JURNAL RESPONSIF, Vol. 4 No.2 Agustus 2022, pp. 162~167
E-ISSN**:** 2685-6964

PENERAPAN METODE *PENETRATION TESTING* PADA KEAMANAN JARINGAN NIRKABEL

Nugroho Adhi Santoso[1], Muhamad Ainurohman[2], Rifki Dwi Kurniawan[3]

[1]STMIK YMI TEGAL
e-mail:nugrohoadisantoso29@gmal.com

[2]STMIK YMI TEGAL
e-mail: ainurohman24@gmail.com

[3]STMIK YMI TEGAL
e-mail: rifki.dk@gmail.com

Abstrak

Penerapan Keamanam jaringan nirkabel merupakan sebuah sistem yang digunakan untuk meindentifikasi dan melakukan pencegahan pencurian data dan informasi pada jaringan komputer. Kekurangan jaringan nirkabel menjadi semua pengguna dapat mendeteksi sinyal radio sesuai jenis frekuensi beberapa tools yang tersedia secara bebas di internet untuk mendapatkan hak akses kontrol secara tidak sah. Metode yang digunakan pada penelitian ini adalah *penetration testing* untuk menguji keamanan jaringan nirkabel di SMK Bhakti Praja Adiwerna Kabupaten Tegal dengan batasan pada frekuensi 2,4 GHZ dan 5 GHZ, Dengan Berbagai macam ketegori perangkat jaringan *router* dan *Acces point*. Tujuannya untuk Menguji keamanan pada jaringan nirkabel menggunakan tools yang tersedia pada sistem operasi kali linux versi 2021.1. Hasil dari penelitian ini dapat disimpulkan bahwa metode *penestrasion testing* mempunyai suatu kelebihan dapat menguji jaringan Nirkabel dan dapat menindetenfikasi WPA Key dengan database *Wordlist* sehingga dapat menjadi bahan untuk penerapan Keamanan pada jaringan nirkabel.

Keywords*: Jaringan Nirkabel, Penetration testing, Kali Linux 2021.1*

Abstract

The application of wireless network security is a system used to identify and prevent the theft of data and information on computer networks. The weakness of the wireless network is that all users can detect radio signals according to the type of frequency, some tools are freely available on the internet to obtain access control rights illegally. The method used in this study is penetration testing to test the security of the wireless network at SMK Bhakti Praja Adiwerna, Tegal Regency with a frequency limit of 2.4 GHZ and 5 GHZ, with various categories of router and access point network devices. The aim is to test security on a wireless network using the tools available on the Kali Linux operating system version 2021.1. The results of this study can be concluded that the penetration testing method has the advantage of being able to test wireless networks and can identify WPA Key with a Wordlist database so that it can be used as material for implementing security on wireless networks.

Keywords*: Wireless Network, Penetration Testing, Kali Linux 2021.*

1. Pendahuluan

Jaringan komputer merupakan sebuah sistem di mana dapat menghubungkan beberapa komputer untuk bertukar data dan informasi yang bersamaan (Saskara et al., 2019). Jaringan nirkabel atau jaringan area lokal *nirkabel* (*WLAN*). Pada bidang *Wi-Fi* digunakan teknologi jaringan nirkabel di SMK Bhakti Praha Adiwerna Kabupaten Tegal Siswa dan guru mungkin tidak memperhatikan keamanan komunikasi data dalam jaringan nirkabel yang dibangun. Oleh karena itu, banyak peretas dan pengguna yang dapat menyalahgunakan jaringan nirkabel secara ilegal tertarik untuk menguji Keamananya. Mengingat keamanan jaringan nirkabel lebih rentan dari segi keamanan daripada jaringan kabel, maka perlu dibuat sistem keamanan pada institusi

Naskah diterima 10 Agustus 2022; direvisi 24 Agustus 2022; diterbitkan 30 Agustus 2022

pendidikan untuk menjaga keamanan data Anda di jaringan nirkabel (Bayu et al., 2017).

