BAB I
PENDAHULUAN

1.1. Latar Belakang

Pertumbuhan teknologi informasi yang semakin pesat tentu semakin memudahkan kebutuhan masyarakat dalam hal informasi. Aspek kemudahan kecepatan kehandalan dan keamanan tentu menjadi aspek penting dalam perkembangan teknologi informasi. Salah satu contoh dari perkembangan teknologi informasi adalah Teknologi Jaringan *Wireless* atau dapat disebut juga *Wireless Local Area Network(*WLAN). Penggunaaan teknologi ini sudah menjamur di berbagai tempat atau pun fasilitas fasilitas umum yang dikenal dengan nama Wifi Publik[1].

Namun seiring dengan perkembangan teknologi wifi tersebut,berkembang pula ancaman terhadap keamanan teknologi wifi disertai dengan tidak sedikit pula yang melalaikan aspek keamanan komunikasi informasi pada teknologi jaringan wifi tersebut [2]. Keamanan jaringan merupakan salah satu bab yang penting dalam mengamankan data[3]. Kelemahan teknologi jaringan nirkabel atau Wireless dapat dikategorikan sebagai dua kelemahan, yaitu kelemahan yang terdapat pada sisi konfigurasi dan kelemahan yang terdapat pada sisi enkripsi yang digunakan[4]

Oleh karena itu perlu dilakukan sebuah analisis keamanan pada jaringan wireless khususnya Wifi Public. *Penetration Testing Execution Standard* merupakan salah satu metode yang dapat digunakan dalam kegiatan analisis tersebut. Metode ini berisi tentang langkah langkah dalam melakukan analisis keamanan jaringan, seperti *planning , discovery, attack, reporting* [5] . Analisis

akan dilakukan dengan cara mensimulasikan serangan pada jaringan nirkabel menggunakan hardware dan software yang telah didesain khusus untuk melakukan serangan serangan dalam jaringan nirkabel.

Kantor Sekretariat Daerah Kabupaten Sleman merupakan kantor pemerintahan yang menyediakan fasilitas Wifi untuk umum. Wifi umum tersebut terbilang cukup ramai digunakan baik oleh masyarakat umum maupun pegawai kantor tersebut. Mudah nya akses penggunaan wifi tersebut bisa disalahgunakan oleh orang orang yang tidak bertanggung jawab, apabila belum adanya pencegahan untuk mengatasi masalah keamanan pada jaringan wifi tersebut.

Penelitian ini menghasilkan sebuah *report* analisa yang berisi hasil dari penilaian keamanan yang dapat digunakan sebagai saran atau acuan guna meningkatkan keamanan komunikasi informasi pada jaringan wifi public Kantor Sekretariat Daerah Kabupaten Sleman

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, maka permasalahan yang akan dirumuskan pada penelitian ini adalah Menganalisa keamanan jaringan wifi publik pada Kantor Sekretariat Daerah Kabupaten Sleman menggunakan Metode Penetration Testing Execution Standard (PTES) dalam upaya mencegah kejahatan siber yang marak terjadi

1.3. Pertanyaan Penelitian

Berdasarkan latar belakang beserta perumusan masalah yang telah disampaikan, maka dapat disusun sebuah pertanyaan penelitian yaitu "Bagaimana tingkat keamanan wifi publik pada Kantor Sekretariat Kabupaten Sleman dalam upaya pencegahan serangan keamanan siber yang marak terjadi?"

1.4. Batasan Masalah

Adapun batasan masalah pada Penelitian ini , penulis membatasi masalah yang akan dianalisis , diantaranya adalah

1. Analisis keamanan wifi publik akan menggunakan metode Penetration Testing Execution Standard
2. Hanya jaringan Wifi Publik yang akan menjadi media untuk dilakukannya analisa di penelitian ini
3. Analisis akan dilakukan dengan melakukan *information gathering, vulnerability analysis, threat modeling, exploitation*
4. Serangan hanya menggunakan parameter *ARP Spoofing (Man-In-The-Middle-Attack), Wifi Deauthtentication Attack, Evil Twin Attack , Mac Spoofing*
5. Penulisan hanya akan memberikan saran atau solusi apa yang sebaiknya dilakukan dalam mengatasi serangan yang dilakukan penulis

1.5. Maksud dan Tujuan Penelitian

Adapun tujuan yang hendak dicapai penulis dalam penelitian ini, yaitu Mengetahui tingkat keamanan pada layanan Wifi Publik pada Kantor Sekretariat Daerah Kabupaten Sleman dengan cara menganalisis tingkat keamanannya.

