Analisis Celah Keamanan Jaringan WPA dan WPA2 Dengan Menggunakan Metode Penetration Testing

Albert Okario[1], I Putu Gede Hendra Suputra[2]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jalan Raya Kampus Udayana, Bukit Jimbaran, Kuta Selatan, Badung, Bali Indonesia
[1]okarioalbert@gmail.com
[2]hendra.suputra@gmail.com

Abstract

With the rapid development of communication and information technology, wireless local area network (WLAN) security has become crucial and a major concern, as data traffic is transmitted without the need for cables. Internet-connected network devices are inherently insecure and can be exploited by crackers or hackers. When data communicates or connects in the data traffic, where data is sent and passes through a series of terminals to reach its destination, an irresponsible user has the opportunity to modify or intercept the data. Therefore, designing a WLAN network connected to the internet must be carefully planned to minimize undesirable incidents. The weakness of the IEEE 802.11 network that uses WEP encryption tends to make the encryption code more easily discoverable by hackers. Based on the aforementioned background, we conducted this research to identify vulnerabilities or security flaws in WPA and WPA2-PSK networks using penetration testing methods.

Keywords: *WPA2-PSK Network Security Analysis, Penetration Testing*

1. Pendahuluan

Dalam era digital yang terus berkembang pesat, keamanan jaringan menjadi isu yang semakin penting. Kehadiran jaringan Wi-Fi telah mempermudah akses internet tanpa perlu menggunakan kabel, namun juga menimbulkan risiko keamanan yang perlu diperhatikan. Protokol keamanan Wi-Fi seperti WPA dan WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) dikembangkan untuk melindungi jaringan dari ancaman yang mungkin timbul. Namun, tidak ada sistem keamanan yang sepenuhnya tak terkalahkan. Celah keamanan dapat ada dan sering kali ditemukan oleh peneliti keamanan atau peretas. Oleh karena itu, penting untuk melakukan analisis yang komprehensif terhadap celah keamanan yang ada dalam protokol jaringan Wi-Fi. Dalam penelitian ini, kami akan melakukan analisis celah keamanan pada protokol

WPA dan WPA2-PSK dengan menggunakan metode penetration testing. Penetration testing adalah proses evaluasi keamanan yang bertujuan untuk mengidentifikasi kerentanan dalam sistem dengan mensimulasikan serangan yang dilakukan oleh pihak yang tidak berwenang. Melalui metode penetration testing, kami akan mencoba mengeksplorasi celah keamanan yang mungkin ada dalam protokol WPA dan WPA2-PSK. Tujuan utama dari penelitian ini adalah untuk mengetahui sejauh mana keamanan protokol tersebut dan menyediakan rekomendasi perbaikan untuk mengatasi celah yang ditemukan.

Data yang diperoleh dari penelitian ini akan dianalisis secara menyeluruh untuk mengidentifikasi celah keamanan yang ada dan memberikan rekomendasi yang tepat untuk meningkatkan keamanan jaringan Wi-Fi. Diharapkan bahwa hasil penelitian ini akan memberikan pemahaman yang lebih baik tentang celah keamanan dalam protokol WPA dan WPA2-PSK serta memberikan kontribusi untuk meningkatkan keamanan jaringan Wi-Fi secara umum.

2. Metode Penelitian

2.1 Metode Pengumpulan Data

Metode penelitian adalah kerangka kerja yang digunakan untuk mengarahkan langkah-langkah dalam menyusun hipotesis dan gagasan yang sesuai dengan tujuan penelitian. Metode yang tepat akan mempengaruhi proses penelitian dan hasil yang diperoleh. Pada prosedur penelitian yang dilakukan untuk mendapatkan hasil yang relevan yang sesuai dengan tujuan dari penelitian, terdapat empat langkah utama yang dijalankan:

a. Analisa: Langkah pertama dalam penelitian ini adalah melakukan analisis terhadap rancangan jaringan yang ada pada lokasi penelitian. Analisis ini bertujuan untuk memahami struktur jaringan yang sedang diteliti serta mengidentifikasi potensi celah keamanan yang mungkin ada
b. Perancangan: Langkah selanjutnya adalah merancang spesifikasi kebutuhan perangkat lunak sistem operasi Kali Linux yang akan digunakan dalam metode analisa. Dalam tahap ini, akan dilakukan perencanaan terkait konfigurasi dan persyaratan perangkat lunak yang diperlukan untuk melakukan analisis keamanan.
c. Pengujian: Tahap ini melibatkan pengujian menggunakan metode penetration testing untuk mendapatkan hasil dan menemukan celah keamanan yang ada. Dalam tahap pengujian ini, akan dilakukan serangkaian uji penetrasi untuk menguji efektivitas keamanan jaringan dan mengungkap potensi kerentanan yang mungkin ada.
d. Dokumentasi: Metode terakhir adalah dokumentasi, di mana langkah ini melibatkan studi pustaka, mempelajari jurnal-jurnal yang relevan, serta sumber-sumber lain yang berkaitan dengan topik penelitian. Proses dokumentasi ini penting untuk menggambarkan dan mengkomunikasikan temuan penelitian, langkah-langkah yang dilakukan, analisis data yang telah dilakukan, serta kesimpulan yang diperoleh dari penelitian tersebut.

Dengan melakukan langkah-langkah tersebut, diharapkan dapat menghasilkan data yang relevan dan sesuai dengan tujuan penelitian. Pengumpulan data yang sistematis dan terarah ini akan membantu dalam mencapai hasil penelitian yang sesuai dengan maksud dan tujuan yang telah ditetapkan sebelumnya.

2.2. Metode Penetration Testing

Penetration testing, juga dikenal sebagai pentesting, adalah proses yang disimulasikan untuk menemukan kerentanan, ancaman, dan risiko dalam sistem komputer, jaringan, atau aplikasi perangkat lunak. Dalam keamanan jaringan nirkabel, pentesting sering digunakan untuk menambahkan lapisan keamanan, seperti firewall, pada router. Kerentanan atau vulnerability adalah kelemahan atau celah yang dapat dieksploitasi oleh penyerang untuk mengganggu atau mendapatkan akses ke sistem dan data yang ada di dalamnya. Kerentanan umumnya disebabkan oleh kesalahan desain, konfigurasi, atau perangkat lunak. Tujuan utama dari penetration testing adalah untuk menemukan dan mengidentifikasi potensi kerentanan dan risiko keamanan yang ada dalam sistem. Hal ini memungkinkan pemilik sistem untuk mengambil tindakan yang tepat untuk memperbaiki celah keamanan tersebut sebelum penyerang yang jahat memanfaatkannya. Kerentanan yang sering ditemui meliputi kesalahan konfigurasi, kesalahan perangkat lunak, dan kerentanan lainnya. Dibawah ini merupakan langkah-langkah yang kami lakukan dalam melakukan penetration testing:

a. Perencanaan dan Persiapan

Dalam langkah perencanaan dan persiapan, dilakukan penentuan tujuan dan lingkup pentesting serta memperoleh izin tertulis dari pemilik sistem atau jaringan yang akan diuji, sekaligus mengumpulkan informasi yang diperlukan tentang sistem yang akan diuji, seperti alamat IP, jenis sistem operasi, aplikasi yang digunakan, dan kebijakan keamanan yang ada.

b. Pengumpulan Informasi

Pada langkah pengumpulan informasi, dilakukan pemetaan jaringan untuk mengidentifikasi host yang aktif, menentukan port yang terbuka, serta melakukan pengumpulan informasi lebih lanjut tentang sistem atau jaringan yang akan diuji, termasuk versi perangkat lunak yang digunakan, pengguna yang terdaftar, dan konfigurasi sistem yang relevan.