Pengujian penetrasi adalah metode pengujian yang digunakan untuk menguji kerentanan sistem dan mengidentifikasi kerentanan keamanan dan konfigurasi, kelemahan perangkat keras dan perangkat lunak , dan kelemahan proses operasional dan penanggulangan teknis. Pengujian penetrasi dilakukan secara manual atau otomatis (Hussain et al., 2017). Kali Linux adalah sistem operasi distribusi Linux canggih untuk pengujian penetrasi. Kali Linux adalah ekstensi lengkap dari sistem operasi *BackTrack Linux* (Rusdi & Prasti, 2019).

Jaringan Komputer merupakan komputer terdiri dari lebih dari satu komputer atau perangkat jaringan yang dapat saling berkomunikasi dan bertukar data (Asmania & Ariyadi, 2020). Ada beberapa jenis jaringan komputer berdasarkan wilayah kerjanya, yang dapat dibagi menjadi tiga *topologi*:

a. Arsitektur *Local Area Network (LAN*) merupakan topologi dari jaringan komputer yang tersebar di suatu area. B. Komputer kantor dalam satu ruangan atau gedung yang sama.
b. Arsitektur *Metropolitan Area Network (MAN*) merupakan topologi dari jaringan komputer yang saling terhubung di dalam kota. Jaringan MAN menghubungkan *LAN* Anda ke jaringan *LAN* Kota atau Kabupaten.
c. *Arsitektur Wide Area Network (WAN)* merupakan topologi dari jaringan komputer yang menghubungkan berbagai kota dalam suatu negara melalui *ISP*, memungkinkan komputer untuk berkomunikasi melintasi jarak antar negara dan benua (Asmania & Ariyadi, 2020).

Uji penetrasi adalah serangan jaringan yang disimulasikan pada sistem komputer untuk mengungkap kerentanan, ancaman, dan risiko dalam aplikasi perangkat lunak, jaringan, atau aplikasi *web* yang dapat digunakan penyerang (Haeruddin & Kurniadi, 2021).

Keamanan jaringan komputer sangat penting untuk mengontrol akses jaringan dan mencegah penggunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikendalikan oleh administrator jaringan Dari sudut pandang keamanan, lima poin didefinisikan. Artinya, kerahasiaan, informasi (data) yang diperlukan hanya dapat diakses oleh pihak yang berwenang, integritas, informasi yang diperlukan hanya dapat diubah oleh pihak yang berwenang, ketersediaan, diperlukan informasi yang tersedia Peserta memiliki kewenangan sesuai kebutuhan, otentikasi, identifikasi yang benar pengirim informasi, jaminan bahwa ID yang diperoleh tidak dipalsukan, non-penyangkalan, pengirim informasi Menerima pesan, meminta penerima juga tidak dapat menolak untuk mengirim (Santoso, 2019). Penerapan Keamanan jaringan nirkabel sebagai bagian dari sistem menjadi peningkatan untuk menjaga keamananan data dan integritas data (Jufri & Heryanto, 2021). Keamanan Jaringan Nirkabel untuk Perangkat *AP (Access Point)* Metode keamanan umum adalah *WEP (Wired Equivalent Privacy), WPA (WI-FI Protected Access)*, dan *WPA2 (WI-FI Protected Access 2),* yang merupakan jaringan nirkabel. hampir semua pengguna. Rata-rata penggunaan perangkat *AP* menggunakan metode standar pabrikan (Hermanto & Anam, 2020).

