Jurnal Rekayasa Sistem Informasi dan Teknologi
Volume 3, No 2 November 2025
e-ISSN : 3025-888X

ANALISIS KEAMANAN JARINGAN WIRELESS PADA SMK ISLAM MANBA'UL ULUM MENGGUNAKAN PENDEKATAN PENETRATION TESTING

Ika Mayang Sari[1], Lalu Delsi Samsumar[2], M. Zulpahmi[3]
[1,2,3]Universitas Teknologi Mataram
ikamayangsari11@gmail.com lalu.ellsyam@gmail.com pahmijorge04@gmail.com

Received: 20-08- 2025	Revised: 25-09-2025	Approved: 25-10-2025

ABSTRAK

Perkembangan teknologi informasi mendorong pemanfaatan jaringan nirkabel dalam kegiatan pendidikan. Penelitian ini bertujuan menganalisis keamanan jaringan wireless di SMK Islam Manba'ul Ulum yang menggunakan protokol WPA2. Metode yang digunakan adalah penetration testing berbasis Kali Linux melalui simulasi serangan Handshake Capture dan WPA2 Cracking untuk menguji autentikasi, Deauthentication Attack untuk menguji kestabilan koneksi, serta Man-in-the-Middle (MiTM) Attack untuk menguji kerahasiaan data, dengan bantuan tools Aircrack-ng, Aireplay-ng, Airodump-ng, Bettercap, dan Wireshark. Hasil penelitian menunjukkan seluruh simulasi serangan berhasil dilakukan, meliputi peretasan kata sandi Wi-Fi, pemutusan koneksi pengguna, dan penyadapan data komunikasi, sehingga membuktikan jaringan masih rentan terhadap ancaman keamanan.

Kata Kunci: *Wireless, Penetration Testing, WPA2, Deauthentication, dan MiTM.*

ABSTRACK

The development of information technology has encouraged the use of wireless networks in educational activities. This study aims to analyze the security of the wireless network at SMK Islam Manba'ul Ulum, which applies the WPA2 protocol. The research method used was penetration testing based on Kali Linux by simulating attacks such as Handshake Capture and WPA2 Cracking to test authentication, Deauthentication Attack to test connection stability, and Man-in-the-Middle (MiTM) Attack to test data confidentiality, using tools including Aircrack-ng, Aireplay-ng, Airodump-ng, Bettercap, and Wireshark. The results show that all simulated attacks were successfully executed, including Wi-Fi password cracking, user disconnection, and communication data interception, indicating that the network remains vulnerable to security threats.

Keywords: *Wireless, Penetration Testing, WPA2, Deauthentication, and MiTM.*

PENDAHULUAN

Keamanan jaringan merupakan sangat merugikan dalam menjaga kerahasiaan, integritas, dan ketersediaan data pada sistem komputer. Kelemahan dalam jaringan komputer yang tidak dilindungi dengan baik dapat membuka peluang akses ilegal bagi pihak yang tidak bertanggung jawab, menimbulkan kerugian berupa kehilangan data, kerusakan sistem server, menurunnya kualitas layanan, hingga hilangnya aset penting dari suatu institusi. Hal ini juga berlaku di lingkungan pendidikan, di mana jaringan komputer digunakan untuk mendukung kegiatan belajar mengajar.

SMK Islam Manba'ul Ulum merupakan salah satu lembaga pendidikan yang memanfaatkan jaringan *wireless* sebagai sarana pendukung pembelajaran, khususnya pada mata pelajaran kejuruan di laboratorium komputer. Namun, hasil observasi menunjukkan adanya permasalahan pada keamanan jaringan *wireless* yang digunakan, seperti penggunaan kata sandi yang lemah dan mudah ditebak serta minimnya perlindungan terhadap ancaman siber. Kondisi tersebut membuat jaringan sekolah

rentan terhadap serangan, contohnya pembobolan kata sandi Wi-Fi dan penyalahgunaan akses jaringan, yang termasuk dalam kategori *cybercrime*.

