RABIT : Jurnal Teknologi dan Sistem Informasi Univrab
Volume 10 No. 1 | Januari 2025 : Hal : 1-8

ISSN CETAK : 2477-2062
ISSN ONLINE : 2502-891X

EVALUASI KERENTANAN KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN METODE *PENETRATION TESTING DENGAN AIRCRACK-NG*

[1] Fathul Anam, [2]Fahmi Fachri
[1,2]Teknik Informatika, Teknik, Universitas Ma'arif Nahdlatul Ulama Kebumen
E-mail : fa695040@gmail.com, fahmifachriumnu@gmail.com

ABSTRAK
Kemajuan teknologi jaringan kini menjadi komponen penting dalam proses informasi masyarakat. Dengan meningkatnya penggunaan jaringan nirkabel, pemahaman terhadap keamanan jaringan yang terhubung ke internet sangatlah penting untuk melindunginya dari serangan *hacker*. Pengujian penetrasi adalah langkah awal untuk meningkatkan keamanan jaringan. Penelitian ini bertujuan menemukan dan mengeksploitasi kerentanan pada jaringan nirkabel di lingkungan pondok pesantren menggunakan alat bantu *Aircrack-ng* dengan teknik *dictionary attack*. Hasil analisis menunjukkan adanya kerentanan, seperti sandi yang lemah dan kurangnya enkripsi, yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Berdasarkan temuan ini, direkomendasikan penggunaan sandi yang lebih kompleks dan pembaruan protokol keamanan untuk memperkuat sistem pertahanan jaringan. Dampak penelitian ini diharapkan dapat meningkatkan kesadaran dan pemahaman terkait pentingnya pengujian penetrasi dalam mengidentifikasi dan menangani potensi kerentanannya. Selain itu, hasil penelitian ini diharapkan memberikan kontribusi signifikan dalam upaya melindungi jaringan nirkabel di institusi pendidikan, khususnya pondok pesantren, dari ancaman keamanan siber yang semakin berkembang.

Kata Kunci: jaringan nirkabel, *penetration testing*, *Aircrack-ng*, keamanan jaringan, *dictionary attack*

ABSTRACT
Technological advancements in networking have become an essential component in the information processes of society. With the increasing use of wireless networks, understanding the security of networks connected to the internet is crucial to protect them from hacker attacks. Penetration testing is the first step to improving network security. This study aims to identify and exploit vulnerabilities in wireless networks within the pesantren environment using the Aircrack-ng tool with a dictionary attack technique. The analysis results revealed vulnerabilities, such as weak passwords and a lack of encryption, which could be exploited by malicious actors. Based on these findings, it is recommended to use more complex passwords and update security protocols to strengthen the network defense system. The impact of this study is expected to raise awareness and understanding of the importance of penetration testing in identifying and addressing potential vulnerabilities. Additionally, the results of this research are expected to make a significant contribution to protecting wireless networks in educational institutions, particularly pesantren, from the growing threats of cyberattacks.

Keyword: *wireless networks, penetration testing, Aircrack-ng, network security, dictionary attack*

PENDAHULUAN

Kemajuan teknologi jaringan telah menjadi komponen penting dalam mendukung masyarakat memperoleh informasi. Jaringan internet, terutama yang berbasis nirkabel, semakin dibutuhkan oleh berbagai kalangan, seperti siswa, mahasiswa, guru, dosen, dan pekerja kantoran. Pada Oktober 2022, jumlah pengguna internet di seluruh dunia mencapai 5,07 miliar orang, atau 63,45% dari populasi global, meningkat 3,89% dibandingkan tahun sebelumnya[1][2][3]. Seiring meningkatnya jumlah pengguna internet, penggunaan jaringan nirkabel juga terus bertambah. Teknologi ini memungkinkan perangkat terhubung dan berkomunikasi tanpa kabel, sehingga pemasangan jaringan nirkabel kini menjadi semakin mudah[4]. Namun, banyak jaringan nirkabel tetap menggunakan pengaturan default seperti *IP Address, SSID, DHCP*, hingga kata sandi bawaan, yang membuka celah kerentanan keamanan.[5].

