

**IDENTIFIKASI CELAH KEAMANAN JARINGAN WI-FI
BERBASIS WPA2-PSK DENGAN METODE *PENETRATION*
TESTING MENGGUNAKAN KALI LINUX**

SKRIPSI

**Oleh:
Majesty Marvela Putri
202110715183**



**PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BHAYANGKARA JAKARTA RAYA
2025**

LEMBAR PERSETUJUAN PEMBIMBING

Judul Skripsi : Identifikasi Celah Keamanan Jaringan Wi-Fi Berbasis
WPA2-PSK Dengan Metode *Penetration Testing*
Menggunakan Kali Linux

Nama Mahasiswa : Majesty Marvela Putri

Nomor Pokok Mahasiswa : 202110715183

Program Studi/Fakultas : Informatika/Ilmu Komputer

Tanggal Lulus Ujian Skripsi : 25 Juli 2025

Jakarta, 01 Agustus 2025
MENYETUJUI,

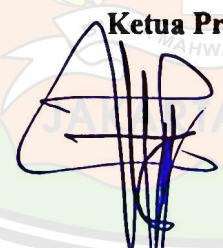
Pembimbing I

Pembimbing II


(Rakhmat Purnomo, S.Pd., S.Kom., M.Kom)
NIDN: 0322108201


(Asep Ramdhani Mahbub, S.Kom., M.Kom)
NIDN: 0329087703

Ketua Program Studi


Ahmad Fathurrozi, S.E., M.M.S.I
NIP: 2012486

Program Studi Informatika
Fakultas Ilmu Komputer
Universitas Bhayangkara Jakarta Raya
2025

LEMBAR PENGESAHAN

Judul Skripsi : Identifikasi Celah Keamanan Jaringan Wi-Fi Berbasis WPA2-PSK Dengan Metode *Penetration Testing* Menggunakan Kali Linux
Nama Mahasiswa : Majesty Marvela Putri
Nomor Pokok Mahasiswa : 202110715183
Program Studi/Fakultas : Informatika / Ilmu Komputer
Tanggal Lulus Ujian Skripsi : 25 Juli 2025

Jakarta, 01 Agustus 2025

MENGESAHKAN,

Ketua Tim Penguji : Ahmad Fathurrozi, S.E., M.M.S.I.
NIP: 2012486

Penguji I : Muhammad Yasir, S.Si., M. Kom
NIDN: 0317129009

Penguji II : Rakhmat Purnomo, S.Pd., S.Kom., M. Kom.
NIDN: 0322108201

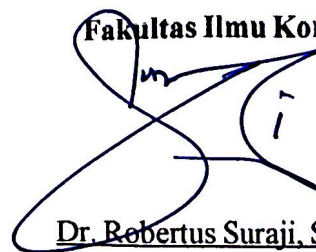
MENGETAHUI,

Ketua
Program Studi Informatika



Ahmad Fathurrozi, S.E., M.M.S.I.
NIP. 2012486

Dekan
Fakultas Ilmu Komputer



Dr. Robertus Suraji, S.S., M.A
NIP. 1904406



UNIVERSITAS BHAYANGKARA JAKARTA RAYA
FAKULTAS ILMU KOMPUTER
PROGRAM STUDI INFORMATIKA

LEMBAR PERNYATAAN BUKAN PLAGIASI

Yang bertanda tangan dibawah ini:

Nama : Majesty Marvela Putri
NPM : 202110715183
Program Studi : Informatika
Fakultas : Ilmu Komputer
Judul Tugas Akhir : Identifikasi Celah Keamanan Jaringan Wi-Fi Berbasis WPA2-PSK Dengan Metode *Penetration testing* Menggunakan Kali linux

Dengan ini menyatakan bahwa hasil penulisan skripsi yang telah saya buat ini merupakan **hasil karya saya sendiri dan benar keasliannya**. Apabila dikemudian hari penulisan skripsi ini merupakan plagiat atau penjiplakan terhadap karya orang lain, maka saya bersedia mempertanggungjawabkan sekaligus bersedia menerima sanksi berdasarkan tata tertib di Universitas Bhayangkara Jakarta Raya.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan dari pihak mana pun.

