

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Jaringan *Wireless* merupakan jaringan yang lebih terbuka dibanding menggunakan kabel. Karena siapapun bisa terkoneksi dan cukup rentan jika tidak ada fitur keamanan dan digunakan oleh banyak perangkat seperti Access Point, Router, Bahkan Hotspot Handphone sekalipun menggunakan Keamanan jaringan *WPA2-PSK*. Salah satu Fitur keamanan yang umum diterapkan adalah autentikasi *Wireless* menggunakan *WPA/WPA2 Pre-Shared-Key* yang diseting pada *Wireless Security profile*. Autentikasi ini akan berlaku untuk semua user yang ingin terkoneksi ke *Wireless*. Dengan penggunaan jaringan *Wireless* yang semakin tinggi, hal ini membuat keamanan jaringan juga menjadi sangat dibutuhkan untuk jaringan yang lebih stabil dan melindungi pemilik jaringan dari serangan hacker maupun cracker yang sering meresahkan apalagi untuk seorang administrator jaringan.

Perlu adanya penelitian lebih lanjut untuk menanggulangi para peretas yang berusaha masuk pada jaringan *Wireless*, terdapat berbagai macam metode yang sering digunakan oleh para hacker untuk masuk kedalam jaringan. *IP Spoofing*, *DDoS (Distributed Denial of Service)*, *Packet Sniffing* dan *Brute Force*. Serangan dengan menggunakan Teknik *Brute Force* merupakan salah 1 cara yang digunakan oleh para penyerang. Serangan ini merupakan suatu cara untuk menemukan password dari account user dengan cara yang sistematis mencoba berbagai kombinasi angka, huruf, atau symbol. Sementara serangan dengan menggunakan

metoda kamus password adalah cara menemukan password dengan mencoba berbagai kemungkinan password yang biasa dipakai user secara umum dengan menggunakan daftar atau kamus password yang sudah di-definisikan sebelumnya.

Acrylic Wifi, Merupakan *Tools* Yang Diperuntukan Seorang Administrator untuk membantu mengelola jaringan *wireless* dari memantau hingga melakukan sebuah simulasi penyerangan menggunakan Teknik brute force dan menggunakan *dic.file*. Diharapkan dari hasil hasil Penelitian ini dapat meningkatkan kualitas keamanan jaringan terutama pada system *WPA2-PSK* serta membuat administrator untuk lebih baik lagi dalam menggunakan sistem keamanan jaringan *Wireless*.

## 1.2 Rumusan Masalah

Melihat Latar belakang masalah diatas, maka yang menjadi pokok permasalahan adalah sebagai berikut:

1. Apakah sistem keamanan jaringan *WPA2-PSK* aman?
2. Apakah serangan *Brute Force* menggunakan Acrylic wifi, mampu menembus system keamanan wpa-2psk?

### 1.3 Batasan Masalah

Dalam Rangka Mengarahkan penelitian berdasarkan rumusan masalah yang telah dipaparkan, maka perlu adanya Batasan masalah sebagai berikut:

1. Alat yang di uji hanya pada perangkat router HG824H5.
2. Pengujian terbatas menggunakan metode *Brute Force* dan software yang digunakan adalah Acrylic wi-fi
3. Panjang kombinasi Password karakter adalah maksimal 8,10,dan 12 yang Kemudian Tanpa Pengulangan.
4. Proses Uji Maksimum dilakukan sebanyak 30x, pada setiap scenario.
5. Kombinasi karakter yang digunakan hanya huruf tertentu yang dipilih oleh penulis.
6. Serangan *Brute Force* hanya Menggunakan Dictionary Penulis.
7. Pengujian Hanya Berfokus pada lama waktu pengujian dan keberhasilan.

### 1.4 Maksud dan Tujuan Penelitian

Sebagai Syarat Kelulusan untuk mendapatkan gelar sarjana di program studi informatika fakultas ilmu computer di universitas amikom Yogyakarta.

Adapun Tujuan Penelitiannya adalah:

1. Membuktikan jaringan yang menggunakan *WPA2-PSK* aman dari serangan metode *Brute Force Attack*.
2. Untuk mengetahui seberapa lama system keamanan yang menerapkan wpa-2psk tahan dari serangan *Brute Force Attack*.

## 1.5 Metode Penelitian

Peneliti menjabarkan cara-cara memperoleh data-data yang digunakan untuk kebutuhan penelitian.

### 1.5.1 Metode Pengumpulan Data

#### 1.5.1.1 Studi Literatur

Penelitian mempelajari dasar teori yang relevan yang diambil dari penelitian-penelitian sebelumnya. Referensi-referensi tersebut diambil peneliti dari jurnal ilmiah dan buku sebagai dasar referensi.

#### 1.5.1.2 Metode Studi Pustaka

Peneliti menggunakan studi literature, yaitu membaca, mencari sumber informasi buku, internet, jurnal yang berkaitan dengan produk penelitian.

### 1.5.2 Metode Analisis

Pada bagian ini peneliti menggunakan metode analisis terutama pada data yang didapat. Metode analisis ini perlu di lakukan karena data yang masuk ke sistem ini agar dapat di olah sehingga menghasilkan suatu output informasi yang dapat di gunakan dalam penelitian.

### 1.5.3 Metode Eksperimental

Pada bagian ini peneliti akan membangun system jaringan sederhana dengan menggunakan keamanan *WPA2-PSK* kemudian melakukan percobaan penyerangan dengan metode *Brute Force*.

## **1.6 Sistematika Penulisan**

Sistematika penulisan skripsi ini memuat uraian secara garis besar isi skripsi untuk tiap-tiap bab, yaitu:

### **BAB I PENDAHULUAN**

Pada bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian, dan sistematika penulisan.

### **BAB II LANDASAN TEORI**

Pada bab ini berisi tentang tinjauan pustaka dan teori-teori yang digunakan peneliti untuk menunjang berlangsungnya penelitian ini.

### **BAB III METODELOGI PENELITIAN**

Dalam bab ini menjelaskan Gambaran umum, alat dan bahan, serta Langkah penelitian Dalam menunjang keberhasilan eksperimen

### **BAB IV IMPLEMENTASI DAN PEMBAHASAN**

Pada bab ini berisi tentang pengujian sistem serta hasil akhir dari pengujian password.

### **BAB V PENUTUP**

Kesimpulan akhir dari pengujian sistem yang telah dibuat serta memberikan saran yang dapat digunakan sebagai acuan pengembangan system selanjutnya.