

BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan jaringan Wi-Fi semakin meluas di berbagai aspek kehidupan, seperti salah satu contohnya yaitu, di rumah. Hampir semua masyarakat saat ini sudah memasang jaringan Wi-Fi di rumahnya untuk menunjang aktivitas sehari-hari seperti bekerja, belajar, mengakses informasi, hingga hiburan digital. Konektivitas yang cepat dan tanpa kabel membuat Wi-Fi menjadi solusi utama bagi kebutuhan jaringan modern.

Wi-Fi memiliki beberapa jenis tipe keamanan, seperti WEP (*Wired Equivalent Privacy*), WPA (*WiFi Protected Access*), WPA2 (*WiFi Protected Access 2*), dan WPA3 (*WiFi Protected Access 3*). Salah satu tipe keamanan yang saat ini paling umum digunakan untuk jaringan Wi-Fi adalah *WiFi Protected Access 2-Pre Shared Key (WPA2-PSK)*. Protokol ini merupakan tipe keamanan jaringan *wireless* yang sudah menggunakan dua jenis enkripsi, yaitu *Advanced Encryption Standard (AES)* dan *Temporal Key Integrity Protocol (TKIP)* [1]. Meskipun WPA2-PSK sudah menawarkan keamanan yang baik, jaringan Wi-Fi yang menggunakan tipe keamanan ini masih dapat menjadi target serangan siber, terutama jika pengguna menggunakan *password* yang lemah, mudah ditebak atau sering dibagikan ke banyak orang. Hal ini berisiko membuka jalan bagi pelaku serangan untuk menyusup ke jaringan tanpa izin.

Beberapa serangan umum seperti *deauthentication attack*, *handshake capture*, hingga *dictionary attack* dapat dilakukan dengan mudah oleh penyerang

hanya dengan menggunakan perangkat lunak tertentu tanpa perlu akses fisik ke jaringan. Hal ini menunjukkan bahwa jaringan Wi-Fi pribadi masih berisiko menjadi target serangan yang dapat membahayakan kerahasiaan dan integritas data pengguna.

Melihat kondisi tersebut, diperlukan sebuah pengujian keamanan yang mampu mengidentifikasi kelemahan autentikasi dalam jaringan Wi-Fi. Salah satu metode yang umum digunakan adalah *penetration testing*, yakni simulasi serangan siber yang bertujuan untuk menemukan dan mengevaluasi celah keamanan sistem. Dalam penelitian ini, digunakan Kali Linux sebagai sistem operasi pengujian karena memiliki banyak alat uji seperti *airodump-ng*, *aireplay-ng*, dan *aircrack-ng* yang sesuai untuk skenario penyerangan terhadap jaringan Wi-Fi.

Selain itu, tingkat risiko dari celah keamanan yang ditemukan perlu diukur secara objektif. Oleh karena itu, penelitian ini juga menggunakan metode *Common Vulnerability Scoring System* (CVSS) v3.1 untuk memberikan skor tingkat keparahan celah yang ditemukan. Dengan pendekatan ini, hasil penelitian dapat memberikan pemahaman yang lebih akurat mengenai kerentanan jaringan Wi-Fi WPA2-PSK, serta dapat menjadi dasar dalam menyusun rekomendasi mitigasi dan peningkatan keamanan jaringan Wi-Fi pribadi.

Beberapa penelitian sebelumnya telah menunjukkan bahwa protokol ini masih memiliki kelemahan. Studi oleh [2] menemukan kerentanan pada port HTTP yang dieksploitasi menggunakan *msfconsole* dan *meterpreter*, sementara studi oleh [3] menunjukkan bahwa dua dari tiga serangan berhasil dilakukan, yaitu *Cracking The Encryption*, *Attacking The Infrastructure* berhasil dilakukan, dan *Bypassing*

MAC address Authentication gagal dilakukan. Namun, penelitian tersebut belum ada yang secara khusus membahas eksploitasi pada tahap awal seperti *Handshake capture* dan *Cracking Dictionary Attack* yang merupakan metode serangan penting dalam konteks keamanan jaringan Wi-Fi. Serta belum juga menggunakan perhitungan sesuai dengan standar resmi, seperti *Common Vulnerability Scoring System* (CVSS) sebagai penilaian kerentanan yang akurat dan dapat dipercaya. Maka dari itu, eksperimen ini bertujuan untuk mengisi celah tersebut, serta memberikan gambaran nyata tentang efektivitas konfigurasi keamanan jaringan yang diuji dan keakuratan nilai kerentanan untuk menjadi dasar dalam menyusun rekomendasi mitigasi dan peningkatan keamanan jaringan Wi-Fi pribadi.

Pentingnya menjaga keamanan jaringan Wi-Fi di lingkungan rumah menjadi sorotan utama dalam penelitian ini. Berdasarkan hasil uji penetrasi menggunakan Kali Linux terhadap *router* Huawei HG8245H5 yang menggunakan WPA2-PSK, ditemukan adanya celah potensi yang memungkinkan serangan *deauthentication* dan *dictionary attack*.