Berdasarkan luas jangkauan jaringan, terdapat beberapa jenis jaringan komputer yang umum digunakan, yaitu:

1. *Personal Area Network (PAN)* yaitu jaringan komputer yang menghubungkan

DOI : https://doi.org/10.36341/rabit.v10i1.5387

perangkat elektronik dalam jarak yang sangat dekat, biasanya tidak lebih dari 10 meter. Jaringan ini dapat berupa *wireless* maupun *wired*.

2. *Local Area Network (LAN)* yaitu jaringan komputer yang menghubungkan beberapa komputer dalam area yang relatif kecil, seperti gedung, kampus, atau kantor. *LAN* memungkinkan komputer-komputer tersebut untuk berkomunikasi dan berbagi sumber daya secara efisien.
3. *Metropolitan Area Network (MAN)* yaitu jaringan komputer yang menghubungkan berbagai lokasi dalam suatu kota atau area metropolitan.
4. *Wide Area Network (WAN)* yaitu jaringan komputer yang menghubungkan beberapa perangkat di area geografis yang luas, seperti kota, negara, atau bahkan benua. *WAN* dapat terdiri dari beberapa jaringan area lokal *(LAN)* yang saling terhubung[6].

Di antara jenis-jenis ini, jaringan nirkabel sering kali digunakan untuk *LAN* karena fleksibilitasnya dalam mendukung kebutuhan rumah tangga, kantor, maupun institusi pendidikan. Sayangnya, minimnya perhatian terhadap pengamanan jaringan nirkabel ini menjadikannya rentan terhadap serangan siber, seperti peretasan kata sandi atau eksploitasi celah enkripsi. [7][8]. Penelitian sebelumnya menunjukkan bahwa jaringan nirkabel sering diserang menggunakan metode seperti *dictionary attack* atau *brute force attack*, yang memanfaatkan kelemahan pada kata sandi atau konfigurasi enkripsi yang lemah. Oleh karena itu, penting untuk memahami sistem keamanan jaringan nirkabel dan mengevaluasi sejauh mana jaringan tersebut mampu bertahan terhadap ancaman dari luar. Salah satu metode yang efektif untuk melakukan evaluasi ini adalah *penetration testing*. Metode ini dapat menilai sistem keamanan yang telah dibuat dengan menggunakan simulasi serangan yang sering digunakan peretas[9]. *Penetration testing* merupakan serangkaian teknik yang mensimulasikan serangan siber untuk mengidentifikasi kerentanan dalam sistem jaringan. Metode ini tidak hanya membantu mendeteksi kelemahan, tetapi juga memberikan panduan tentang langkah-langkah perbaikan yang diperlukan[10]. Metode ini bertujuan untuk mensimulasikan serangan siber untuk menguji sejauh mana jaringan nirkabel dapat bertahan terhadap ancaman dari luar[11].