Jakarta, 01 Agustus 2025

Penulis,



Majesty Marvela Putri

ABSTRAK

Majesty Marvela Putri, 202110715183. Identifikasi Celah Keamanan Jaringan Wi-Fi Berbasis WPA2-PSK Dengan Metode *Penetration testing* Menggunakan Kali linux. Bekasi: Fakultas Ilmu Komputer. Universitas Bhayangkara Jakarta Raya. 2025.

Keamanan dari jaringan Wi-Fi pribadi seringkali kurang diperhatikan, terutama yang menggunakan protokol WPA2-PSK. Tujuan dari penelitian ini adalah untuk menemukan celah keamanan pada jaringan Wi-Fi WPA2-PSK melalui pendekatan pengujian penetrasi dengan kali linux. Pengujian ini dilakukan pada jaringan Wi-Fi pribadi dengan menggunakan adapter TP-Link TL-WN722N yang *support* mode *monitor* dan *injection*. Metode pengujian mengikuti pedoman *NIST SP 800-42*, yang terdiri dari tahap perencanaan, pengintaian, serangan, dan pelaporan. Beberapa jenis serangan yang dilakukan mencakup *Deauthentication Attack* (menggunakan *airodump-ng*), *Handshake capture* (menggunakan *aireplay-ng*), dan *Cracking Dictionary Attack* (menggunakan *aircrack-ng*). Hasil dari pengujian menunjukkan bahwa kata sandi jaringan berhasil ditemukan dengan memanfaatkan informasi yang ada pada target serta *wordlist* yang sesuai. Risiko dari celah keamanan tersebut kemudian dinilai dengan menggunakan *Common Vulnerability Scoring System (CVSS)* v3.1, yang menghasilkan skor sebesar 5.3 – 8.2 yang masuk dalam kategori risiko tinggi (*Medium dan High Severity*). Skor ini menunjukkan bahwa serangan dapat dilakukan dengan mudah dan dapat mengancam kerahasiaan serta integritas jaringan. Penelitian ini menunjukkan bahwa sistem keamanan WPA2-PSK sangat rentan terhadap eksploitasi, terutama ketika pengguna menggunakan kata sandi yang lemah dan mudah ditebak. Oleh karena itu, sangat disarankan bagi administrator jaringan dan pengguna untuk beralih ke protokol keamanan WPA3 dan melakukan pengujian keamanan jaringan secara rutin untuk menghindari serangan siber dikemudian hari.

Kata Kunci: Wi-Fi, WPA2-PSK, *Penetration testing*, Kali linux, *CVSS*, Keamanan Jaringan.

ABSTRACT

Majesty Marvela Putri, 202110715183. *Identifying Security Vulnerabilities in WPA2-PSK-Based Wi-Fi Networks Using Penetration testing Methods with Kali linux.* Bekasi: *Faculty of Computer Science. University of Bhayangkara Jakarta Raya.* 2025

The security of private Wi-Fi networks is often overlooked, especially those using the WPA2-PSK protocol. The purpose of this study is to identify security vulnerabilities in WPA2-PSK Wi-Fi networks through a penetration testing approach using Kali linux. The testing was conducted on a private Wi-Fi network using a TP-Link TL-WN722N adapter that supports monitor mode and injection. The testing method followed the guidelines of NIST SP 800-42, which consists of planning, reconnaissance, attack, and reporting stages. The types of attacks performed included Deauthentication Attack, Handshake capture, and Cracking Dictionary Attack. The results of the testing showed that the network password was successfully discovered by leveraging information available on the target and an appropriate wordlist. The risk of this security vulnerability was then assessed using the Common Vulnerability Scoring System (CVSS) v3.1, which resulted in a score of 5.3–8.2, falling into the medium and high severity category. This score indicates that the attack can be easily carried out and poses a threat to the confidentiality and integrity of the network. This study shows that the WPA2-PSK security system is highly vulnerable to exploitation, especially when users employ weak and easily guessable passwords. Therefore, it is strongly recommended that network administrators and users transition to the WPA3 security protocol and conduct regular network security testing to prevent future cyberattacks.

Keywords: *Wi-Fi, WPA2-PSK, Penetration testing, Kali linux, CVSS, Network Security.*

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI

KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIK

Sebagai sivitas akademik Universitas Bhayangkara Jakarta Raya, saya yang bertanda tangan di bawah ini:

Nama : Majesty Marvela Putri
NPM : 202110715183
Program Studi : Informatika
Fakultas : Ilmu Komputer
Jenis Karya : Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Bhayangkara Jakarta Raya **Hak Bebas Royalti Non-Eksklusif (Non-Exclusive Royalty-Free Right)**, atas karya ilmiah saya yang berjudul:

“Identifikasi Celah Keamanan Jaringan Wi-Fi Berbasis WPA2-PSK Dengan Metode *Penetration testing* Menggunakan Kali Linux”.