Sejumlah penelitian terdahulu juga menunjukkan hal serupa. (Kurniadi, 2021a) menemukan kelemahan pada jaringan WPA2-PSK yang masih menggunakan konfigurasi default. Penelitian oleh (Galang Saputra & Parga Zen, 2023) membuktikan bahwa meskipun jaringan sudah memakai enkripsi WPA2-PSK, masih dapat ditembus dengan teknik *brute force*. Sementara itu, (Aryo et al., 2022) menunjukkan lemahnya keamanan jaringan sekolah lain karena masih bisa dilakukan *sniffing* dan *dictionary attack*. Bahkan penelitian (Nurfanis1, 2024) juga menegaskan bahwa jaringan sekolah dengan mode *open network* sangat mudah dieksploitasi oleh pihak luar.

LANDASAN TEORI

Jaringan komputer merupakan sebuah kumpulan dari banyak perangkat,seperti komputer, *switch, router* atau peralatan jaringan lainnya yang terkoneksi media komukasi tertentu. Jaringan komputer sangat penting untuk mencari kerusakan jaringan dengan cepat dan sederhana.

Jaringan *Wireless* merupakan Kumpulan komputer yang terhubung dari satu komputer ke komputer lain, membentuk jaringan komputer. Jaringan ini menggunakan media udara/gelombang untuk mengirim data. Dalam sebuah jaringan, kecepatan dipengaruhi oleh faktor – faktor seperti perangkat yang sedang digunakan dan perangkat yang menjadi *AP* jarak dan ruang (Pangestu & Liza, 2022).

Berikut jenis jaringan berdasarkan media transmisi:

1. Jaringan Kabel

   Jaringan kabel merupakan jaringan yang digunakan dari satu komputer ke komputer lainnya, diperlukan kabel jaringan. Kabel jaringan mengirimkan informasi dalam bentuk sinyal elektronik atau komputer berjaringan.
2. Jaringan Nirkabel

   Jaringan nirkabel merupakan sebuah jaringan yang menggunakan gelombang radio sebagai media transmisi dan kemudian dipancarkan.

Ancaman Keamanan Jaringan

1. *Handshake Capture* dan WPA2 *Cracking*

Handshake Capture adalah proses mencegat dan menyimpan paket-paket data yang membentuk 4-*Way Handshake*. Karena paket-paket ini mengandung informasi kunci (seperti *ANonce, SNonce,* dan MIC yang dienkripsi menggunakan PSK), seorang penyerang dapat menggunakan informasi ini untuk mencoba "memecahkan" (*cracking*) kata sandi jaringan secara *offline.*

2. *Deauthentication Attack*

Deauthentication Attack adalah jenis serangan *Denial of Service* (DoS) yang menargetkan komunikasi antara perangkat nirkabel seperti laptop atau ponsel dan titik akses Wi-Fi. Tujuan utama serangan ini adalah untuk memutus paksa koneksi perangkat dari jaringan Wi-Fi. Serangan ini mengeksploitasi kelemahan fundamental dalam standar protokol Wi-Fi (IEEE 802.11) yang mengatur bagaimana perangkat terhubung dan terputus dari jaringan.

3. *MiTM (Man in the Middle) Attack*

Man in the middle attack merupakan serangan yang dilakukan oleh satu atau lebih penyerangan, di mana penyerang tersebut mengirim dan memodifikasi pesan sementara dua pihak yang berwenang dalam komunikasi terus menerus. Dengan

melakukan serangan ketika komunikasi sedang berlangsung. Jika kegiatan illegal ini timbul tentu akan sangan merugikan bagi pengguna *wireless* tersebut, di mana dampak dari kerugian nya dapat berupa kehilangan data, atau bocornya identitas rahasia dari pengguna jaringan *wireless* tersebut (Pangestu & Liza, 2022).

Penetration Testing

Penetration Testing merupakan metode eksekusi evaluasi keamanan sistem dan jaringan komputer. Penilaian tersebut diselesaikan dengan melakukan simulasi serangan (*attack).* Hasil dari pegujian *pentest* ini sangat penting untuk meningkatkan tingkat keamanan sistem komputer dari sistem *administrator* jaringan, selain dapat memberikan informasi tentang kerentanan sistem, tetapi juga memudahkan untuk menilai keamanan sistem yang sedang berjalan. Kegiatan ini biasa disebut sebagai "*etchical hacking*"(Kurniadi, 2021).