Kali linux adalah sistem operasi dari keluarga *Linux* tingkat lanjut yang digunakan untuk pengujian keamanan dan *penetration testing* terhadap suatu sistem dann jaringan komputer[12]. Sistem operasi *Kali Linux* memiliki lebih dari 300 tools untuk *penetration testing* bersifat *open source* atau gratis, memenuhi FHS *complaint*, dukungan luas untuk perangkat nirkabel, lingkungan pengembangan yang aman, dan tersedia dalam berbagai bahasa[13]. Di antara berbagai alat *penetration testing, Aircrack-ng* adalah salah satu yang paling populer karena kemampuannya dalam monitoring jaringan, mengumpulkan paket data, menangkap *handshake*, dan *cracking* kata sandi. *Aircrack-ng* dipilih dalam penelitian ini karena kemampuannya yang handal dan fleksibel untuk melakukan pengujian penetrasi pada jaringan nirkabel. Alat ini efektif dalam mengeksploitasi kerentanan dengan berbagai teknik serangan, termasuk *dictionary attack*, dan mendukung berbagai protokol enkripsi seperti WEP, WPA, dan WPA2. Dibandingkan dengan alat lain seperti *Reaver*, yang hanya fokus pada serangan WPA2 melalui WPS, atau Kismet yang lebih berfokus pada pemetaan jaringan, *Aircrack-ng* menawarkan fungsionalitas yang lebih luas dan dokumentasi lengkap. Keunggulan ini menjadikannya pilihan ideal untuk mengidentifikasi dan mengatasi kerentanannya di berbagai konfigurasi jaringan nirkabel[14]. Namun, penelitian terdahulu umumnya hanya membahas penggunaan *Aircrack-ng* secara teknis tanpa mengkaji secara mendalam efektivitasnya dalam konteks tertentu, seperti lingkungan pendidikan. Hal ini menciptakan gap penelitian yang menjadi fokus studi ini.

Penelitian ini bertujuan mengeksplorasi kerentanan jaringan nirkabel di lingkungan

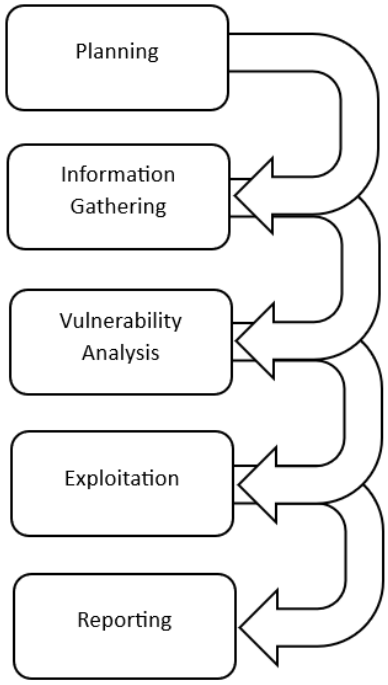
DOI : https://doi.org/10.36341/rabit.v10i1.5387 *Corresponding Author* : Fahmi Fachri

pondok pesantren menggunakan metode *penetration testing* berbasis *Aircrack-ng*. Studi ini diharapkan memberikan kontribusi penting dalam memahami risiko penggunaan jaringan nirkabel serta membantu institusi atau individu mengambil langkah preventif untuk meningkatkan keamanan jaringan mereka.[15][10].

METODE

Penelitian ini menggunakan metode *penetration testing*, yang merupakan teknik standar untuk mengidentifikasi kerentanan sistem dengan simulasi serangan siber. Dalam penelitian ini, digunakan *teknik dictionary attack*, yang dipilih karena kemudahan implementasi dan efektivitasnya dalam menguji kelemahan kata sandi jaringan. Teknik ini memanfaatkan *wordlist* yang telah disiapkan untuk mencoba menebak kata sandi jaringan target.

Tahapan *penetration testing* dalam penelitian ini meliputi lima langkah utama, yaitu *Planning, Information Gathering, Vulnerability Analysis, Exploitation*, dan *Reporting*. Diagram alur kerja tahapan dapat dilihat pada Gambar 1.



Gambar 1. Tahapan *penetration testing*

Pada gambar diatas dapat dilihat tengang tahapan dalam metode *pentration testing* terbagi menjadi beberapa langkah yaitu:

1. *Planning*

   Tahap pertama adalah *planning*, yang bertujuan untuk memastikan pengujian berjalan sesuai dengan tujuan dan tidak mengganggu operasional sistem yang diuji. Pada tahap ini, dilakukan identifikasi tujuan pengujian, lingkup sistem yang akan diuji (misalnya, jumlah perangkat yang terdiri dari 1 router utama dan 4 perangkat klien), serta risiko yang mungkin terjadi. Diskusi dengan pemilik sistem menjadi bagian penting dalam perencanaan, untuk memperoleh izin dan menjelaskan batasan pengujian, seperti waktu pelaksanaan dan protokol yang tidak boleh terganggu. Keberhasilan tahap ini ditandai dengan tersusunnya rencana kerja yang disepakati oleh semua pihak terkait.
2. *Information Gathring*