Keamanan *WLAN* Protokol *WLAN* yang digariskan oleh *IEEE* terdiri dari tiga standar keamanan: *Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), dan Wi-Fi Protected Access 2 (WPA2). Wired Equivalent Privacy (WEP) IEEE 802.11* mengembangkan *WEP* pada tahun 1999 untuk memberikan keamanan pada jaringan nirkabel dibandingkan dengan jaringan kabel Enkripsi *WEP* didasarkan pada enkripsi aliran *RC4* simetris dengan kunci enkripsi *40-bit* dan *104-bit WEP. Wi-Fi Protected Access (WPA) Wi-Fi Alliance* menciptakan *WPA* pada tahun 2003 untuk meningkatkan kerentanan *WEP* dan keberadaan kerentanan *WPA* menggunakan algoritma hash yang disebut Protokol Integritas Kunci *Temporal* (*TKIP*) untuk meningkatkan enkripsi data. TKIP mengenkripsi kunci dan menambahkan fitur pemeriksaan integritas untuk mencegah gangguan dengan kunci terenkripsi *Wi-Fi Protected Access 2 (WPA 2) Wi-Fi Alliance* meningkatkan *WPA* pada tahun 2004 dengan merancang 802.11i (*WPA2*), yang menggunakan konsep *Robust Security Network* (*RSN*) (Kissi & Asante, 2020).

Group 802.11i melengkapi metode keamanan *IEEE* yang telah ditentukan sebelumnya. Perkembangan ini disebut *WPA2. WPA2* digunakan sebagai tingkat keamanan tertinggi saat menerapkan keamanan kriptografi. Aplikasi keamanan utama untuk enkripsi di *WPA2* adalah enkripsi *AES. AES* lebih kompleks daripada

RC4 WEP. Menggunakan *WPA2* membutuhkan perangkat keras baru yang dapat meningkatkan dan mendukung komputasi yang ditangani oleh *WPA2*. Oleh karena itu, tidak semua adaptor mendukung tingkat keamanan *WPA2* ini. Mode keamanan *WPA2-PSK* menawarkan dua jenis enkripsi: *TKIP* dan *AES*. Protokol integritas kunci sementara (tkip) menggunakan metode enkripsi yang lebih aman, dan menggunakan mikrofon (kode integritas *token*) untuk melindungi jaringan anda dari serangan (Baihaqi et al., 2018).

Nirkabel adalah jaringan nirkabel yang saling terhubung melalui gelombang *radio* atau nirkabel. Keunggulan teknologi ini digabungkan tanpa menggunakan kabel atau perangkat elektronik lainnya sebagai media transmisi (Sabdho & Maria, 2018).Dari sini dapat disimpulkan bahwa topologi jaringan nirkabel adalah jaringan nirkabel yang terhubung melalui gelombang radio. Teknologi ini terhubung tanpa kabel atau perangkat elektronik lainnya sebagai media transmisi pertukaran data dan informasi (Mulyanto et al., 2022). Pada jaringan komunikasi nirkabel dapat diukur dengan berbagai parameter seperti jarak jangkauan, indikator kekuatan sinyal yang diterima (*RSSI*), *throughput*, dan *delay*. *RSSI* adalah ukuran kekuatan sinyal radio yang diterima oleh penerima. Faktor jarak antara pemancar dan penerima terutama menentukan *RSSI*) (Rofii et al., 2018).

Manfaat adanya Sistem operasi yaitu mengelola perangkat keras komputer. Perangkat Keras harus menyediakan mekanisme yang sangat penting untuk memastikan pengoperasian sistem komputer berjalan dengan benar. Peranan Sistem Operasi merupakan bagian terpenting pada komputer . interaksi antara perangkat dengan perangkat keras komputer (Putri, 2021).

Kali Linux (Kali) adalah *sistem* operasi distribusi *Linux* yang dikembangkan dengan fokus pada tugas pengujian penetrasi. *Kali Linux* sebelumnya dikenal sebagai *BackTrack*. Ini mengintegrasikan tiga distribusi pengujian penetrasi *Linux* yang berbeda: *IWHAX*, *WHOPPIX*, dan *Auditor*. *BackTrack* adalah salah satu sistem distribusi Linux paling populer, terbukti dengan jumlah unduhan melebihi 4 juta di *BackTrack Linux 4.0* pra-final. Linux (Bayu et al., 2017).