Kali Linux

Kali Linux merupakan sistem operasi dari keluarga *Linux* tingkat lanjut yang digunakan untuk pengujian keamanan *penetration testing* bersifat *open source* atau gratis, memenuhi FHS *complaint*, dukungan luas untuk perangkat nirkabel, lingkungan pengembangan yang aman, dan tersedia dalam berbagai bahasa (Anam & Fachri, 2025). Berikut beberapa *tools* yang digunakan:

1. *MAC Adddres*

MAC Address adalah sebuah alamat jaringan yang menunjukkan simpul (node) tertentu dalam jaringan, yang dapat digunakan untuk mengidentifikasi komputer atau node lainnya dalam jaringan.

2. *Aircrack-Suite*

Aircrack-ng suite adalah kumpulan tools open-source yang digunakan untuk menganalisis dan menguji keamanan jaringan Wi-Fi. Fungsinya meliputi monitoring paket, melakukan serangan uji seperti deauthentication, serta memecahkan kunci enkripsi WEP, WPA, dan WPA2 melalui metode brute force atau dictionary attack. Beberapa tool penting di dalamnya antara lain airmon-ng untuk mode monitor, airodump-ng untuk menangkap paket, aireplay-ng untuk injeksi paket, dan aircrack-ng untuk cracking password. Suite ini umumnya digunakan dalam penetration testing guna mengidentifikasi kelemahan jaringan wireless secara legal dan etis.

3. *Bettercap*

Bettercap adalah alat multi-fungsi yang kuat dan fleksibel untuk serangan *Man-in-the-Middle (MITM)* dan penetrasi jaringan. Alat ini didesain modular dan mudah digunakan, memungkinkan pengguna untuk melakukan berbagai aktivitas seperti *spoofing DNS, sniffing* kredensial, modifikasi lalu lintas jaringan, dan bahkan injeksi kode.

4. *Wireshark*

Wireshark adalah penganalisis protokol jaringan gratis dan *open-source* yang memungkinkan untuk melihat lalu lintas yang melintas di jaringan komputer secara detail. *Wireshark* bekerja dengan "mendengarkan" dan menangkap paket data saat data tersebut bergerak melalui antarmuka jaringan, kemudian menerjemahkannya ke dalam format yang dapat dibaca manusia.

5. *Wordlistss*

Wordlistss merupakan sekumpulan kata atau frasa yang disusun dalam format file teks dan dimanfaatkan dalam proses *brute force* maupun *dictionary attack* untuk melakukan percobaan terhadap kata sandi.

6. MDK4

MDK4 (*Mesh Deauthentication Tool Kit versi 4*) merupakan perangkat lunak *open-source* yang berfungsi untuk melakukan berbagai bentuk pengujian terhadap keamanan jaringan nirkabel, terutama jaringan *Wi-Fi*. *Tools* ini merupakan pengembangan dari versi sebelumnya, yaitu MDK3, dengan peningkatan dari segi kestabilan serta mendukung lebih banyak varian metode serangan nirkabel.

METODE PENELITIAN

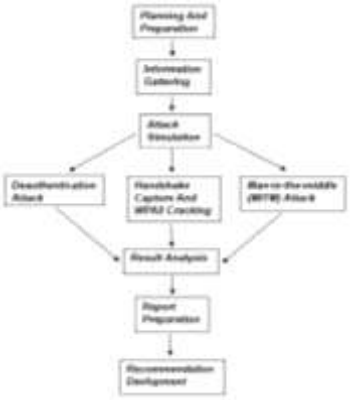
Jenis Penelitian

Jenis penelitian yang digunakan dalam penelitian ini adalah kualitatif. Alasan pemilihan metode penelitian kualitatif adalah karena penelitian kualitatif bersifat deskriptif, sering menggunakan analisis, dan membuat proses penafsirannya lebih terlihat. Penelitian kualitatif adalah penelitian yang berbasis penelitian yang informasi dan kesimpulannya diperoleh dari hasil interaksi langsung antara peneliti, objek penelitian, dan populasi yang dilakukan pada tempat penelitian.

Kemudian dilakukan eksperimental dengan menggunakan metode *penetration testing*. Metode eksperimen dipilih karena penelitian dilakukan melalui uji coba langsung pada jaringan wireless di lingkungan SMK Islam Manba'ul Ulum untuk mengamati respon sistem terhadap simulasi serangan.