   Tahap ini berfokus pada pengumpulan informasi mengenai target jaringan yang akan diuji. Informasi yang dikumpulkan meliputi konfigurasi jaringan seperti *SSID*, alamat IP, jenis enkripsi, serta perangkat keras yang digunakan, seperti vendor dan model *router*. Pengumpulan data dilakukan dengan menggunakan alat seperti *airodump-ng*, yang dapat menangkap paket data dari jaringan untuk analisis lebih lanjut. Keberhasilan tahap ini ditandai dengan diperolehnya informasi yang cukup untuk melanjutkan ke tahap analisis kerentanan, seperti konfigurasi *default* yang masih digunakan oleh perangkat.
3. *Vulnerability Analysis*

   Setelah informasi target terkumpul, dilakukan *vulnerability analysis* untuk mengidentifikasi potensi kerentanan pada jaringan. Proses ini melibatkan pemindaian jaringan menggunakan alat seperti *airodump-ng* dan *nmap* untuk mencari celah keamanan, seperti *port* terbuka, konfigurasi *default*, atau kelemahan enkripsi. Analisis ini penting untuk menentukan kerentanan yang dapat dimanfaatkan pada tahap berikutnya. Keberhasilan tahap ini ditandai dengan ditemukannya minimal satu kerentanan

DOI : https://doi.org/10.36341/rabit.v10i1.5387 *Corresponding Author* : Fahmi Fachri

signifikan yang dapat dieksploitasi, seperti kata sandi lemah atau layanan tidak aman.

4. *Exploitation*

   Tahap ini adalah inti dari pengujian penetrasi, di mana kerentanan yang telah diidentifikasi dimanfaatkan untuk mendapatkan akses ke jaringan. Teknik *dictionary attack* digunakan untuk mencoba menebak kata sandi jaringan dengan memanfaatkan file *handshake* yang telah ditangkap sebelumnya. Alat *Aircrack-ng* digunakan dalam proses ini untuk memeriksa kata sandi dari *wordlist* yang disiapkan sebelumnya (berisi 1.000 kemungkinan kata sandi umum). Keberhasilan tahap ini ditandai dengan diperolehnya kata sandi jaringan, yang menunjukkan bahwa jaringan tersebut rentan terhadap serangan.

5. *Reporting*

   Tahap terakhir adalah *reporting*, di mana semua temuan dari pengujian dirangkum dalam laporan tertulis. Laporan mencakup deskripsi kerentanan yang ditemukan, tingkat risiko, serta rekomendasi tindakan perbaikan, seperti penggunaan kata sandi yang lebih kompleks atau pembaruan protokol keamanan. Laporan ini disusun dalam format yang mudah dipahami oleh pemilik sistem dan disertai dengan bukti hasil pengujian. Keberhasilan tahap ini ditandai dengan diterimanya laporan oleh pemilik sistem sebagai dasar untuk tindakan mitigasi lebih lanjut.

HASIL

1. *Planning*

Pada tahap planning ini akan dilakukan persiapan mengenai alat dan bahan yang akan digunakan untuk *penetration testing*. Dalam penelitian ini peneliti akan menargetkan jaringan nirkabel yang berada pada pondok pesantren Al-Hidayah Kebumen. Bahan yang diperluan yaitu *wordlist* yang digunakan untuk uji coba dengan teknik *directonary attack*. Dalam pembuatan *wordlist* terebut peneliti akan memanfaatkan *tools* dari *kali linux* yang bernama CUPP (*Common User Password Profiler*) untuk membuat *wordlist* berdasaran kata dan aturan yang dimasukan.