c. Analisis Kerentanan

Dalam tahap analisis kerentanan, dilakukan analisis kerentanan otomatis dengan menggunakan alat pemindai kerentanan untuk mengidentifikasi kerentanan umum yang terdapat dalam sistem atau jaringan yang diuji, serta dilakukan analisis kerentanan manual yang melibatkan pemeriksaan lebih mendalam secara manual terhadap kode, konfigurasi, dan pengujian yang lebih cermat untuk mencari kerentanan yang mungkin tidak terdeteksi secara otomatis.

d. Eksploitasi dan Mendapatkan Akses

Pada langkah eksploitasi dan mendapatkan akses, dilakukan upaya untuk mengeksploitasi kerentanan yang telah teridentifikasi untuk mendapatkan akses ke sistem atau jaringan yang diuji, dan dalam kasus berhasil mendapatkan akses awal, langkah selanjutnya adalah mencoba mendapatkan akses yang lebih tinggi, seperti akses administrator atau hak istimewa lainnya, dengan tujuan mengevaluasi sejauh mana sistem dapat melindungi data sensitif atau kritis.

e. Pemeliharaan Akses dan Penetrasi Lanjutan

Pada tahap pemeliharaan akses dan penetrasi lanjutan, dilakukan upaya untuk mempertahankan akses yang telah diperoleh agar dapat melakukan evaluasi lebih lanjut terhadap sistem atau jaringan yang diuji, serta dilakukan penetrasi lanjutan untuk mengeksplorasi lebih dalam sistem atau jaringan yang diuji guna mengidentifikasi kerentanan atau celah keamanan yang mungkin terlewatkan sebelumnya.

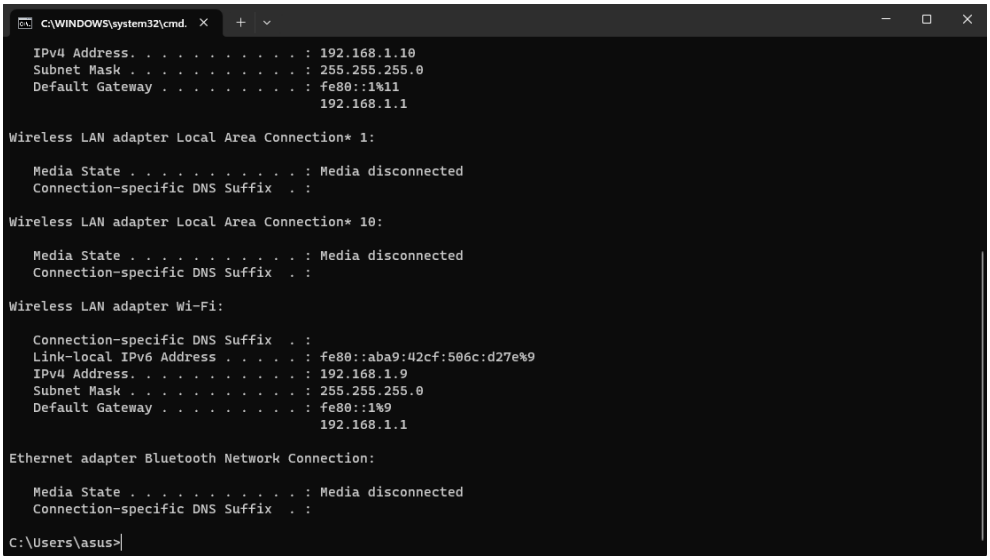
f. Pelaporan dan Rekomendasi

Pada langkah pelaporan dan rekomendasi, dibuat laporan yang berisi temuan secara rinci, termasuk kerentanan yang ditemukan, metode yang digunakan, serta hasil dari pengujian, sekaligus memberikan rekomendasi perbaikan kepada pemilik sistem atau jaringan tentang tindakan yang harus diambil untuk memperbaiki kerentanan dan meningkatkan keamanan.

