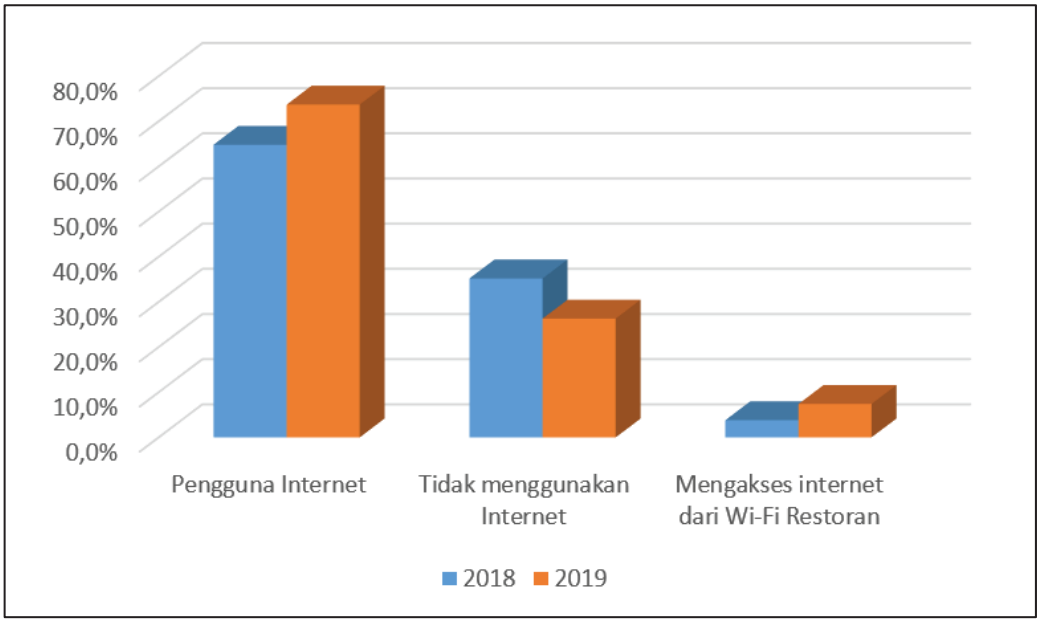
BAB I PENDAHULUAN

I.1 Latar Belakang

Penggunaan teknologi *wireless* digunakan karena lebih praktis dan dapat digunakan pada jarak yang jauh tanpa memerlukan kabel perantara untuk berkomunikasi. Salah satu contoh penerapan *wireless* saat ini yang paling banyak digunakan adalah Wi-Fi. Teknologi *wireless* berupa Wi-Fi ini sudah dapat ditemukan di berbagai tempat umum seperti kampus, kafe/restoran, hotel, bandara, bahkan pada warung kopi (Hayati, 2014). Terlebih lagi fasilitas tersebut dapat digunakan secara gratis untuk semua pengunjung, hal ini dapat mengancam keamanan informasi pengunjung yang terkoneksi dengan jaringan publik tersebut. Walaupun Wi-Fi tersebut sudah menggunakan *password* untuk keamanannya, bagi orang yang tidak bertanggung jawab hal tersebut adalah hal yang tidak sulit untuk meretas *password* Wi-Fi, bahkan mencuri data dan informasi sensitif dari pengguna Wi-Fi publik lainnya.

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melakukan survei mengenai pengguna internet di Indonesia pada tahun 2018 dan 2019. Berdasarkan survei di tahun 2018, penetrasi pengguna internet berjumlah 171,17 juta jiwa atau sebanyak 64,8% dari total populasi penduduk Indonesia yaitu 264,16 juta orang. Survei pengguna yang mengakses internet dari Wi-Fi pada restoran sebanyak 3,8% di tahun 2018 (APJII, 2018). Pada tahun 2019 Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) melakukan survey kembali. Berdasarkan Survei di tahun 2019, penetrasi pengguna internet berjumlah 196,71 juta atau sebanyak 73,7% dari total populasi penduduk Indonesia yaitu 266,91 juta orang (APJII, 2019). Survei pengguna yang mengakses internet dari Wi-Fi pada restoran sebanyak 7,4% di tahun 2019. Berdasarkan hasil survey jumlah pengguna internet meningkat sebanyak 8,9% dan banyaknya jumlah pengguna yang mengakses internet dari Wi-Fi restoran meningkat sebanyak 3,6% dari tahun sebelumnya.