Gambar 2. Tahapan CUPP

Penelitian ini menggunakan alat yang sesuai untuk pengujian *penetration testing*, seperti adaptor TP-Link TL-WN722N, yang memungkinkan pengambilan paket data menggunakan mode monitor dan *injection*. Pemilihan alat yang tepat seperti ini penting untuk memastikan hasil yang akurat dalam uji penetrasi. Adapter ini dipilih karena model ini menggunakan chpset Ateros yang mendukung mode monitor dan *injection packet*.

Gambar 3. Adaptor TL-WN722N

2. *Information Gathering*

Seteleh alat dan bahan sudah disapkan, selanjutnya akan dilakukan proses *information gathring*. Pada proses ini kami akan menggunakan *Airodump-ng* yang merupakan salah satu fitur dari *tools Aircrack-ng*. Informasi yang didapatkan setelah menjalankan *Airodump-ng* yaitu SSID dari jaringan, BSSID, *channel, encoder,* dan *encryption type*.

Gambar 4. Hasil monitoring menggunakan *airodump-ng*

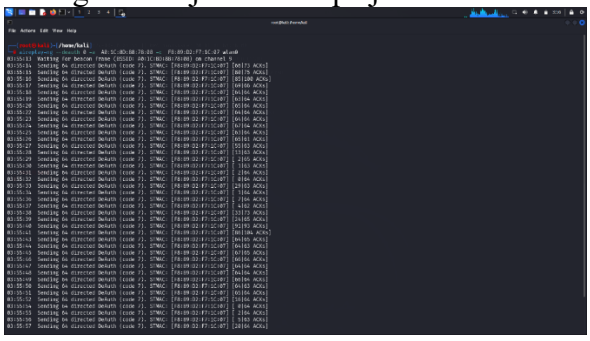
Hasil monitoring dengan menggunakan *Airoduimp-ng* tersebut akan mendapatkan informasi penting dalam proses pengujian jaringan. Pada gambar 4 diatas dapat diketahui

DOI : https://doi.org/10.36341/rabit.v10i1.5387
Corresponding Author : Fahmi Fachri

bahwa jaringan menggunakan *encoder* WPA2 dengan *encryption type* PSK sehingga jaringan tersebut menggunakan sistem keamanan setandar dari WPA2-PSK. Selain itu dapat dilihat pula *channel*, SSID dan BSSID dari jaringan tersebut.

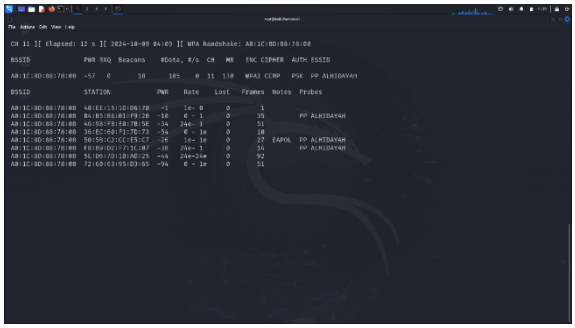
3. *Vulnerability Analysis*

Setelah mendapatan informasi yang dibutuhkan, selanjutnya akan dilakukan *sniffing* pada jaringan agar mendapatkan file *.cap* dari hasil *WPA handsake* yang dijalankan antara *access point* dengan perangkat sekitar. Pada tahap ini memerlukan bantuan adaptor TP-Link TL-WN722N yang digunakan untuk perantara antara kali linux dan *Acces point* jaringan yang diuji. Selanjutnya dengan menggunakan 2 fitur dari *Aircrack-ng* yaitu *Airoduimp-ng* dan *areplay-ng* dapat dilakukan *de-auntethacion* pada BSSID sekaligus melakukan monitor pada BSSID yang dituju sehingga di dapatkan *WPA-Handsake* yang tersimpan dalam file dengan ekstensi *.cap*. Dengan Menggunakan file *.cap* dari handshake WPA2, serangan cracking pada kata sandi sederhana dapat diselesaikan dalam waktu sekitar 30 detik hingga 5 menit, tergantung pada kompleksitas kata sandi dan perangkat yang digunakan. Jika kata sandi yang digunakan terdiri dari 12 karakter dengan kombinasi angka, huruf, dan simbol, waktu yang dibutuhkan untuk memecahnya dapat meningkat menjadi beberapa jam



