CoMBInES
CONFERENCE ON MANAGEMENT, BUSINESS, INNOVATION, EDUCATION AND SOCIAL SCIENCES

Volume 1 No 1 (2021)

Diterima : February 01, 2021
Disetujui : February 05, 2021
Diterbitkan : February 24, 2021

Conference on Management, Business, Innovation, Education and Social Science
https://journal.uib.ac.id/index.php/combines

Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode *Penetration Testing* (Studi Kasus : TP-Link Archer A6)

Haeruddin[1], Arif Kurniadi[2]
Email korespondensi : [1] haeruddin@uib.edu, [2]1731016.arif@uib.edu

[1]Fakultas Ilmu Komputer, Universitas Internasional Batam, Batam, Indonesia
[2]Fakultas Ilmu Komputer, Universitas Internasional Batam, Batam, Indonesia

Abstrak

Jaringan *wireless* adalah sebuah teknologi yang digunakan untuk menerima maupun mengirim di jaringan lokal tanpa menggunakan kabel atau melalui gelombang radio. Kelemahan jaringan *wireless* adalah orang sekitar bisa melakukan *hacking* menggunakan *tools* yang tersedia di internet untuk mendapatkan *password* atau mengambil data secara *ilegal*.

Penelitian ini menggunakan metode *Penetration Testing* untuk menganalisis sistem keamanan jaringan *WLAN* ditempat umum, *hotspot*, dan kafe. Tujuannya untuk mensimulasikan bentuk serangan jaringan menggunakan *tools* yang tersedia di *kali linux*.

Hasil dari penelitian ini menunjukan bahwa hanya dua dari tiga serangan yang berhasil. Oleh karena itu, harus meningkatkan keamanan pada simulasi yang berhasil dilaksanakan.

Kata Kunci: *Hotspot, Penetration Testing, WLAN*.

Abstract

Wireless *network* is a technology used to receive or send on local network without using cable or radio wave. The *downside of wireless* networks is that people around can do *hacking using tools*available on the internet to obtain *passwords* or retrieve data *illegally.*

This research uses *Penetration Testing method* to analyze WLAN network security system *in* public places, *hotspots* and cafes. The goal is to simulate a form of network attack using *tools* available at times *linux.*

The results showed that only two out of three attacks were successful. Therefore, it must increase security on simulations that are successfully implemented.

Keyword: *Hotspot, Penetration Testing, WLAN*.

Pendahuluan

Perkembangan teknologi jaringan komputer memudahkan orang untuk memenuhi kebutuhannya informasi. Salah satu teknologi yang berkembang pesat adalah teknologi media transmisi nirkabel atau *wireless*(Sabdho & Ulfa, 2018). Media transmisi yang

digunakan *wireless* adalah gelombang radio yang dipancarkan ke semua area yang bisa dijangkau oleh gelombang radio tersebut. Beberapa vendor menyediakan fitur-fitur yang memudahkan pengguna maupun administrator jaringan untuk menggunakannya, sehingga sering dijumpai masih menggunakan konfigurasi *default* dari vendor. Oleh karena itu, para *hacker* sering melakukan aksinya untuk menguji kemampuan yang telah dipelajari sebelumnya. Kemudian terhubung dalam satu jaringan yang sama dan mengambil data pengguna lainnya secara illegal(Wahyudi, 2018).

Namun para *hacker* melancarkan aksinya ditempat umum seperti kafe, *public hotspot*, dan restoran. Karena sebagian pengguna tidak peduli dengan keamanan komunikasi data di tempat publik, maka tempat hacker untuk melakukan uji coba illegal melalui jaringan *wireless* yang terhubung ke *hacker*(Samsumar & Gunawan, 2017). Dibanding dengan jaringan kabel atau *LAN*, jaringan *wireless* lebih rentan dan mudah masuk kedalam jaringan *wireless* yang tersedia. Cukup mendapatkan *password wifi* sudah bisa terhubung ke jaringan yang dituju oleh *hacker*(Amarudin, 2018).