Gambar 1. 1 Grafik Survei Mengenai Pengguna Internet (APJII, 2019)

Jaringan *wireless local area network* (WLAN) menggunakan frekuensi radio sebagai media untuk melakukan pertukaran data. Hal tersebut menyebabkan *layer* satu dan *layer* dua yaitu *physical* dan *data link* terekspos pada daerah jangkauan jaringan *wireless*. Jaringan WLAN biasanya beroperasi dalam dua rentang frekuensi yaitu 2,4 GHz dan 5,0 GHz pada standar 802.11a/b/g/n. Didalam setiap *band*, terdapat banyak saluran (*channel*).

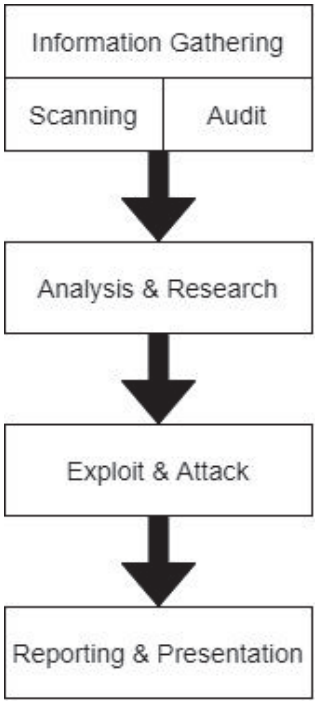
Setiap orang dapat melakukan *monitoring* terhadap seluruh wilayah jaringan *wireless* dengan memasukkan kartu jaringan (*wireless card*) ke dalam *mode monitor* di saluran yang sama. Komunikasi WLAN terjadi melalui *frame* untuk melakukan komunikasi. Ada tiga jenis *frame* MAC 802.11 yaitu: *data*, *control*, dan *management* (Jordan & Chaouki, 2002). Mayoritas penyerangan terhadap jaringan WLAN menargetkan *frame management*, karena *frame* tersebut bertanggung jawab untuk *authentication*, *association*, *disassociation*, *beacons*, dan *probe request/response* (Sheldon dkk., 2012). Serangan nirkabel seperti *denial of services* (DoS), serangan *man-in-the-middle* (MITM) diimplementasikan dalam *frame* 802.11 dan tidak dapat dideteksi pada lapisan tiga melalui *access point* secara langsung (Wang dkk., 2011).

Di daerah Jakarta Timur, dapat mudah ditemukan restoran yang menyediakan fasilitas Wi-Fi yang dapat digunakan oleh pengunjung restoran. Untuk mengetahui apakah jaringan WLAN pada restoran di daerah Jakarta Timur, peneliti menggunakan metode dan berbagai *tools* untuk melakukan pengujian penyerangan.

Pada penelitian ini peneliti melakukan analisa dan evaluasi terhadap Wi-Fi restoran di Jakarta Timur menggunakan metode *penetration testing* yaitu metode dengan melakukan pengujian sistem keamanan dengan mensimulasikan berbagai bentuk penyerangan terhadap keamanan jaringan dan metodologi pengujian yaitu *Information Systems Security Assessment Framework* (ISSAF) *WLAN Security Assessment Methodology*.

Untuk melakukan *penetration testing* peneliti menggunakan airgeddon yang telah di *download* dan di instal pada sistem operasi Kali Linux. Penggunaan airgeddon membantu peneliti melakukan pengujian penyerangan tanpa perlu melakukan konfigurasi *tools* pada kali linux dari awal untuk melakukan *penetration testing* terhadap jaringan WLAN restoran. Airgeddon dapat menjalankan penyerangan hanya dengan memilih menu yang sudah disediakan, dan secara otomatis airgeddon akan melakukan integrasi antara *tools* yang terdapat pada Kali Linux untuk melakukan berbagai macam jenis serangan. Untuk dapat menggunakan airgeddon *wireless interface card* harus masuk kedalam *mode monitor* terlebih dahulu.

Peneliti menggunakan ISSAF *WLAN Security Assessment Methodology* karena metodologi tersebut memiliki beberapa keunggulan yaitu struktur intuitif yang dapat memberikan arahan kepada penguji sistem melalui langkah-langkah yang mudah dipahami serta memberikan rekomendasi *tools* untuk melakukan *penetration testing* (Mussadiq, 2014). ISSAF *WLAN Security Assessment Methodology* memiliki empat tahapan yaitu 1) *Information gathering, Scanning* & *Audit*, 2) *Analysis & Research*, 3) *Exploit & Attack,* 4) *Reporting Presentation*. Berikut adalah tahapan yang dilakukan dengan standar ISSAF *WLAN Security Assessment Methodology* yang dapat dilihat pada Gambar 1. 2.