2. Metode Penelitian

Pada Penelitian ini menggunakan metode uji penetrasi. Tahapan investigasi yang merupakan langkah-langkah yang dilakukan dalam uji penetrasi adalah sebagai berikut:

Gambar 1. Metode Penetrasion Testing

a. *Planning and Preparation*
Mendefinisikan ruang lingkup dan tujuan pengujian, termasuk sistem yang akan ditangani dan metodologi pengujian yang akan digunakan Kumpulkan data (nama domain jaringan dan *server, server email.)* untuk lebih memahami cara kerja target dan potensi kerentanan. Langkah pertama adalah pada saat proses pengujian rencana awal dan Pekerjaan persiapan berfokus pada mengidentifikasi kerentanan dan secara bertahap meningkatkan keamanan.

b. *Reconnasissance*
Reconnaissance, atau yang biasa disebut dengan pengumpulan data, tergolong uji intrusi data pasif karena pengumpulan data dilakukan secara manual, melalui dokumentasi atau informasi publik yang relevan, atau dengan bertanya langsung kepada pemangku kepentingan yang *terlibat* dalam sistem.

c. *Discovery*
Discovery adalah langkah mengumpulkan informasi menggunakan alat otomatis dari sistem pemindaian untuk menemukan kerentanan, termasuk pemindaian jaringan, *server*, perangkat, dan data. Langkah selanjutnya adalah memahami bagaimana target merespons berbagai upaya penyusupan.

d. *Analyzing information and risk*
Ini adalah *fase* di mana Anda menganalisis informasi terperinci yang diperoleh sebelumnya tentang risiko (*fase* pengintaian dan deteksi) dan kerentanan keamanan. Dari jumlah tersebut,dapat

disebabkan oleh kerentanan dalam sistem yang diinstal.

e. *Active intrusion attempts*
Ini adalah *fase*, yang secara aktif memberikan beberapa instruksi dari perspektif keamanan sistem sehingga kerentanan yang terdeteksi dapat diperbaiki atau diperbarui.

f. *Final analysis*
Analisis keseluruhan akhir memberikan pedoman teknis untuk meningkatkan keamanan berdasarkan semua temuan dan rencana analisis sistematis.

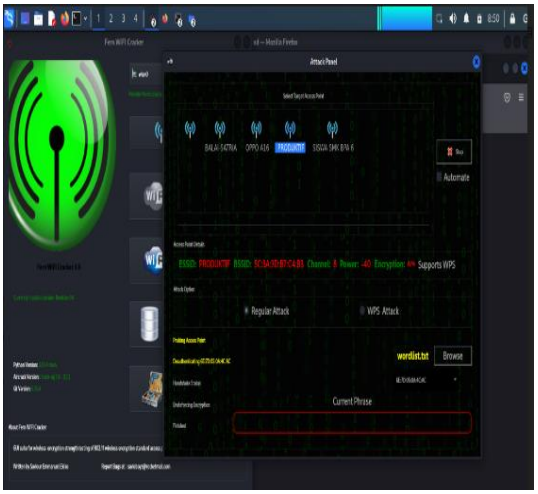
g. *Report preparation*
Langkah terakhir dalam kegiatan pengujian penetrasi ini adalah memberikan laporan temuan. Laporan ini diberikan kepada semua pihak yang terlibat dan bertanggung jawab terhadap sistem dan digunakan sebagai acuan untuk meningkatkan keamanan sistem.

3. Hasil dan Pembahasan

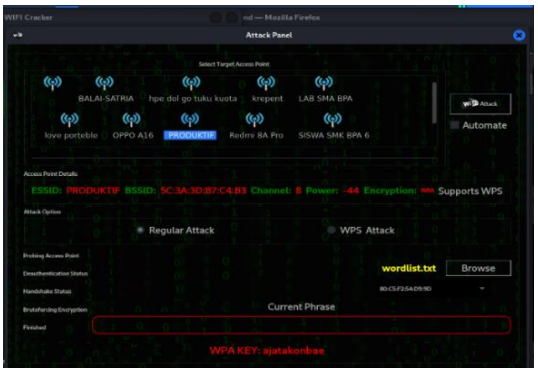
Pengujian ini menargetkan jaringan nirkabel SMK Bhakti Praja Adiwerna Kabupaten Tegal. Pada tahap ini penulis menggunakan sistem operasi dengan *Live* Mode yang terinstall pada laptop melalui *USB* yaitu sistem operasi *Kali Linux.* Tes berjalan dalam tiga fase berbeda:

3.1 *Cracking The Encryption*

Langkah pertama dalam prosedur pengujian penetrasi adalah memastikan bahwa semua titik akses dilindungi oleh sistem keamanan *terenkripsi (WEP, WPA, WPA2-PSK,).*Oleh karena itu penulis menggunakan *tools Fren Wifi Cracker* untuk menargetkan enkripsi *WPA2-PSK* sebagai target *SSID* PRODUKTIF dan *SSID* SMK BHAKTI PRAJA ADIWERNA. Jika berhasil, akan tampilan seperti pada Gambar 2 dan Gambar 3 sebagai hasil.



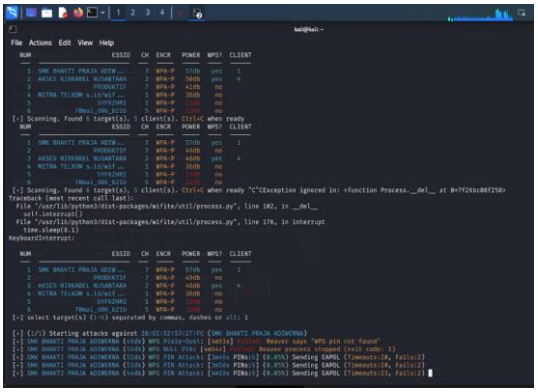
Gambar 2. Tampilan *Fren Wifi Cracker.*



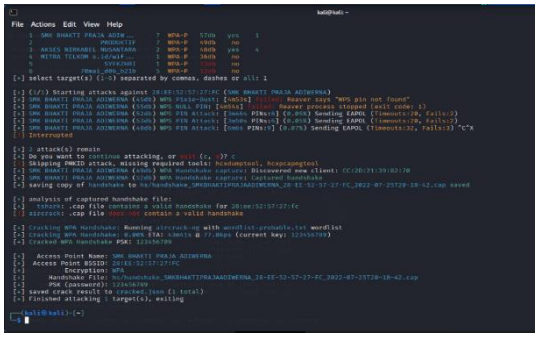
Gambar 3. Hasil *Cracker Wifi WPA Key*

3.2 *Attacking WPA key*

Pada tahap kedua, *SSID* SMK Bhakti Praja Adiwerna diuji dalam *mode CLI* menggunakan alat *tools aircrack-ng.*



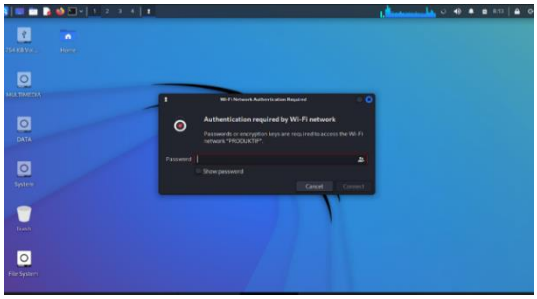
Gambar 4. Proses *Attack SSID.*



Gambar 5. Hasil *Attack SSID.*

3.3 *Authentication Wifi Password*

Pada Tahap Ketiga menguji *WPA key* yang sudah di dapat dari hasil *Cracker SSID* dan *Attack SSID* di tampilkan pada Gambar 5.



Gambar 6. *Authentication Wifi Password.*

Untuk menyelidiki kerentanan kunci *WPA Key* ,hasil pengujian pada jaringan ini menunjukkan bahwa *WLAN* SSID PRODUKTIF dan SSID SMK BHAKTI PRAJA ADIWERNA sangat rentan terhadap tiga tingkat serangan. Secara umum, Tabel 1 menunjukkan hasil penggunaan metode pengujian penetrasi .