Dikarenakan lebih rentan diserang oleh *hacker*, maka dibutuhkan sebuah metode untuk melakukan ujicoba apakah jaringan *wireless* yang telah terpasang sudah aman atau sesuai dengan standard operasional. Metode ini biasa disebut dengan metode *penetration testing*. Metode *Penetration Testing* adalah proses simulasi serangan pada sistem yang memerlukan sertifikasi keamanan jaringan untuk mencegah peretas atau penyerang jaringan yang menyebabkan kehilangan data pribadi dan data perusahaan. Orang yang melakukan metode ini juga disebut sebagai *pentester*(Mushlih et al., 2019). Dalam pengujian ini, perlu disetujui oleh pemilik sistem, jika tidak maka disebut sebagai tindakan illegal atau di-*hack*. Hasil test *pentest* sangat penting bagi administrator jaringan untuk meningkatkan keamanan sistem perusahaan.

Menurut urian diatas, untuk mengevaluasi sistem keamanan jaringan *wireless* dapat dilakukan dengan cara melakukan simulasi bentuk serangan jaringan atau dengan kata lain *penetration testing*. Oleh karena itu, lihat hasil penggunaan metode ini untuk menguji sistem keamanan jaringan *wireless*.

Tinjauan Pustaka

Penelitian telah berkembang dari beberapa aspek referensi yang berkaitan dengan subjek pertanyaan telah diperoleh. Penelitian tersebut meliputi:

Menurut (Bayu et al., 2017) penelitannya yang berjudul "Analisis Keamanan Jaringan *WLAN* Dengan Metode *Penetration Testing*" menggunakan metode *penetration testing* sebagai bentuk simulasi serangan yang akan terjadi atau mencari celah keamanan di jaringan *wireless*. Singkatnya, tujuan pengujian penetrasi hanya untuk melindungi organisasi. Dengan menggunakan hasil uji penetrasi yang efektif, organisasi yang berpartisipasi dapat mengidentifikasi dan mengurangi kerentanan. Tahapan pertama dari metode ini adalah *planning*, pada tahapan ini, selain mendapatkan persetujuan dari manajemen atas proses pengujian, penyelesaian ruang lingkup pengujian dan catatan yang terdokumentasi, aturan dalam pengujian juga diidentifikasi, dan akhirnya target pengujian ditentukan. Tahap *planning* menetukan berhasil tidaknya uji penetrasi yang akan dilakukan dan belum ada uji teknis. Tahapan penetration testing yang dibahas dalam penelitian ini adalah *planning, discovery, attack and reporting*.

Menurut (Sari et al., 2017) penelitannya yang berjudul "Analisis Sistem Keamanan Jaringan *Wireless (WEP,WPAPSK/WPA2PSK) MAC Address,* Menggunakan Metode *Penetration Testing*" menjelaskan bahwa sebuah jaringan bisa dikatakan aman harus memenuhi enam persyaratan, yaitu kerahasiaan yang hanya bisa diakses oleh pihak yang berwenang dan cegah pihak yang tidak berwenang membaca informasi rahasia dan harus

aman. Lalu integritas yang pastikan data yang diterima tetap tidak berubah selama transmisi, baik itu dimodifikasi, didpulikasi atau dikembalikan. Layanan keamanan disediakan memerlukan otentikasi, untuk memastikan identitas pengguna yang berkomunikasi di jaringan yang benar. Kemudian memerhatikan kejadian yang tidak terjadi penyangkalan, ketersedian dan akses kendali.

Menurut (Ismail & Pramudita, 2020) penelitiannya yang berjudul "Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT. Puma Makmur Aneka Engineering Bekas" menjelaskan bahwa mengidentifikasi kerentanan keamanan dalam keadaan terkendali, sehingga dapat menghapusnya. Pakar sistem komputasi menggunakan pengujian *pentesting* untuk memecahkan masalah yang melekat dalam penilaian kerentanan, dengan fokus sensitivitas terhadap tingkat keparahan tinggi. Pengujian penetrasi adalah alat penilaian nilai yang bermanfaat bagi bisnis dan operasinya.