Beserta perangkat yang ada (bila diperlukan). Dengan hak bebas royalti non-eksklusif ini, Universitas Bhayangkara Jakarta Raya berhak menyimpan, mengalihmediakan, mengelolanya dalam bentuk pangkalan data (*database*), mendistribusikannya dan mempublikasikannya di Internet atau media lain untuk kepentingan akademis tanpa perlu meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik hak cipta.

Segala bentuk tuntutan hukum yang timbul atas pelanggaran hak cipta dalam karya ilmiah ini menjadi tanggung jawab saya pribadi

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 01 Agustus 2025

Yang Menyatakan



Majesty Marvela Putri

KATA PENGANTAR

Segala puji bagi Allah SWT, yang telah melimpahkan rahmat dan hidayah nya sehingga saya dapat menyelesaikan Penelitian Tugas Akhir yang berjudul **“Identifikasi Celah Keamanan Jaringan Wi-Fi Berbasis WPA2-PSK Dengan Metode *Penetration testing* Menggunakan Kali linux”**. Penulisan tugas akhir ini saya kerjakan sebagai tanggung jawab dan bukti tertulis akan syarat lulus dalam menyelesaikan tugas akhir program studi Informatika pada fakultas Ilmu Komputer Universitas Bhayangkara Jakarta raya yang saya ambil pada semester 8 ini.

Dalam penyusunan penelitian tugas akhir ini penulis banyak sekali mendapatkan bantuan dari berbagai pihak, oleh sebab itu penulis ingin mengungkapkan rasa terima kasih kepada:

1. Bapak Irjen Pol (Purn) Prof. Dr. Drs. H. Bambang Karsono, S.H., M.M., Ph.D., D.Crim., (Honoris Causa) selaku Rektor Universitas Bhayangkara Jakarta Raya.
2. Bapak Dr. Robertus Suraji, S.S., M.A selaku Dekan Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
3. Bapak Ahmad Fathurrozi, S.E., M.M.S.I. selaku Ketua Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
4. Bapak Rakhmat Purnomo S.Pd., S.Kom., M.Kom. selaku pembimbing I dalam penelitian tugas akhir Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.
5. Bapak Asep Ramdhani Mahbub, S.Kom., M.Kom. selaku pembimbing II dalam penelitian tugas akhir Program Studi Informatika Fakultas Ilmu Komputer Universitas Bhayangkara Jakarta Raya.

6. Bapak Hendarman Lubis, S.Kom., M.Kom. selaku dosen Pembimbing Akademik.
7. Kepada cinta pertama dan panutanku Bapak Supriyanto terima kasih atas pengorbanan dan kerja keras bapak dalam membesarkan, kerja keras dan mendidik penulis sehingga dapat mengenyam pendidikan hingga sarjana. Kepada pintu surgaku Ibunda Indah Triasih terima kasih atas kasih sayang dan perhatian serta doa yang diberikan kepada penulis, meskipun beliau berdua tidak sempat merasakan pendidikan bangku perkuliahan dan menjadi sarjana, namun mereka mampu senantiasa memberikan yang terbaik untuk penulis, serta tak kenal lelah mendoakan serta memberikan perhatian dan dukungan hingga penulis mampu menyelesaikan studinya sampai meraih gelar sarjana. Doa yang selalu penulis panjatkan adalah, agar bapak dan ibu selalu diberi kesehatan, umur yang panjang, dan bahagia selalu.
8. Kepada Majesty Marvela Putri, ya! diri penulis sendiri, yang telah bertahan hingga saat ini, disaat penulis tidak percaya terhadap diri sendiri, namun penulis tetap mengingat bahwa setiap langkah kecil yang telah diambil adalah bagian dari perjalanan, meskipun terasa sulit atau lambat. Perjalanan menuju impian bukanlah lomba *sprint*, tetapi lebih seperti maraton yang memerlukan ketekunan, kesabaran, dan tekad yang kuat. Tidak hanya itu, segala masalah dan pikiran buruk yang selalu menghantui pikiran yang selama ini menghambat proses penyelesaian skripsi ini yang juga memotivasi saya untuk terus ambisi dalam menyelesaikan skripsi ini, terima kasih sudah dapat bertahan dan mampu menyelesaikan studi ini. Apapun pilihan yang telah dipegang sekarang, terima kasih sudah berjuang sejauh ini dan memilih untuk tetap berusaha dan tidak

lelah mencoba. Ini merupakan pencapaian yang patut dirayakan untuk diri sendiri. Berbahagialah selalu apapun kekurangan dan kelebihanmu mari tetap berjuang untuk masa depan.