3. Hasil dan Diskusi

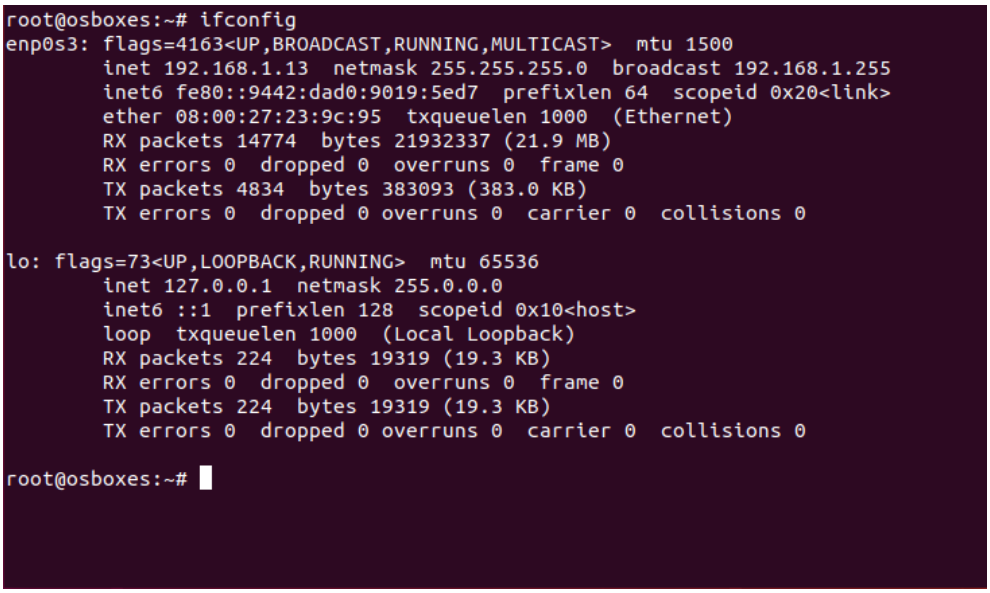
3.1 Tahapan Penelitian

Tahapan awal yang kami lakukan adalah pengumpulan data, yang dilanjutkan dengan penerapan metode penetration testing. Penetration testing dilakukan dengan melakukan pengecekan alamat IP (Internet Protocol) pada setiap perangkat yang terlibat dalam sistem. Selanjutnya, kami melakukan proses scanning dan discovering untuk mengidentifikasi port-port yang terbuka dan layanan-layanan yang berjalan pada port tersebut, menggunakan protokol TCP dan UDP. Dalam proses ini, kami menggunakan alat seperti Nmap untuk mengenali status port, seperti open, open|filtered, closed, closed|filtered, filtered, dan unfiltered. Kami juga melakukan pengecekan IP Windows dan melakukan identifikasi IP router yang terlibat dalam sistem. Cek ip yang digunakan untuk mengatahui ip windows dan juga router:



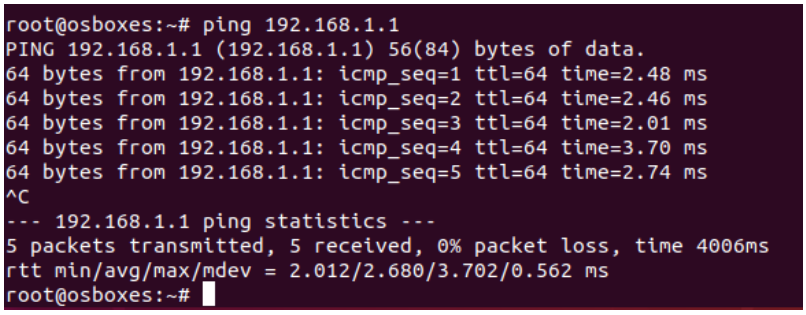
Gambar 1. Ip Windows dan Router

Setelah melakukan pengecekan IP menggunakan perintah ipconfig pada sistem operasi Windows, ditemukan bahwa IP Windows adalah 192.168.1.9 dengan subnet mask 255.255.255.0, dan IP router adalah 192.168.1.1. Selanjutnya, kami akan melakukan pengecekan IP pada sistem operasi Kali Linux:



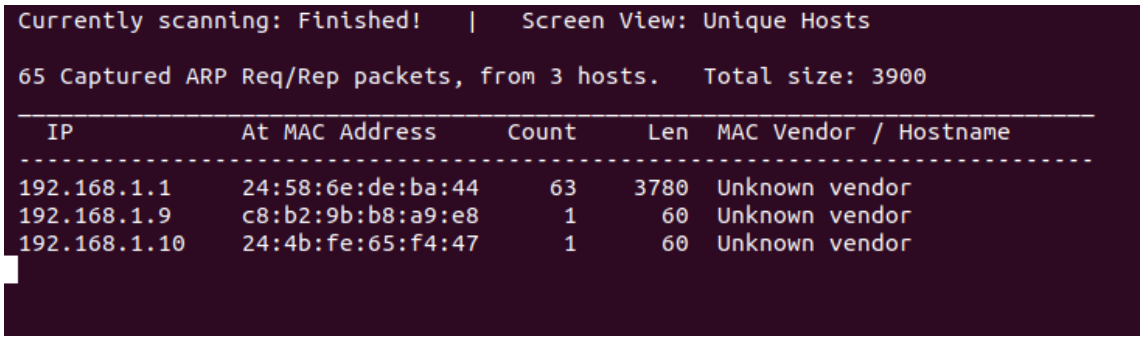
Gambar 2. Ip Linux

Melalui pengecekan tersebut, ditemukan bahwa IP dari Kali Linux adalah 192.168.1.13 dengan netmask 255.255.255.0. Informasi ini mengindikasikan bahwa jaringan yang digunakan adalah jaringan kelas C. Untuk menguji koneksi, kami dapat menggunakan perintah ping sebagai bukti bahwa komputer Kali Linux dapat terhubung ke jaringan dengan mengirimkan paket ke alamat IP yang dituju dan menerima respons balik.

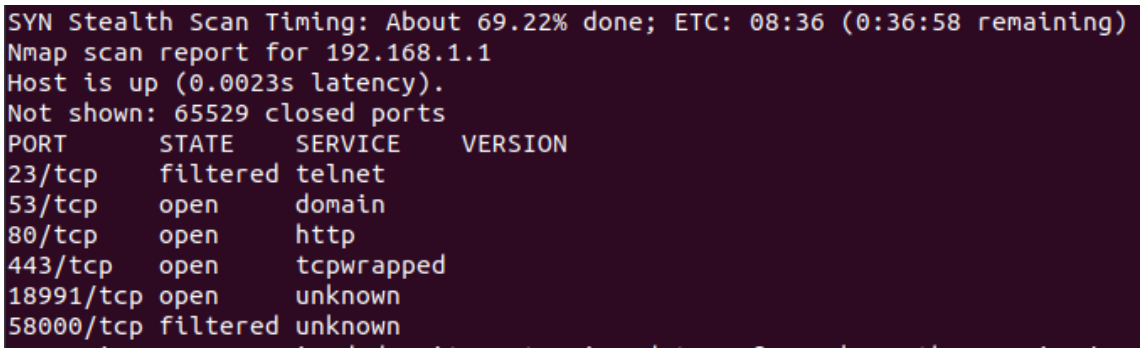


Gambar 3. Ping Gateway/Ip Router

Setelah mengetahui IP dari perangkat-perangkat dan jaringan yang terhubung, langkah selanjutnya adalah melakukan proses scanning dan discovering jaringan. Untuk melakukan scanning jaringan, kami menggunakan perintah "sudo netdiscover -r 192.168.1.0/24" yang akan melakukan scanning pada rentang IP 192.168.1.0 hingga 192.168.1.255 untuk menemukan perangkat-perangkat yang terhubung dalam jaringan tersebut. Selain itu, kami juga menggunakan perintah "nmap -p- -sV -O 192.168.1.1" yang akan melakukan scanning pada IP router 192.168.1.1 dengan melihat semua port yang terbuka (option -p-) dan mengidentifikasi layanan-layanan yang berjalan pada port tersebut (option -sV) serta melakukan pendeteksian sistem operasi (option -O).



