebagai salah satu institusi pendidikan tinggi terkemuka, menyediakan berbagai fasilitas penunjang kegiatan akademik dan non-akademik, termasuk akses internet nirkabel. Fasilitas ini krusial tidak hanya bagi mahasiswa dan dosen untuk mendukung kegiatan pembelajaran dan penelitian,

tetapi juga bagi berbagai unit di lingkungan universitas untuk operasional sehari-hari. Sebagai contoh, di Laboratorium Telekomunikasi Fakultas Teknik, akses internet nirkabel dimanfaatkan secara ekstensif untuk simulasi jaringan, pengujian perangkat, dan akses ke sumber daya komputasi awan yang menunjang riset di bidang telekomunikasi.

Namun, di balik kemudahan akses yang ditawarkan oleh jaringan nirkabel, terdapat potensi risiko keamanan siber yang signifikan. Peningkatan ancaman kejahatan siber, seperti pencurian data melalui *sniffing*, penyebaran *malware*, atau serangan *phishing*, menjadi perhatian serius. Meskipun pengelolaan jaringan seringkali dilakukan oleh staf atau administrator teknis, pengawasan tersebut seringkali terbatas pada jam kerja operasional. Serangan siber, di sisi lain, dapat terjadi kapan saja, termasuk di luar jam pengawasan langsung, sehingga meningkatkan kerentanan sistem. [4]

Oleh karena itu, sangat penting bagi Laboratorium Telekomunikasi, untuk memastikan bahwa infrastruktur jaringan dan data yang dikelola terlindungi dari berbagai ancaman. Dalam upaya mitigasi risiko tersebut, penelitian ini akan melakukan pengujian keamanan data menggunakan metode *Penetration Testing*. Pengujian ini bertujuan untuk menganalisis dan mengevaluasi efektivitas sistem keamanan teknologi WLAN khususnya pada lapisan autentikasi dan enkripsi nirkabel yang telah diterapkan di lingkungan Laboratorium Telekomunikasi, guna mengidentifikasi potensi kerentanan dan merekomendasikan perbaikan yang diperlukan. [5]

Urgensi pelaksanaan *Penetration Testing* ini didasarkan pada identifikasi celah keamanan yang signifikan pada segmen nirkabel. Hasil observasi awal mengindikasikan bahwa akses poin yang tersedia masih memiliki kerentanan terhadap dua jenis serangan utama, yaitu *Cracking The Encryption* dan *Man-In-The-Middle* (MITM). Kerentanan pada spektrum frekuensi ini menunjukkan bahwa sistem keamanan nirkabel yang diimplementasikan belum memberikan perlindungan yang memadai bagi pengguna, sehingga berpotensi menjadi jalur masuk bagi pihak yang tidak berwenang untuk mengganggu stabilitas layanan internet.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka penulis merumuskan masalah, yaitu bagaimana tingkat kerentanan keamanan jaringan terhadap ancaman serangan eksternal yang mengancam keamanan jaringan WLAN?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini untuk menganalisa tingkat kerentanan keamanan jaringan *Wireless* LAN terhadap serangan luar dengan menggunakan metode *Penetration Testing*.

1.4 Pembataan Masalah

Sehubungan dengan keterbatasan yang dimiliki, dari segi waktu, pemikiran serta biaya, maka batasan masalah pada penelitian ini yaitu :

1. Penelitian ini menggunakan tools Aircrak-ng, *Ettercap*, dan *Wireshark* sebagai alat uji.
2. Menguji infrastruktur protokol keamanan WLAN.
3. Menguji keamanan enkripsi WPA2 pada jaringan WLAN.
4. Menguji pada satu *Access Point.*
5. Minimal 1 user yang aktif pada saat pengujian.

1.5 Sistematika Penulisan

Agar penulisan proposal tugas akhir ini teratur, maka sistematika penulisan dibagi dalam beberapa bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, perumusan masalah, tujuan penelitian, pembatasan masalah, dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini membahas tentang studi kepustakaan dan dasar teori.

BAB III METODOLOGI PENELITIAN

Bab ini terdiri dari tempat dan waktu penelitian, alat dan bahan penelitian, metode penelitian, variabel atau data, analisis hasil serta diagram alir penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bab yang berisi *Analisa Cracking Encryption, Man In The Middle Attack*, serta hasil *Penetration Testing*.

BAB V PENUTUP

Bab ini berisikan kesimpulan dan saran berdasarkan hasil dan pembahasan yang telah dilakukan penulis.