Penetration testing merupakan teknik evaluasi keamanan dengan mensimulasikan serangan nyata terhadap sistem jaringan untuk mengidentifikasi kerentanan, ancaman, dan risiko(Padilah et al., 2021). Kegiatan ini biasa disebut sebagai "*etchical hacking*"(Kurniadi, 2021b).

Berikut langkah – langkah dalam melakukan pengujian pada *Penetration Testing*:



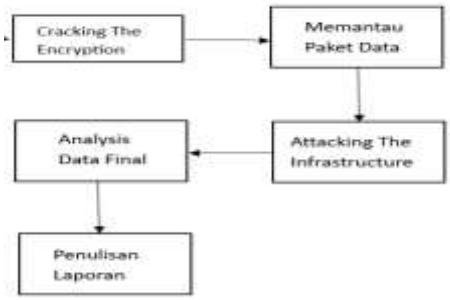
Gambar 3 Langkah-Langkah *penetration testing*

Tahapan Penelitian

Tahapan penelitian ini diawali dengan perencanaan dan observasi awal terhadap kondisi jaringan wireless di SMK Islam Manba'ul Ulum untuk mengetahui potensi kerentanan yang ada. Selanjutnya dilakukan pengumpulan informasi melalui proses pemindaian jaringan guna memperoleh data konfigurasi dan enkripsi yang digunakan. Setelah itu dilakukan simulasi serangan berupa *Handshake Capture* dan *WPA2 Cracking*, *Deauthentication Attack*, serta *Man-in-the-Middle (MiTM) Attack* untuk menguji ketahanan jaringan. Hasil dari simulasi serangan kemudian dianalisis untuk

menilai tingkat keamanan jaringan, dan tahap terakhir adalah menyusun rekomendasi perbaikan guna meningkatkan perlindungan sistem.

Tahapan penyelidikan dilakukan melalui identifikasi enkripsi jaringan, pemantauan lalu lintas data, simulasi serangan (*WPA2 Cracking, Deauthentication,* dan *MiTM*), serta analisis hasil untuk menilai kerentanan dan memberikan rekomendasi perbaikan.



Gambar 4 Diagram Tahapan Penyelidikan

HASIL DAN PEMBAHASAN

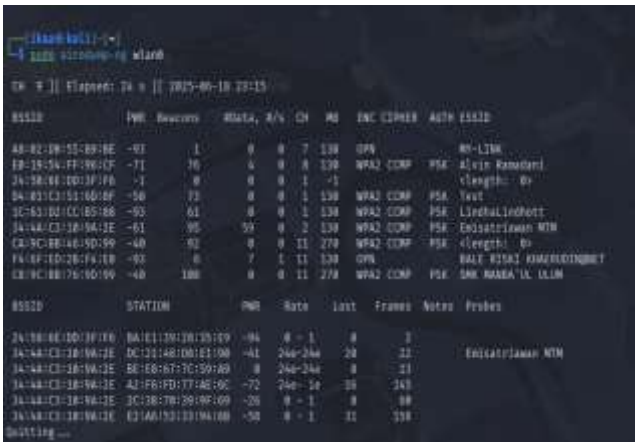
Tahap implementasi adalah tahap penerapan sistem agar dapat berfungsi sesuai dengan kebutuhan dan perancangan sebelumnya. Selain itu juga pada implementasi ini akan di jelaskan bagaimana sistem ini akan bekerja sesuai alur yang diterpakan. Adapun *hardware* yang digunakan anatara lain yaitu *PC* yang dimana berfungsi sebagai tempat *instalasi Kali Linux.* Sedangkan *software* yang digunakan adalah *Aircrack-ng Suite* dan *hanshake capture* dan *WPA2 cracking*, *deauthentication attack* serta *man-in-the-middle attack* untuk melakukan serangan pengujian pada saat penelitian berlangsung.