Gambar 5. Proses *de-authentatication*

Pada gambar 5 diatas ditunjukan proses *de-authentaticaton* dengan menggunakan aireplay-ng untuk BSSID A0:1C:8D:88:78:08, yang merupakan BSSID dari SSID PP ALHIDAYAH yang telah dilacak sebelumnya.



Gambar 6. Proses penangkapan *capture handsake*

Pada gambar 6 tersebut menujukan proses penangkapan *capture handsake* setelah menjalankan *Airoduimp-ng* pada SSID PP ALHIDAYAH telah berhasil ditandai dengan adanya *WPA Handsake* yang terjadi pada saat penangkapan ini terjadi.

4. *Exploitation*

Setelah file *.cap* sudah diperoleh, maka dapat dilakukan peretasan *password* yang terdapat pada file *.cap* dengan menggunakan *Aircrack-ng* yang dipadukan dengan *wordlist* yang telah disiapkan sebelumnya dengan menggunakan *tools* CUPP (*Common User Password Profiler*).

Gambar 7. Proses penangkapan *capture handsake*

Pada gambar 7 tersebut menujukan bahwa *password* dari Wi-Fi dengan SSID PP ALHIDAYAH yang di enkripsi dengan keamanan WPA2-PSK berhasil diperoleh menggunakan *Aircrack-ng*. Dapat diketahui bahwa *password* dari SSID PP ALHIDAYAH yaitu “pkb12345”. Dengan kata sandi tersebut, waktu yang diperlukan untuk memecahnya menggunakan serangan brute force adalah kurang dari 1 menit pada perangkat dengan spesifikasi menengah.

5. *Reporting*

Tahapan yang terakhir dalam mtode *penetration testing* yaitu *reporting*. Hasil pengujian pada SSID PP ALHIDAYAH menujukan bahwa jaringan ini rentan terhadap

DOI : https://doi.org/10.36341/rabit.v10i1.5387 *Corresponding Author* : Fahmi Fachri

serangan yang telah dilakukan. Hasil pengujian jaringan menggunakan metode *penetration testing* ditunjukan pada Tabel 1 dibawah ini.

Tabel 1. Hasil pengujian *penetration testing*

No	Jenis serangan	Data yang dibutuhkan	Keterangan
1	*De-authenticati on Attack*	BSSID, Channel, dan Client BSSID	Berhasil
2	*Capture Handshake*	BSSID dan Channel	Berhasil
3	*WPA/WPA2 Cracking*	Handsake dan Wordlist	Berhasil

Hasil dari *penetration testing* yang telah dilakukan menunjukkan bahwa jaringan memiliki beberapa kerentanannya, antara lain:

1. Keamanan jaringan yang lemah ditunjukkan dengan penggunaan kata sandi yang terlalu sederhana dan mudah ditebak.
2. Tidak adanya enkripsi yang kuat. Penggunaan protokol keamanan yang lemah atau bahkan tidak terkonfigurasi dengan benar, sehingga memudahkan peretas dalam melakukan penetrasi.
3. Kurangnya pemantauan. Tidak adanya sistem pemantauan yang efektif, sehingga memungkinkan peretas untuk dengan mudah melakukan serangan tanpa terdeteksi.