Gambar 4. Proses Discovery



Gambar 5. Proses Scanning

Setelah itu gunakan tool meterpreter, Meterpreter adalah sebuah alat yang umumnya digunakan oleh peneliti keamanan dan pengujian penetrasi untuk mendapatkan akses ke sistem yang rentan, ia merupakan sebuah payload yang digunakan dalam kerangka kerja Metasploit. Meterpreter memungkinkan pengguna untuk mengendalikan sistem yang diserang secara jarak jauh dan melakukan berbagai tindakan, termasuk mengambil alih akses administrator. Dalam pengujian yang telah dilakukan, sistem operasi Metasploitable memang diketahui memiliki kerentanan yang dapat dieksploitasi. Metasploitable sebenarnya adalah distribusi sistem operasi

khusus yang dirancang untuk tujuan pengujian keamanan dan rentan terhadap serangan yang diketahui. Dengan menggunakan Metasploit dan payload seperti Meterpreter, pengguna dapat mengidentifikasi, mengeksploitasi, dan menguji kerentanan sistem tersebut. Penting untuk dicatat bahwa penggunaan Meterpreter atau alat serupa untuk tujuan ilegal, seperti mencuri data atau merusak sistem tanpa izin pemiliknya, adalah kegiatan yang melanggar hukum dan tidak etis. Penggunaan alat-alat tersebut harus selalu dilakukan dengan persetujuan dan dalam lingkungan pengujian keamanan yang sah. Dan dari hasil pengujian yang kami lakukan sistem operasi metasploitable dapat dieksploitasi.

4. Kesimpulan

Berdasarkan hasil pengujian terhadap sistem operasi pada jaringan yang menggunakan keamanan WPA dan WPA2, maka dapat disimpulkan seperti berikut ini:

a. Jalur lalu lintas data pada jaringan, jika dilakukannya proses scanning dan discovering selalu ada kemungkinan didapatkannya vulnerability atau suatu celah melalui port yang terbuka, namun proses scanning dan discovering sendiri bisa berjalan cukup lama tergantung dari jenis proteksi jaringan yang digunakan.]
b. port http yang terbuka menjadi salah satu bahaya yang dimana dapat dieksploitasi oleh meterpreter melalui msfconsole pada kali linux
c. orang-orang yang tidak bertanggung jawab sendiri dapat menggunakan tool seperti aircrack-ng dalam meretas password suatu jaringan yang semakin mempermudah dalam melakukan eksploitasi

Daftar Pustaka

[1]. Adiguna, M. A., & Widagdo, B. W “Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r),” Jurnal Sistem Komputer dan Kecerdasan Buatan., vol. 5, No. 2, pp. 1-8, 2022.
[2]. Arif, K, “THESIS WPA2-PSK NETWORK SECURITY ANALYSIS USING THE PENETRATION TESTING METHOD (CASE STUDY: TP-LINK ARCHER A6),” 2021
[3]. Daulay, M. I, “ANALISIS PERBANDINGAN KEAMANAN WEP, WPA, WPA2, PADA ACCESS POINT,” 2019.
[4]. Fauzan, M. F., & dan Irawan, A. S. Y, “Wireless Attack : Menggunakan Tools Aircrack Pada Kali Linux Untuk Melakukan WPA Attack,” Jurnal Lentera., vol. 20, No. 1, pp. 63-74, 2021.
[5]. Haeruddin, & Kurniadi, A, “Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : TP-Link Archer A6),” Conference on Management, Business, Innovation, Education and Social Science., vol. 1, no. 1, pp. 508-515, 2021.
[6]. Setyawan, F., & Amnur, H, “Keamanan Jaringan Wireless Dengan Kali Linux,” Jurnal Ilmiah Teknologi Sistem Informasi., vol. 3, no. 1, pp. 16-22, 2022.