Tabel 1 Hasil Pengujian

Jenis Serangan	Informasi yang dibutuhkan	Status serangan
Cracking The encryption	Channel yang digunakan dan BSSID dari *acces point*.	Berhasil
Attacking The infrastructure	Attacker harus berada dalam jangkauan jaringan *wireless*, *MAC Addres* dari dari perangkat tester.	Berhasil
Man-In-The-Middle Attack	*Attacker* mendapatkan lalu lintas jaringan.	Berhasil
WPA2 Crack	*Attacker* mendapatkan *password* dari jaringan *wireless*	Berhasil
Deauthentication Attack	*Attacker* Dapat memutuskan koneksi dari jaringan *wireless*	Berhasil

1. Serangan Handshake Capture dan WPA2 Crack

Sebelum memulai serangan *handshake* terlebih dahulu dilakukan pemindaian jaringan sekitar untuk melihat jaringan target terdeteksi atau tidak.

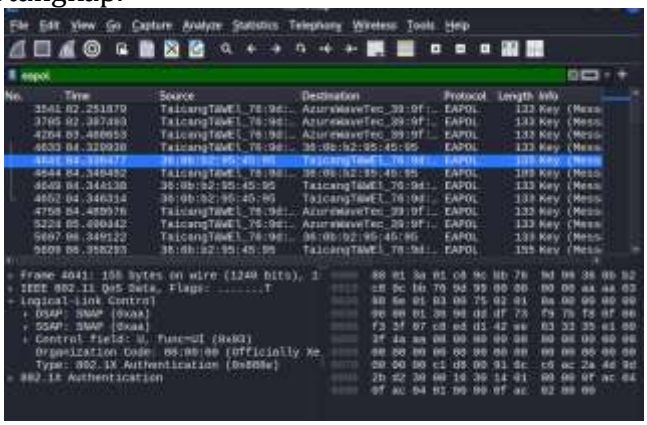


Gambar 5 Scanning Informasi Jaringan

Dapat dilihat pada gambar 5 bahwa jaringan target yaitu Jaringan SMK Islam Manba'ul Ulum sudah terdeteksi.

Gambar 6 Penangkapan Handshake

Pemutusan paksa kepada jaringan target menggunakan *deauthentication attack* agar *handshake* dapat tertangkap.

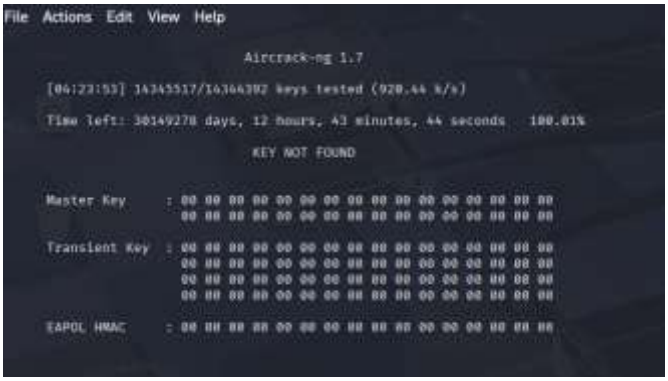


Gambar 7 Data EAPOL

Paket EAPOL yang berhasil ditangkap nantinya akan digunakan dalam analisis keamanan jaringan atau dalam simulasi serangan cracking WPA2, yang disimulasikan menggunakan tools seperti Aircrack-ng.

Gambar 8 Hasil WPA2 Crack

Dapat dilihat Gambar 8 menunjukkan hasil dari proses *cracking password Wi-Fi* menggunakan *tool Aircrack-ng* di sistem operasi Kali Linux. Proses ini dilakukan dengan memanfaatkan file *handshake* yang telah berhasil ditangkap sebelumnya, yaitu hac5-01.cap. Dalam simulasi ini, digunakan metode *dictionary attack* dengan *wordlists rockyou.txt* untuk mencoba mencocokkan *password* jaringan Wi-Fi berdasarkan daftar kata yang tersedia. Target yang dituju memiliki alamat MAC C8:9C:BB:76:9D:99. Setelah proses berjalan, *Aircrack-ng* berhasil menemukan *password* jaringan Wi-Fi tersebut, yaitu 12345678.