9. Kepada idola penulis yaitu Choi Hyunsuk, Park Jihoon, Yoshi, Kim Junkyu, Yoon Jaehyuk, Asahi, Kim Doyoung, Haruto, Park Jeongwoo, So Junghwan (TREASURE), terima kasih yang secara tidak langsung telah menjadi inspirasi, penyemangat, dan mengisi masa-masa sulit dalam pengerjaan skripsi penulis, melalui karya-karya dan suara indahny sehingga menjadi lebih berwarna. Terima kasih sudah mengajarkan bahwa dalam meraih impian harus ada perjuangan dan jiwa pantang menyerah.

Penelitian tugas akhir yang disusun ini, mungkin masih terdapat banyak kekurangan dan masih jauh dari sempurna, oleh karena itu penulis dengan hati terbuka menerima masukan baik berupa kritik, maupun saran-saran yang dapat membangun untuk memperbaiki kekurangan-kekurangan yang ada. Semoga tugas akhi ini bermanfaat, baik bagi penulis pribadi maupun bagi orang lain yang membacanya.

Jakarta, 01 Agustus 2025

Hormat Saya,



Majesty Marvela Putri

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN BUKAN PLAGIASI	iv
ABSTRAK	v
<i>ABSTRACT</i>	vi
LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI	vii
KATA PENGANTAR.....	viii
DAFTAR ISI.....	xi
DAFTAR TABEL	xiv
DAFTAR GAMBAR.....	xv
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi Masalah	3
1.3 Rumusan Masalah	4
1.4 Tujuan Penelitian.....	5
1.5 Manfaat Penelitian.....	5
1.6 Batasan Masalah.....	6
1.7 Sistematika Penulisan.....	6
BAB II TINJAUAN PUSTAKA.....	8
2.1 Kajian Literatur	8
2.2 Landasan Teori	9
2.2.1 Konsep Dasar Jaringan Komputer	9
2.2.2 Jaringan <i>Wireless Local Area Network</i> (WLAN)	10

2.2.3	Serangan <i>Wireless</i> LAN.....	11
2.2.4	<i>Wireless Fidelity</i> (Wi-Fi)	12
2.2.5	Protokol Keamanan WPA2-PSK	14
2.2.6	IP Address	15
2.2.7	MAC Address.....	16
2.2.8	SSID dan BSSID	16
2.2.9	Huawei HG8245H5.....	17
2.2.10	TP-Link WN722N	18
2.2.11	<i>Virtual Machine</i>	19
2.2.11	<i>Penetration Testing</i> (NIST SP 800-42)	20
2.2.12	Kali Linux	23
2.2.13	<i>Tools</i> dalam <i>Penetration Testing</i> Jaringan Wi-Fi	24
2.2.14	<i>Common Vulnerability Scoring System calculator</i> (CVSS)	25
BAB III METODOLOGI PENELITIAN		30
3.1	Objek dan Tempat Penelitian	30
3.2	Kerangka Penelitian	31
3.3	Metode Pengumpulan Data	34
3.4	<i>Roadmap</i> Penelitian.....	35
3.5	Analisis Kebutuhan Alat Penelitian.....	36
3.5.1	Kebutuhan Perangkat Keras (<i>Hardware</i>)	36
3.5.2	Kebutuhan Perangkat Lunak (<i>Software</i>).....	38
3.6	Skenario Pengujian.....	38
BAB IV HASIL DAN PEMBAHASAN		41
4.1	Gambaran Umum Pelaksanaan Pengujian.....	41
4.2	Hasil Pengujian <i>Penetration testing</i>	41
4.2.1	Tahap Perencanaan (<i>Planning</i>)	41