Menurut (Wibowo et al., 2017) penelitannya yang berjudul "Keamanan Jarıngan WLAN Terhadap Serangan Wıreless Hackıng Pada Dınas Komunıkası & Informatıka DIY" pengujian ini didasarkan pada konsep nirkabel serangan peretasan, termasuk *spoofing ARP* dan *cracking WPA2-PSK.* Hasil dari pengujian di Biro Komunikasi dan Informasi DIY pada jaringan *WLAN* menunjukkan bahwa sistem keamana jaringan yang digunakan aman, namun terdapat celah keamanan masih ada dibeberapa jaringan *Wi-Fi* yang harus di tingkatkan dan mengaktifkan fungsi *ARP*.

Menurut (Rusdi & Prasti, 2019) penelitiannya yang berjudul "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux" menjelaskan bahwa dikarenakan kemudahan untuk instalasi jaringan nirkabel, sangat rentan terhadap gangguan keamanan eksternal. Enkripsi ganda ini telah diterapkan untuk melindungi kemanan jaringan *wireless* ini. Namun, enksripsi ini mudah dipecahkan oleh *hacker*. Oleh karena itu perlu ditingkatkan keamanan jaringan di perusahaan tersebut.

Berdasarkan penelitian yang telah dilakukan oleh peneliti sebelumnya maka penulis berencana melaksanakan penelitian mengenai "Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing" seperti yang telah dilakukan oleh (Bayu et al., 2017). Selanjutnya penulis harus memenuhi enam persyaratan sebagai syarat dalam keamanan jaringan seperti pada (Sari et al., 2017). Pengujian keamanan jaringan ini dilakukan untuk menghindari jenis-jenis serangan yang ada pada (Ismail & Pramudita, 2020). Pengujian ini dilakukan pada WPA2-PSK untuk mengetahui celah-celah keamanan yang masih ada pada jaringan *wireless* seperti di penelitian (Wibowo et al., 2017). Lalu penulis melakukan pengujian, menggunakan *tool-tool* yang tersedia di sistem operasi kali linux pada TP-Link Archer A6 seperti di penelitian (Rusdi & Prasti, 2019).

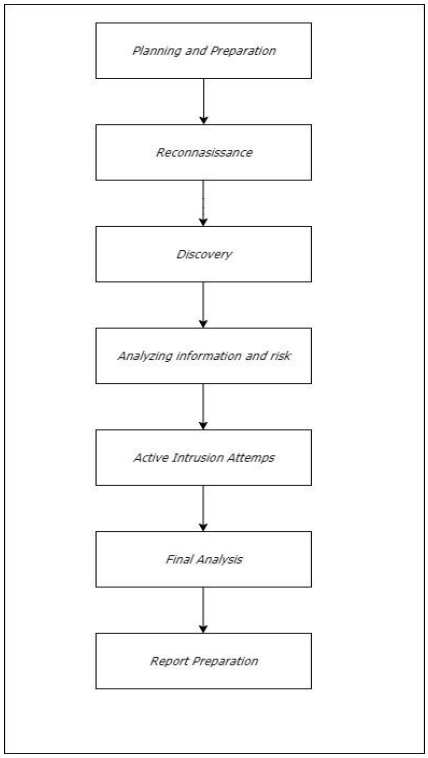
Metodologi Penelitian

Penetration Testing adalah serangan jaringan yang disimulasikan pada sistem komputer untuk mengungkap kerentanan, ancaman, dan resiko dalam aplikasi perangkat lunak, jaringan atau aplikasi web yang dapat digunakan penyerang. Dalam konteks keamanan jaringan *wireless*, *pentesting* sering digunakan untuk menambahkan *firewall* pada *router.* Kerentanan atau *vulnerability* adalah sebuah resiko resmi bahwa penyerang dapat mengganggu atau mendapatkan sistem atau data apa pun yang terkandung di dalamnya. Dalam tahap pengembangan dan implementasi sistem, kerentanan sering kali dimasukkan secara tidak sengaja. Kerentanan umum termasuk kesalahan desain atau konfigurasi, kesalahan perangkat lunak, dll.