1.6. Manfaat Penelitian

Dengan adanya maksud dan tujuan penelitian , sudah semestinya ada pula Manfaat yang diperoleh dari penelitian ini , antara lain:

1. Menghasilkan Report hasil analisis keamanan yang nantinya menjadi saran atau solusi bagi Kantor Sekretariat Daerah Kabupaten Sleman dalam hal peningkatan keamanan jaringan wifi publik nya

2. Memberikan gambaran serta solusi akan dampak yang dapat diakibatkan dari celah keamanan yang terdeteksi pada jaringan WLAN
3. Memberikan tambahan pengetahuan bagi para pengguna wifi publik tentang kerentanan keamanan pada jaringan yang sering para pengguna pakai

1.7. Metode Penelitian

Metode penelitian akan menggunakan metode Penetration Testing Execution Standard dalam melakukan analisis keamanan pada jaringan wireless.

1. Metode Pengumpulan Data

Penulis mengunakan metode Obsevasi dalam melakukan pengumpulan data yang akan dijabarkan sebagai berikut:

A. Metode Observasi

Data diperoleh dengan cara melihat secara langsung tempat atau objek yang menjadi bahan penelitian pada Kantor Sekretariat Daerah Kabupaten Sleman. Lalu melakukan Observasi guna mendapatkan data yang terkait atau dibutuhkan.

Tabel 1. 1 Alat dan Software

No	Alat/Software/Hardware	Fungsi
1	Laptop Attacker	Sebagai user penyerang
2	Laptop & Android	Sebagai user biasa
3	Wifi Public Kantor Sekretarit Daerah Kab Sleman	Sebagai media peretasan/ media analisis
4	Nessus	Information Gathering Vulnerability Analysis

5	Nmap/Zenmap	Information Gathering Vulnerability Analysis
6	Dmitry	Information Gathering Vulnerability Analysis

Tabel 1. 2 Software yang akan digunakan

No	Software	Fungsi
1	Ettercap	Exploitation
2	Driftnet	Exploitation
3	Bettercap	Exploitation
4	Dsniff	Exploitation
5	Aircrack	Exploitation
6	Airgeddon	Exploitation
7	Fluxion	Exploitation
8	Wireshark	Analysis
9	MacChanger	Exploitation
10	Hotspot Device Software	Exploitation

Tabel 1. 3 Ekspektasi Hasil

Jenis Serangan	Sofware	Hasil
ARP Spoofing/ Man In the Middle Attack	Ethercap,Bettercap, Dsniff	Sukses
ARP Spoofing/ Man In the Middle Attack	Driftnet	Gagal
Deauth Attack	Aircrack	Sukses

Fake AP	Airgeddon & Fluxion & Hotspot Device Software	Sukses
MAC Spoofing	Macchanger	Sukses

2. Metode Perancangan

Metode penelitian bersifat Analisa Kuantitatif dimana metode ini menggunakan metode Penetration Testing Execution Standard dimana akan dikumpulkan nya data dari objek lalu akan dilakukan berbagai percobaan dalam hal menguji tingkat keamanannya.

1.8. Sistematika Penulisan

Bab I **PENDAHULUAN**

Dalam bab ini membahas Pendahuluan yang isinya antara lain latar belakang, rumusan dan batasan masalah, tujuan, manfaat dan metode penelitian.

Bab II **TINJAUAN PUSTAKA**

Bab ini berisi Kajian pustaka, Penelitian terdahulu yang berkaitan dengan penelitian,, Landasan teori yang berisi teori teori yang secara detail membahas ilmu yang berkaitan dengan penelitian

Bab III **METODE PENELITIAN**

Bab ini membahas mengenai metode penelitian, alat dan bahan penelitian serta alur penelitian. Analisis semua masalah yang ada dimana akan diselesaikan dengan penelitian yang dilakukan

Bab IV **HASIL DAN PEMBAHASAN**

Menampilkan Hasil penelitian serta Analisa dan pembahasan yang telah dilakukan dalam penelitian

Bab V **PENUTUP**

Membahas mengenai Penutup berupa kesimpulan dan saran