Berdasarkan uraian latar belakang diatas, maka penulis bermaksud untuk melakukan penelitian dengan judul **“IDENTIFIKASI CELAH KEAMANAN JARINGAN WI-FI BERBASIS WPA2-PSK DENGAN METODE PENETRATION TESTING MENGGUNAKAN KALI LINUX”**.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah diuraikan, maka dapat diidentifikasi beberapa masalah untuk pengujian *penetration testing* pada jaringan Wi-Fi yang menggunakan tipe keamanan WPA2-PSK, adalah sebagai berikut:

1. Perlu dilakukan metode *penetration testing* untuk mengidentifikasi celah keamanan dan kerentanan terhadap serangan eksploitasi awal, seperti *Handshake capture* dan *dictionary attack* pada jaringan Wi-Fi yang menggunakan protokol keamanan WPA2-PSK.
2. Penerapan metode *penetration testing* untuk jaringan Wi-Fi dengan protokol keamanan WPA2-PSK menggunakan kali linux perlu dilakukan sesuai standar, seperti standar *NIST (National Institute of Standards and Technology)* SP 800-42 untuk memastikan konsistensi dan kualitas hasil pengujian.
3. Belum ada laporan yang menilai tingkat risiko celah keamanan di jaringan Wi-Fi WPA2-PSK menggunakan metode penilaian standar *Common Vulnerability Scoring System calculator (CVSS)*. Karena itu, tidak ada landasan penilaian yang kuat untuk memberikan rekomendasi perbaikan yang terukur dan relevan.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah diatas, dapat dirumuskan suatu masalah yang relevan adalah:

1. Bagaimana cara mengidentifikasi celah keamanan pada jaringan Wi-Fi WPA2-PSK melalui *penetration testing* awal dengan serangan *Handshake capture* dan *dictionary attack* menggunakan kali linux?
2. Bagaimana penerapan metode *penetration testing* menggunakan kali linux sesuai dengan standar *NIST (National Institute of Standards and Technology)* SP 800-42 untuk memperoleh hasil pengujian yang konsisten dan berkualitas?

3. Bagaimana cara menilai tingkat risiko celah keamanan pada jaringan Wi-Fi yang menggunakan protokol keamanan WPA2-PSK dengan menggunakan metode penilaian standar, seperti *Common Vulnerability Scoring System calculator (CVSS)*, sehingga dapat menghasilkan penilaian yang terukur dan relevan?

1.4 Tujuan Penelitian

1. Mengidentifikasi celah keamanan pada jaringan Wi-Fi dengan tipe keamanan WPA2-PSK terhadap serangan-serangan yang merugikan pengguna jaringan Wi-Fi, seperti *Deauthentication*, *Handshake Capture*, dan *Cracking Dictionary Attack*.
2. Menerapkan metode *penetration testing* menggunakan kali linux sesuai standar, seperti *NIST (National Institute of Standards and Technology)* SP 800-42 guna mendapatkan hasil pengujian yang terstruktur, konsisten, dan berkualitas.
3. Untuk menilai tingkat risiko celah keamanan pada jaringan Wi-Fi dengan protokol keamanan WPA2-PSK menggunakan metode penilaian standar *Common Vulnerability Scoring System calculator (CVSS)*, serta menyusun rekomendasi perbaikan yang terukur dan relevan berdasarkan hasil pengujian.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat membantu meningkatkan keamanan jaringan Wi-Fi yang menggunakan protokol keamanan WPA2-PSK dengan cara mendeteksi dini kerentanan yang ada dengan melakukan *penetration testing*, untuk memperkuat perlindungan jaringan, serta menjaga data penting dari serangan siber.

Dan dapat dijadikan bahan evaluasi dan dasar dalam merancang jaringan Wi-Fi yang aman.

1.6 Batasan Masalah

Berdasarkan rumusan masalah penelitian, terdapat batasan masalah dalam penelitian sebagai berikut:

1. Melakukan uji penetrasi pada jaringan Wi-Fi pribadi berbasis WPA2-PSK pada router Huawei tipe HG8245H5, dan menggunakan TP-Link WN722N v4 sebagai *Monitor Mode & Packet Injection Adapter*.
2. Melakukan uji penetrasi dan eksploitasi menggunakan *tools airodump-ng, aireplay-ng, aircrack-ng* yang ada pada kali linux, yang digunakan untuk melakukan serangan tahap awal seperti, *Deauthentication Attack, Handshake capture*, dan *Cracking Password* dengan metode *Dictionary Attack*.
3. Penelitian ini dibatasi pada penilaian tingkat risiko celah keamanan pada jaringan Wi-Fi dengan protokol WPA2-PSK menggunakan metode standar penilaian *Common Vulnerability Scoring System calculator (CVSS)*, serta tidak mencakup metode penilaian risiko lainnya diluar standar tersebut.

1.7 Sistematika Penulisan

Berikut merupakan sistematika yang terdapat pada penelitian ini yang terdiri dari lima bab, yaitu:

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang, identifikasi masalah, tujuan penelitian, manfaat penelitian, rumusan masalah, batasan masalah.

BAB II TINJAUAN PUSTAKA

Berisi tentang berbagai teori-teori yang berkaitan dengan permasalahan yang akan dibahas.

BAB III METODOLOGI PENELITIAN

Merupakan bab yang menjelaskan tentang lokasi penelitian, metode pengumpulan data, metode analisis data, dan metode teknik lain yang digunakan dalam penelitian

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisikan langkah-langkah proses pengujian yang dilakukan dan hasil yang diperoleh dari proses pengujian yang dilakukan pada target yang sudah ditentukan.

BAB V KESIMPULAN DAN SARAN

Di akhir bab ini berisi mengenai kesimpulan penelitian serta saran yang berhubungan dengan penyusunan tugas akhir.