Tujuannya untuk menemukan kemungkinan celah resiko keamanan yang ada di sistem. Kesalahan yang terjadi biasanyaa terdapat pada kesalahan konfigurasi, kesalahan perangkat lunak, dll. Pengujian penetrasi biasanyaa mengevaluasi kemampuan

perlindungan sistem jaringan dan pengguna dari ancaman eksternal dan internal. *Penetration Testing* dilakukan dalam kondisi Ketika sistem keamanan menemukan ancaman baru dari *hacker*, memperbarui sistem dan mempersiapkan program startegi kebijakan baru atau *end-user*.

Secara umum, Langkah-langkah yang diambil dalam *penetration testing* adalah sebagai berikut:



Gambar 1. Metode *Penetration Testing*

1. Planning and Preparation

Tentukan ruang lingkup dan tujuan dari pengujian, termasuk sistem yang akan diproses dan metode pengujian yang akan digunakan. Kumpulkan data(misalnya nama jaringan dan *domain server*, *server email*) untuk lebih memahami cara kerja target dan pontensi kerentanan. Langkah pertama adalah selama proses pengujian dalam rencana awal dan pekerjaan persiapan berfokusk pada menentukan kerentanan dan melakukan perbaikan keamanan secara bertahap.

2. Reconnasissance

Reconnasissance atau biasa disebut sebagai pengumpulan data dapat diklarifikasikan sebagai data pasif *penetration testing* karena pengumpulan data secara manual, melalui dokumen terkait atau informasi publik atau menanyakan langsung kepada pihak-pihak yang terlibat dalam sistem.

3. *Discovery*

Discovery adalah Langkah mengumpulkan informasi menggunakan alat otomatis untuk memindai sistem untuk menemukan kerentanan, termasuk memindai jaringan, server, perangkat dan data. Langkah selanjutnya adalah memahami bagaimana target akan merespon berbagai upaya intrusi.

4. *Analyzing information and risk*

Merupakan tahapan analisis informasi secara detail resiko yang diperoleh sebelumnnya(fase *Reconnasissance* dan *Discovery*) dan celah keamanan yang mungkin disebabkan oleh kerentanan di sistem yang diinstal.

5. *Active intrusion attempts*
Ini adalah tahap di mana beberapa intruksi diberikan secara aktif dari posisi segi keamanan sistem, sehingga kerentanan yang ditemukan dapat diperbaiki atau ditingkatkan.

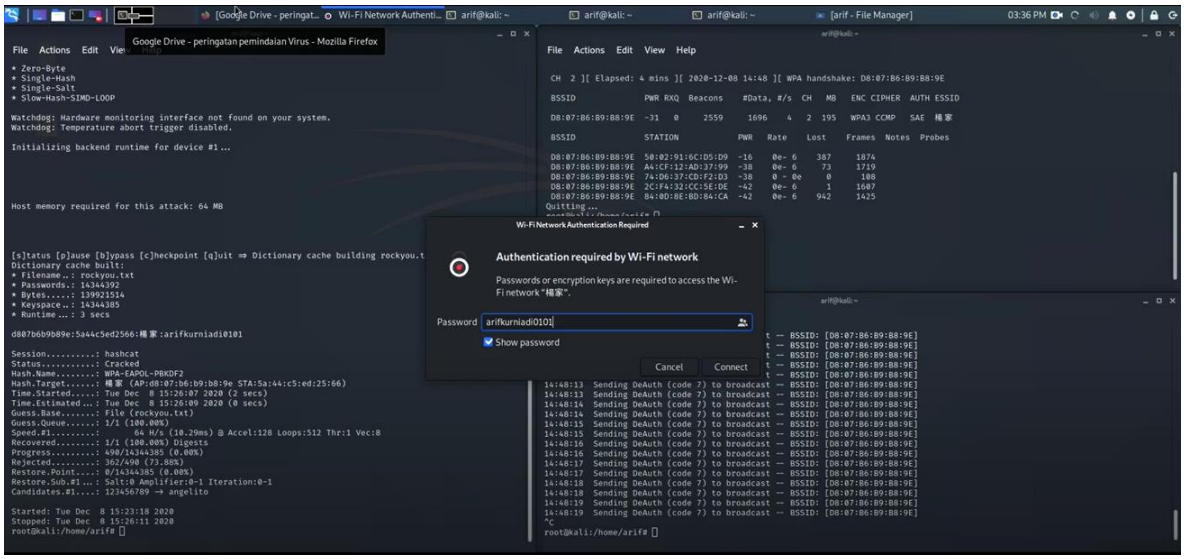
6. *Final analysis*
Analisis akhir secara keseluruhan menggambarkan semuaa temuan dan setelah adanya rencana analisis yang sistematis, petunjuk teknis untuk meningkatkan keselamatan.