Gambar 1. 2 Fase dan Tahapan *Assessment* ISSAF *WLAN Security Assessment Methodology* (Rathore dkk., 2006)

Berdasarkan uraian diatas, penelitian ini dilakukan untuk mengevaluasi dan menganalisis kerentanan keamanan jaringan Wi-Fi pada restoran. Oleh karena itu dengan menggunakan metode dan *tools* yang sudah dijelaskan sebelumnya untuk mengevaluasi dan menganalisa keamanan jaringan Wi-Fi, maka peneliti mengambil judul tugas akhir "Analisis Keamanan Jaringan *Wireless* LAN Dengan Menggunakan ISSAF *WLAN Security Assessment Methodology* Studi Kasus Pada Restoran di Jakarta Timur".

I.2 Perumusan Masalah

Dengan berdasarkan latar belakang, maka rumusan masalah pada tugas akhir ini yaitu sebagai berikut:

1. Bagaimana cara pengujian kerentanan terhadap keamanan jaringan Wi-Fi restoran di daerah Jakarta Timur?
2. Bagaimana analisis hasil pengujian keamanan yang ditemukan pada jaringan Wi-Fi restoran di daerah Jakarta Timur?
3. Bagaimana solusi yang dapat dilakukan untuk mengantisipasi dan mencegah penyerangan yang dapat dilakukan pada Wi-Fi restoran di daerah Jakarta Timur?

I.3 Tujuan Penelitian

Tujuan yang hendak dicapai peneliti dalam penelitian ini adalah sebagai berikut:

1. Untuk melakukan pengujian kerentanan terhadap keamanan jaringan Wi-Fi restoran di daerah Jakarta Timur
2. Untuk memberikan hasil analisis pengujian keamanan yang ditemukan pada jaringan Wi-Fi restoran di daerah Jakarta Timur
3. Untuk memberikan solusi kepada restoran dan pengguna Wi-Fi publik untuk melakukan antisipasi dan pencegahan terhadap serangan yang dapat dilakukan pada jaringan Wi-Fi restoran di daerah Jakarta Timur

I.4 Batasan Penelitian

Pada bagian ini menjelaskan batasan dari penelitian yang dapat berupa asumsi atau limitasi terhadap objek yang akan diteliti, adapun batasan masalah pada tugas akhir ini yaitu:

1. Perangkat yang akan dilakukan serangan memiliki koneksi internet
2. Perangkat korban masih menggunakan *web browser* versi lama dan belum ter*update*
3. Penggunaan standar ISSAF *WLAN Security Assessment Methodology* hanya sebagai pedoman untuk melakukan proses penemuan keamanan jaringan *wireless*
4. Hanya melakukan penyerangan *Penetration Testing* untuk menguji kerentanan jaringan *wireless*
5. *Website* yang dikunjungi oleh korban belum menggunakan protokol *HTTP Strict Transport Security* (HSTS)
6. Korban penyerangan sebelumnya tidak pernah mengunjungi situs *website* tujuan
7. Ruang lingkup hanya pada jaringan lokal tiap restoran

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1. Bagi pengelola restoran yang dikunjungi di wilayah Jakarta timur dapat menggunakan informasi celah keamanan sebagai saran untuk meningkatkan keamanan jaringan Wi-Fi restoran.

2. Bagi peneliti lain yang bergerak dalam sistem informasi pendidikan tinggi, penelitian ini bermanfaat untuk mengetahui macam-macam celah keamanan dari jaringan Wi-Fi, jenis serangan yang dapat dilakukan pada jaringan Wi-Fi, dan sebagai pengetahuan untuk dapat mengantisipasi penyerangan pada jaringan Wi-Fi yang dapat merugikan.

I.6 Sistematika Penulisan

Adapun penulisan dalam penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Pada bab ini berisi uraian mengenai konteks permasalahan, latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

Bab II Tinjauan Pustaka

Bab ini berisi literatur yang relevan dengan permasalahan yang diteliti dan dibahas pula hasil-hasil penelitian terdahulu.

Bab III Metodologi Penelitian

Pada bab ini dijelaskan langkah-langkah penelitian secara rinci meliputi: model konseptual, sistematika penelitian, alasan pemilihan metode, dan jadwal kegiatan.

Bab IV Perancangan Pengujian

Bab ini menguraikan detail perancangan pengujian, *hardware* dan *software* yang akan digunakan selama penelitian serta tahapan pengujian terhadap jaringan target.

Bab V Hasil dan Evaluasi

Pada bab ini, disajikan hasil rancangan, temuan kerentanan, dan hasil pengujian penyerangan.

Bab VI Kesimpulan dan Saran

Pada bab ini dijelaskan kesimpulan dari penelitian yang dilakukan serta jawaban dari rumusan masalah yang disebutkan sebelumnya. Saran penelitian dikemukakan pada bab ini untuk penelitian selanjutnya.