Gambar 9 WPA2 Crack Dengan Password Berbeda

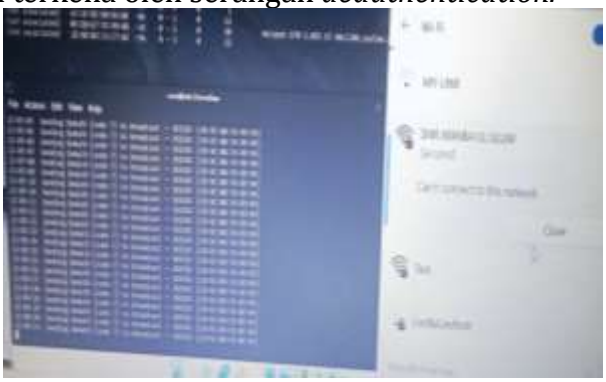
Setelah dimplementasikan beberapa serangan di atas dapat diketahui bahwa keamanan dari *password* yang digunakan masih tergolong sangat lemah dan memungkinkan untuk bisa dibobol dengan mudah oleh pihak yang tidak bertanggung jawab meskipun jaringan tersebut menggunakan keamanan WPA2-Psk. Oleh karena itu setelah celah keamanan tersebut ditemukan, maka dilakukan ulang pengujian ulang *password* menggunakan *password* yang dikombinasi dengan beberapa simbol menggunakan WPA2 *crack.*

2. Serangan Deauthentication

Setelah perintah dijalankan, proses *deauthentication* berlangsung secara terus-menerus, mengirimkan ratusan hingga ribuan paket ke *access point* dengan tujuan memaksa klien yang sedang terhubung untuk terputus dari jaringan.

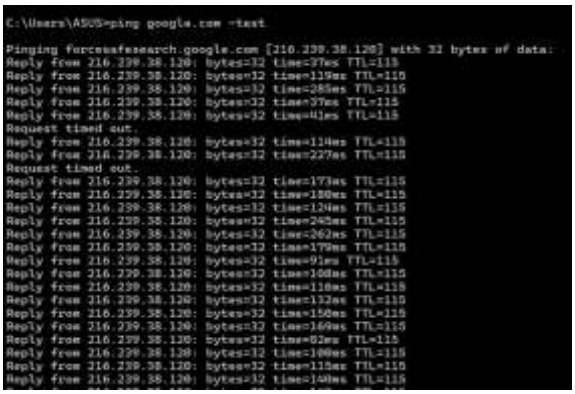
Gambar 10 Serangan Berlangsung

Dapat dilihat pada gambar 11, jaringan sudah terputus dan tidak bisa diakses. Ini menandakan bahwa tingkat keamanan yang digunakan oleh jaringan SMK Islam Manba'ul Ulum rentan terkena oleh serangan *deauthentication.*



Gambar 11 Jaringan Terputus

Kemudian terlihat pada gambar 12, hasil ping menunjukkan bahwa koneksi ke Google berjalan, tetapi mengalami waktu tanggap (*latency*) yang tidak konsisten dan beberapa kehilangan paket (*packet loss*). Hal ini diakibatkan karena jaringan wifi tidak stabil.



Gambar 12 Dampak Serangan Deauthentication

3. Serangan Man-In-The-Middle (MitM)

Output ini menunjukkan bahwa *Bettercap* telah berhasil mengumpulkan dan menyusun peta jaringan lokal secara rinci. Tahapan ini sangat krusial dalam MITM karena memungkinkan penyerang untuk memilih target berdasarkan aktivitas, vendor perangkat, atau alamat IP tertentu sebelum memulai manipulasi lalu lintas data melalui teknik seperti *ARP spoofing* atau *packet sniffing.*

Gambar 13 Tampilan ARP Spoofing

Gambar 4.18 menunjukkan proses serangan *ARP Spoofing* yang berhasil dilakukan terhadap target dengan IP 10.5.48.3 oleh *attacker* dengan IP 10.5.48.5. Setelah serangan dijalankan, penyerang mengaktifkan fitur *sniffing* untuk memantau lalu lintas data yang lewat di jaringan lokal tersebut.