7. *Report preparation*
Tahap terakhir dari kegiatan *pentesting* ini adalah memberikan laporan hasil investigasi yang diberikan kepada semuaa pihak yang terkait dan bertanggung jawab atas sistem yang digunakan sebagai acuan untuk meningkatkan keamanan sistem.

Hasil dan Pembahasan

Pengujian kali ini ditujukan pada sebuah *router*, yaitu TP-Link Archer A6. Pada tahap ini, penulis menggunakan dua buah sistem operasi yang salah satunya terinstal dalam *virtual machine*, yaitu sistem operasi *kali linux* dan satunya lagi menggunakan sistem operasi *windows*. Pengujian dilakukan dengan 3 tahapan berbeda, yaitu:

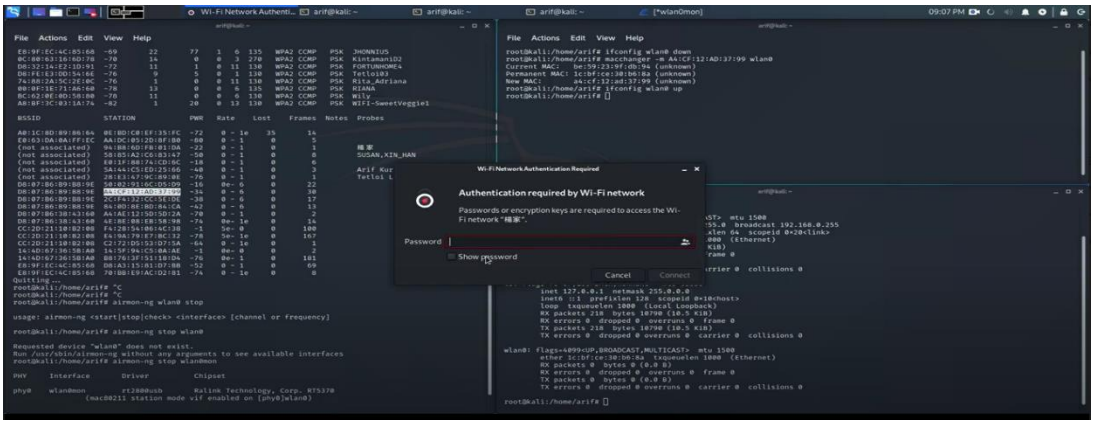
1. *Cracking The Encryption*
Pada tahap pertama, tujuan dari serangan ini adalah untuk mengetahui apa semuaa jalur akses dilindungi oleh sistem keamanan terenkripsi (seperti WEP, WPA, WPA2-PSK). Untuk tujian ini, penulis telah menetapkan tujuan untuk enkripsi WPA2-PSK sebagai target untuk diuji. Penulis memindai titik akses dan kemudian menetukan target yang digunakan untuk memecahkan kunci keamanan. Pertama menggunakan *tools aircrack-ng* untuk melakukan pengambilan *packet data* yang terkirim ke *router access point.* Sesudah mendapatkan file yang diinginkan, Langkah selanjutnya melakukan *decryption* menggunakan *tools hashcat*. *Hashcat* membutuhkan *database* atau kamus yang berisikan *password* yang tersedia dan memungkinkan untuk bisa mendapat *password*. Jika berhasil, maka akan muncul tampilan seperti yang ditunjunkkan pada gambar 1 berikut.