Untuk mengatasi kerentanannya, terdapat beberapa solusi yang dapat diterapkan, yaitu:

1. Gunakan kata sandi yang kuat. Pastikan kata sandi yang digunakan terdiri dari kombinasi huruf besar, huruf kecil, angka, dan karakter khusus. Hindari menggunakan kata-kata yang mudah ditebak, seperti nama, tanggal lahir, atau kata-kata umum yang sering digunakan. Kata sandi yang kuat akan meningkatkan waktu yang diperlukan untuk memecahnya menggunakan serangan *brute force* atau *dictionary attack*. Dengan kata sandi yang lebih kompleks dan panjang (lebih dari 12 karakter), dapat mengurangi kemungkinan jaringan terkena serangan yang berhasil.
2. Aktifakan enkripsi WPA3. WPA3 adalah protokol keamanan Wi-Fi terbaru yang menawarkan perlindungan lebih kuat dibandingkan WPA2. WPA3 menyertakan fitur-fitur seperti perlindungan terhadap serangan *brute force* dan lebih aman dalam menangani data sensitif. Jika perangkat mendukung WPA3, mengaktifkannya akan memberikan lapisan perlindungan yang lebih baik terhadap serangan yang mencoba menebak password atau memanfaatkan celah dalam protokol WPA2.
3. Perbarui *firmware router*. Pastikan *firmware router* selalu diperbarui ke versi terbaru untuk mendapatkan pembaruan keamanan yang penting. Pembaruan *firmware* sering kali menyertakan perbaikan *bug* dan tambalan keamanan yang mengurangi potensi kerentanannya.
4. Gunakan *firewall*. *Firewall* adalah alat yang sangat berguna untuk melindungi jaringan dari serangan luar. Dengan menggunakan *firewall*, dapat memblokir akses yang tidak sah dan melindungi data di dalam jaringan. Pastikan *firewall* dikonfigurasi dengan benar untuk memfilter lalu lintas yang mencurigakan dan mencegah peretas mendapatkan akses ke jaringan.
5. Aktifkan fitur keamanan tambahan**.** Banyak router modern memiliki fitur keamanan tambahan, seperti *WPS (Wi-Fi Protected Setup)* dan *MAC filtering. WPS* dapat mempermudah proses koneksi perangkat ke jaringan, namun jika tidak dikonfigurasi dengan benar, dapat menjadi celah bagi peretas untuk mendapatkan akses ke jaringan. *MAC filtering* dapat membatasi perangkat yang dapat terhubung ke jaringan berdasarkan alamat *MAC* mereka, namun fitur ini harus digunakan dengan hati-hati karena dapat membatasi fleksibilitas jaringan.

DOI : https://doi.org/10.36341/rabit.v10i1.5387 *Corresponding Author* : Fahmi Fachri

KESIMPULAN

Berdasarkan hasil penelitian keamanan jaringan menggunakan metode penetration testing dengan *Aircrack*-ng pada jaringan nirkabel di Pondok Pesantren Al-Hidayah Kebumen, ditemukan bahwa jaringan tersebut masih memiliki beberapa kerentanannya. Kerentanannya antara lain adalah keamanan jaringan yang lemah, tidak adanya enkripsi yang kuat, dan kurangnya pemantauan yang efektif. Untuk mengatasi kerentanan tersebut, solusi yang dapat diterapkan meliputi penggunaan kata sandi yang kuat, pengaktifan enkripsi WPA3, pembaruan *firmware router*, penggunaan *firewall*, aktivasi fitur keamanan tambahan, serta pelaksanaan audit keamanan secara berkala.

Kontribusi utama dari penelitian ini adalah memberikan pemahaman yang lebih mendalam mengenai kerentanannya pada jaringan nirkabel dan pentingnya langkah-langkah preventif dalam meningkatkan keamanan jaringan. Dengan hasil penelitian ini, diharapkan dapat membantu instansi atau individu dalam mengambil tindakan yang tepat untuk memperkuat keamanan jaringan mereka, serta memberikan kontribusi signifikan terhadap pengembangan kebijakan dan praktik terbaik di bidang keamanan jaringan.