Tabel 1.Hasil Penetrasi Jaringan Nirkabel.

Kategori Serangan	Data yang dibutuhkan	Keterangan
Cracking The Encryption	*Wordlist database Password*	Berhasil
Attacking WPA key	*Wordlist database Password*	Berhasil
Authentication Wifi Password	*Wpa Key Hasil Attacking WPA Key*	Berhasil

4. **Kesimpulan**

Berdasarkan hasil penelitian dengan menggunakan metode pengujian penetrasi menggunakan Kali *Linux* (studi kasus: SMK BHAKTI PRAJA ADIWERNA) keamanan jaringan menggunakan metode pengujian penetrasi pada jaringan nirkabel . Sistem ini memiliki banyak kelemahan karena masih menggunakan password yang dapat dibobol atau diserang. Oleh karena itu perlu dilakukan penguatan keamanan jaringan *wireless* SMK Bhakti Praja Adiwerna Kabupaten Tegal dengan melakukan konfigurasi yang lebih aman dan penambahan kunci *WPA Key* dengan kombinasi angka.

Referensi

Asmania, & Ariyadi, T. (2020). Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel Pada Kejaksaan Tinggi Sumatera Selatan. *Bina Darma Conference on Computer Science*, 76–86.

Baihaqi, Yanti, Y., & Zulfan. (2018). Implementasi Sistem Keamanan WPA2-PSK pada Jaringan WiFi. *Jurnal Serambi Engineering*, *3*(1), 248–254. https://doi.org/10.32672/jse.v3i1.353

Bayu, I. K., Yamin, M., & Aksara, L. F. (2017). Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO. *SemanTIK*, *3*(2), 69–78.

Haeruddin, & Kurniadi, A. (2021). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus: TP-Link Archer A6). *CoMBInES-Conference on Management …*, *1*(1), 508–515.

Hermanto, D., & Anam, M. S. (2020). Implementasi Sistem Keamanan Hotspot Jaringan Menggunakan Metode OpenSSL (Secure Socket Layer). *Jurnal CoreIT*, *6*(1), 57–64.

Hussain, M. Z., Hasan, M. Z., & Taimoor, M. C. A. (2017). Penetration Testing In System Administration. *International Journal of Scientific & Technology Research*, *6*(6), 275–278.

Jufri, M., & Heryanto. (2021). Peningkatan Keamanan Jaringan Wireless Dengan Menerapkan Security Policy Pada Firewall. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *5*(2), 98–108. https://doi.org/10.35145/joisie.v5i2.1759

Kissi, M. K., & Asante, M. (2020). Penetration Testing of IEEE 802.11 Encryption

Protocols using Kali Linux Hacking Tools. *International Journal of Computer Applications*, *176*(32), 26–33. https://doi.org/10.5120/ijca2020920365

Mulyanto, Y., Herfandi, & Kirana, R. C. (2022). Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing. *JINTEKS*, *4*(1), 26–35.

Putri, R. A. (2021). Aplikasi Simulasi Algoritma Penjadwalan Sistem Operasi. *Jurnal Teknologi Informasi*, *5*(1), 98–102. https://doi.org/10.36294/jurti.v5i1.2215

Rofii, F., Fachrudin, H., & Sholawati, S. (2018). Kinerja Jaringan Komunikasi Nirkabel Berbasis Xbee pada Topologi Bus, Star dan Mesh. *ELKOMIKA*, *6*(3), 393. https://doi.org/10.26760/elkomika.v6i3.393

Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. *Seminar Nasional Teknologi Informasi Dan Komputer 2019*, 260–269.

Sabdho, H. D., & Maria, U. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. *Semhavok*, *1*(1), 15–24.

Santoso, J. D. (2019). Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System. *Infos*, *1*(3), 44–50.

Saskara, G. A. J., Indrawan, I. P. O., & Putra, M. P. (2019). Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru. *Jurnal Pendidikan Teknologi Dan Kejuruan*, *16*(2), 236. https://doi.org/10.23887/jptk-undiksha.v16i2.18559