Gambar 1. *Cracking The Encryption*

2. Bypassing MAC Address Authentication

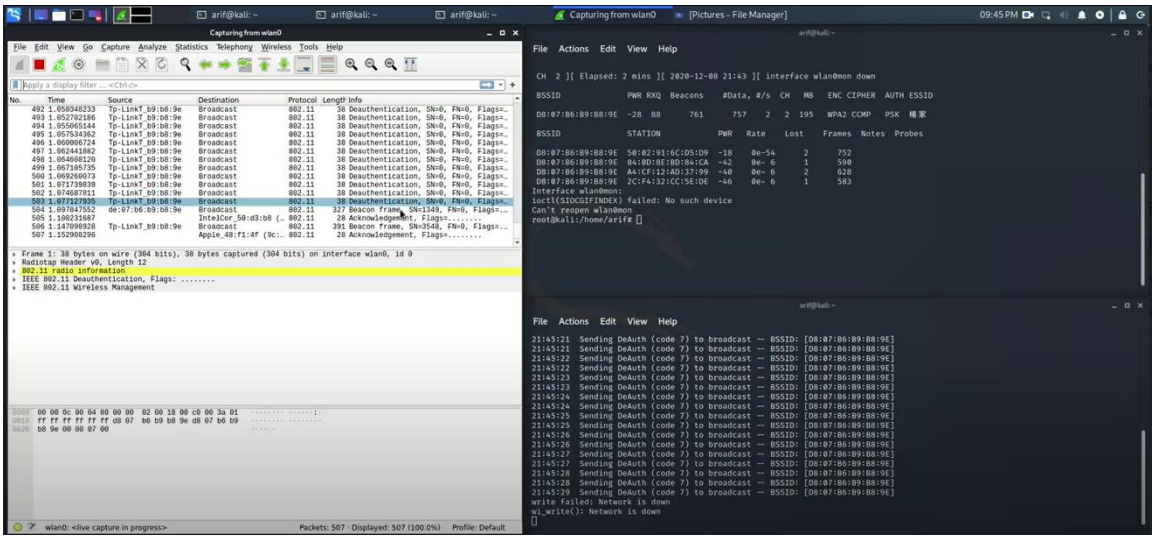
Pada tahap kedua, tujuan dari pengujian ini adalah untuk mengetahui apa sistem itu menggunakan *mac address filtering* atau tidak. Tahap ini, penulis menggunakan *tools aircrack-ng* dan *macchanger*. Pertama penulis akan melakukan *monitoring* menggunakan *aircrack* untuk mengambil *MAC Address* target dan menyalinnya. Lalu, penulis menggunakan tools macchanger untuk mengganti *default MAC Address* yang terdapat pada *usb wifi dongle* dan diganti ke *MAC Address* yang telah didapatkan sebelumnya. Namun ditemukan bahwa sistem keamanan jaringan *wireless* tersebut menggunakan *MAC filtering*.



Gambar 2. *Bypassing MAC Address Authentication*

3. Attacking The Infrastructure

Pada tahap ketiga, jaringan *wireless* akan melakukan penyerangan sehingga bisa mendapatkan hasil apakah bisa mempengaruhi kinerja jaringan. Nama lain dari bentuk serangan ini adalah *DoS attack* yang dirancang untuk melemahkan koneksi pengguna lain di jaringan tersebut. informasi awal yang diperlukan adalah kata sandi jaringan *wireless* yang akan diuji agar komputer tester dapat terhubung ke jaringan tersebut. Penulis menggunakan dua *tools*, yaitu *airmon* untuk mendapatkan *MAC Address* target. Setelah mendapatkan MAC Addressnya, penulis menggunakan *tools aireplay* untuk mengeksekusinya. Hasil dari pengujian ini, berhasil melemahkan jaringan *wireless* tersebut seperti pada gambar 3.