DAFTAR PUSTAKA

[1] R. Febriyana, Y. Muhyidin, and D. Singasatia, "Analisis Keamanan Jaringan Pada Router Huawei Hg8245h5 Dan Repeater Mercusys Mw300re Menggunakanwi-Fi Deuther Untuk Uji Keamanan Wpa2/Psk Dengan Metodepenetration Testing," *Sci. J. Ilm. Sains dan Teknol.*, vol. 2, no. 11, pp. 176–192, 2024, Accessed: Oct. 20, 2024. [Online]. Available: https://jurnal.kolibi.org/index.php/scientica/article/view/2749

[2] T. Rahman, I. Z. Nibras, and S. Sumarna, "Monitoring Adminstrasi Jaringan Dengan Mikrotik Dan Telegram Bot Pada Internet Service Provider," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 9, no. 2, pp. 162–172, 2024.

[3] A. Gumara, F. C. A. Uguy, A. R. Fitria, and R. Abdillah, "Pengaruh Media Sosial Terhadap Kesehatan Mental Dewasa Awal di Bekasi," *Obs. J. Publ. Ilmu Psikol.*, vol. 2, no. 4, pp. 48–57, 2024.

[4] M. A. Rizkiawan and H. Ramza, "Analisis Quality Of Sevice Jaringan Nirkabel Menggunakan Wireshark Dengan Metode Action Research," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 8, no. 5, pp. 9876–9882, 2024.

[5] F. Wadly, R. Septian, and Z. Ramadhan, "Strategi Penanggulangan Kelemahan Terhadap Ancaman Keamanan Pada Jaringan Wireless," *J. Nas. Teknol. Komput.*, vol. 3, no. 2, pp. 59–67, 2023.

[6] H. Aspriyono and A. Susanto, *Jaringan komputer dan perkembangannya*. Penerbit Andi, 2024.

[7] A. R. Raharja, M. M. ST, and M. Kom, *Keamanan Jaringan*. Penerbit Kbm Indonesia, 2024.

[8] H. Haeruddin and A. Kurniadi, "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6)," in *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences*, 2021, pp. 508–515.

[9] S. E. Prasetyo and T. Windranata, "Perbandingan Sistem Autentikasi Wpa2 Eap-Psk Pada Jaringan Wireless Dengan Metode Penetration Testing Menggunakan Fluxion Tools," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 7, no. 1, pp. 43–51, 2022.

[10] A. A. Chandra, A. T. Zy, and A. Nugroho, "Penerapan Teknik Penetration Testing Terhadap Cross Site Scripting (XSS) Dalam Pengembangan Website," *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 9, no. 2, pp. 262–270, 2024.

[11] R. W. Ismail and R. Pramudita, "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekasi," *J.*

Mhs. Bina Insa., vol. 5, no. 1, pp. 53–62, 2020.

[12] T. Yusnanto, M. A. Muin, and S. Wahyudiono, "Analisa Infrastruktur Jaringan Wireless dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux," *J. Educ.*, vol. 4, no. 4, pp. 1470–1476, 2022.

[13] I. M. P. Utama, K. R. Putri, A. A. E. Wirayuda, V. A. T. P. Herlambang, I. M. E. Listartha, and G. A. J. Saskara, "Analisis Perbandingan Kinerja Tool Website Directory Brute Force dengan Target Website DVWA," *Inform. J. Ilmu Komput.*, vol. 18, no. 3, pp. 278–285, 2022.

[14] J. Syahronny and A. Tedyyana, "Analisis Keamanan Wireless Terhadap Serangan Denial of Service menggunakan Metode Penetration Testing pada Dinas XYZ," *TEKTONIK J. Ilmu Tek.*, vol. 1, no. 4, pp. 417–428, 2024.

[15] D. E. Faishol, T. A. Cahyanto, and M. Rahman, "Analisis Dan Evaluasi Protokol Keamanan Jaringan Nirkabel Wi-Fi Protected Access 3 dengan Metode Penetration Testing," *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, vol. 9, no. 1, pp. 420–432, 2024.

DOI : https://doi.org/10.36341/rabit.v10i1.5387 *Corresponding Author* : Fahmi Fachri