ANALISIS HASIL

Hasil pengujian menunjukkan bahwa jaringan wireless di SMK Islam Manba'ul Ulum masih rentan terhadap berbagai jenis serangan. Pada uji *Handshake Capture* dan *WPA2 Cracking*, kata sandi Wi-Fi berhasil diretas menggunakan *dictionary attack*, yang membuktikan lemahnya autentikasi dengan WPA2-PSK. Namun, saat dilakukan simulasi ulang dengan kata sandi berbeda yang lebih kompleks, proses peretasan tidak berhasil, sehingga membuktikan bahwa tingkat kekuatan kata sandi sangat berpengaruh terhadap keamanan jaringan. Serangan *Deauthentication* juga berhasil memutus koneksi klien secara paksa, menandakan potensi terjadinya *Denial of Service (DoS)* yang dapat mengganggu kegiatan pembelajaran. Sementara itu, simulasi *Man-in-the-Middle (MiTM)* menunjukkan bahwa data komunikasi pengguna dapat disadap dan dimanipulasi, sehingga menimbulkan ancaman serius terhadap kerahasiaan dan integritas data.

Tabel 2 Analisis Hasil

Jenis Serangan	Tools yang Digunakan	Hasil Uji	Dampak
Handshake Capture & WPA2 Cracking	*Airodump-ng, Aircrack-ng, Wordlist*	Password Wi-Fi berhasil diretas menggunakan *dictionary attack*.	Membuktikan lemahnya autentikasi WPA2-PSK dengan kata sandi sederhana.
Deauthentication Attack	*Aireplay-ng, MDK4*	Koneksi klien terputus paksa dari jaringan.	Potensi *Denial of Service* (DoS) yang mengganggu aktivitas belajar mengajar.
Man-in-the-Middle (MiTM)	*Bettercap, Wireshark*	Data komunikasi pengguna berhasil disadap dan dimanipulasi.	Ancaman kebocoran data, penyalahgunaan identitas, dan hilangnya privasi.

KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan mulai dari perancangan hingga analisis keamanan jaringan wireless di SMK Islam Manba'ul Ulum dengan metode *penetration testing* menggunakan serangan (*Handshake Capture & WPA2 Cracking, Deauthentication Attack,* dan *Man-in-the-Middle Attack*) dengan bantuan Kali Linux, Aircrack-ng Suite, Bettercap, dan Wireshark, maka dapat diambil kesimpulan bahwa jaringan wireless di SMK Islam Manba'ul Ulum masih tergolong rentan. Hal ini dibuktikan dengan hasil penelitian yang menunjukkan bahwa dari ketiga jenis serangan yang dilakukan, semuanya berhasil dijalankan. *Handshake Capture & WPA2 Cracking* berhasil membobol kata sandi Wi-Fi yang lemah, *Deauthentication Attack* berhasil memutus koneksi klien, dan *Man-in-the-Middle Attack* berhasil menyadap lalu lintas data pengguna. Kondisi ini menandakan bahwa sistem keamanan WPA2-PSK yang digunakan belum cukup kuat apabila hanya mengandalkan kata sandi sederhana, sehingga jaringan masih berpotensi dimanfaatkan oleh pihak tidak berwenang

DAFTAR PUSTAKA

Anam, F., & Fachri, F. (2025). EVALUASI KERENTANAN KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN METODE PENETRATION TESTING DENGAN AIRCRACK-NG. *Rabit : Jurnal Teknologi Dan Sistem Informasi Univrab*, *10*(1), 1–8. https://doi.org/10.36341/rabit.v10i1.5387

Aryo, G., Pongdatu, N., Michael, A., & Patalo, E. E. (2022). *Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing di SMK Xyz Tana Toraja*. *2*(2). https://doi.org/10.47178/infinity.v2i2

Galang Saputra, S., & Parga Zen, B. (2023). *Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES)*. *1*(2), 2023. https://ojs.unigal.ac.id/index.php/jsig/index

Kurniadi, A. (2021a). *Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6)* (Vol. 1, Issue 1). https://journal.uib.ac.id/index.php/combines

Nurfanis1, Z. M. M. E. (2024). *ANALISIS KEAMANAN JARINGAN WIRELESS MENGGUNAKAN METODE PENETRATION TESTING DI SMK BANGUN NEGERI HU'U*. nurfanismulyana03@gmail.com, Zen3d.itb@gmail.com, creativepio@gmail.com

Padilah, I., Delsi Samsumar, L., & Teknologi Mataram, U. (2021). *Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing pada SMAN 1 Suela*.

Pangestu, T., & Liza, R. (2022). Analisis Keamanan Jaringan pada Jaringan Wireless dari Serangan Man In The Middle Attack DNS Spoofing. *JITEKH*, *10*(2), 60–67.