Gambar 3. *Attacking the Infrastructure*

Untuk mengetahui tingkat kerentanan pada hasil pengujian kali ini pada jaringan *WLAN*, melalui tiga tahapan serangan, dapat dibuktikan bahwa kerentanan *WLAN* pada TP-Link Archer A6 bisa dikatakan sangat lemah. Secara umum, penggunaan metode pengujian *Pentesting* untuk mengimplementasikan pengujian keamanan jaringan *WLAN* ditunjukkan pada tabel 1.

Tabel 1. Hasil Pengujian

Jenis Serangan	Informasi yang dibutuhkan	Status
Cracking The Encryption	*Database Password, handshake dengan pengguna lain,* channel dan *MAC Address* yang digunakan *access point*	Berhasil
Bypassing MAC address Authentication	List *user* dalam jaringan yang sama dan menganmbil salah satu *MAC Address* untuk *handshake*	Gagal
Attacking The Infrastructure	Penguji harus tetap berada di jaringan yang sama dengan *user* lainnya	Berhasil

Kesimpulan

Berdasarkan penelitian yang dilakukan selama analisis keamanan jaringan *WPA2-PSK* Menggunakan Metode *Penetration Testing*(Studi Kasus: TP-Link Archer A6) menggunakan kali linux dapat menarik kesimpulan adalah keamanan jaringan dengan menggunakan metode pengujian *Penetration Testing* pada TP-Link Archer A6 masih banyak kelemahan sistem, dikarenakan masih menggunakan konfigurasi *default* dari *vendor.* Oleh karena itu diperlukan peningkatan keamanan pada TP-Link Archer A6 dengan mengkonfigurasi lebih aman dan tidak menggunakan konfigurasi *default router*. Hasil

penelitian menunjukan bahwa dari tiga serangan yang dilakukan, hanya satu serangan yang memiliki status gagal, yaitu tipe serangan *Bypassing MAC address Authentication.*

Daftar Pustaka

Amarudin. (2018). *Mikrotik Router Os Menggunakan Metode Port*.

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.

Ismail, R. W., & Pramudita, R. (2020). Metode Penetration Testing pada Keamanan Jaringan Wireless Wardriving PT . Puma Makmur Aneka Engineering Bekasi. *Jurnal Mahasiswa Bina Insani*, *5*(1), 53–62.

Mushlih, M., Fitri, R., & Wardiah, I. (2019). Penetration Testing Tool Untuk Menguji Kerentanan Sql Injection Secara Otomatis Berbasis Web. *Seminar Nasional Riset …*, *5662*(November), 41–47. http://e-prosiding.poliban.ac.id/index.php/snrt/article/view/409

Rusdi, M. I., & Prasti, D. (2019). *Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux*. 260–269.

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

Samsumar, L. D., & Gunawan, K. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi. *Ilmiah Teknologi Informasi Terapan*, *IV*(1), 73–82.

Sari, D. M., Yamin, M., & Aksara, L. B. (2017). Analisis Sistem Keamanan Jaringan Wireless (WEP, WPAPSK/WPA2PSK) Mac Address, Menggunakan Metode Penetration testing. *SemanTIK*, *3*(2), 203–208. https://doi.org/10.1016/j.neuropharm.2007.08.010

Wahyudi, E. (2018). Analisis Keamanan WPA2-PSK Dan Radius Server Pada Jaringan Nirkabel Menggunakan Metode Wireless Penetration Testing. *Journal Ilmiah Rinjani_Universitas Gunung Rinjani*, *6*(1), 199–206.

Wibowo, M. G. H., Triyono, J., & Sutanta, E. (2017). Keamanan Jaringan Wlan Terhadap Serangan Wireless Hacking Pada Dinas Komunikasi & Informatika Diy. *Seminar Nasional & Call for Paper : Pengembangan Smart City Menuju Pembangunan Kota Yang Cerdas Dan Berkelanjutan*, *1*(1), 2–9.