4.2.2	Tahap Pengintaian (<i>Discovery</i>).....	41
4.2.3	Tahap Serangan (<i>Attack</i>).....	45
4.2.4	Tahap Pelaporan (<i>Reporting</i>).....	57
4.3	Pengukuran Tingkat Risiko dengan CVSS Score v3.1	60
4.3.1	Penilaian CVSS Serangan <i>Deauthentication Attack</i>	60
4.3.2	Penilaian CVSS Serangan <i>Handshake capture</i>	62
4.3.3	Penilaian CVSS Serangan <i>Cracking Dictionary Attack</i>	64
4.4	Rekomendasi Perbaikan	66
BAB V PENUTUP.....		69
5.1	Kesimpulan.....	69
5.2	Saran.....	70
DAFTAR PUSTAKA.....		71
LAMPIRAN.....		74



DAFTAR TABEL

Tabel 2. 1 Penelitian Terdahulu	8
Tabel 2. 2 Spesifikasi IEEE 802.11	12
Tabel 2. 3 Jenis Protokol Keamanan Wi-Fi	13
Tabel 2. 4 Perbedaan Versi Tp-Link TL-WN722N	19
Tabel 2. 5 Tabel Numerik Bagian Exploitability Metrics.....	28
Tabel 2. 6 Tabel Impact Metrics	28
Tabel 3. 1 Roadmap Penelitian	35
Tabel 3. 2 Kebutuhan Perangkat Keras.....	37
Tabel 3. 3 Kebutuhan Perangkat Lunak.....	38
Tabel 3. 4 Penjelasan skenario pengujian	39
Tabel 4. 1 Hasil Pemindaian Target.....	45
Tabel 4. 2 Serangan ARP Spoofing	54
Tabel 4. 3 Hasil Pengujian	58
Tabel 4. 4 Celah Keamanan	59
Tabel 4. 5 Penilaian CVSS Deauthentication	60
Tabel 4. 6 Penilaian CVSS Handshake capture	62
Tabel 4. 7 Penilaian CVSS Cracking Dictionary Attack	64
Tabel 4. 8 Hasil akhir perhitungan CVSS.....	66
Tabel 4. 9 Rekomendasi Perbaikan.....	66

DAFTAR GAMBAR

Gambar 2. 1 Tahapan Metodologi <i>Penetration testing</i>	21
Gambar 3. 1 Lokasi Penelitian.....	30
Gambar 3. 2 Kerangka Penelitian	31
Gambar 3. 4 Diagram alur skenario Pengujian	39
Gambar 4. 1 Adapter Wi-Fi Terhubung.....	42
Gambar 4. 2 <i>Mode Managed</i>	43
Gambar 4. 3 <i>Mode Monitor</i>	44
Gambar 4. 4 <i>Passive Reconnaissance</i>	44
Gambar 4. 5 File <i>wpa_handshake-02.cap</i>	46
Gambar 4. 6 <i>sudo aireplay-ng</i>	47
Gambar 4. 7 Hasil tangkapan WPA2-PSK <i>4-way-handshake</i>	48
Gambar 4. 8 <i>Cracking by rockyou.txt</i>	49
Gambar 4. 9 Hasil <i>cracking key not found</i>	50
Gambar 4. 10 <i>Cracking with wordlist.txt</i>	51
Gambar 4. 11 <i>KEY FOUND</i>	51
Gambar 4. 12 Proses kali linux terkoneksi ke jaringan target dengan nmtui.....	52
Gambar 4. 13 Melihat perangkat aktif di router target	53
Gambar 4. 14 Hasil <i>arp-spoofing</i>	53
Gambar 4. 15 <i>Sniffing</i> menggunakan <i>wireshark</i>	55
Gambar 4. 16 Perhitungan otomatis CVSS <i>deauthentication</i>	61
Gambar 4. 17 Perhitungan otomatis CVSS <i>handshake capture</i>	63
Gambar 4. 18 Perhitungan Otomatis CVSS <i>Cracking Dictionary Attack</i>	65

DAFTAR LAMPIRAN

Uji Plagiarisme

Biodata Mahasiswa

Kartu Konsultasi Bimbingan

Kartu Bimbingan Skripsi Dosen Pembimbing I

Kartu Bimbingan Skripsi Dosen Pembimbing II

Rekomendasi Dari Pembimbing I Untuk Tugas Akhir

Rekomendasi Dari Pembimbing II Untuk Tugas Akhir

Bukti Submit Artikel

