

# BAB I PENDAHULUAN

## 1.1 Latar Belakang Masalah

Pemanfaatan teknologi berbasis wireless pada saat ini sudah semakin banyak, baik digunakan untuk pendidikan maupun untuk komersil. Warnet Fortran merupakan salah satu warnet yang memanfaatkan teknologi ini. Namun di balik kepopuleran teknologi ini terdapat kelemahan yang harus di benahi. Kelemahan teknologi ini sangat rentan terhadap serangan yang dilakukan oleh attacker, itu dapat terjadi karena komunikasi yang berlangsung sangat terbuka. Diperlukan pengamanan yang berlapis agar dapat meminimalkan serang tersebut.

Celah keamanan ini tercipta juga dimungkinkan karena kurangnya perhatian oleh admin terhadap jaringan wirelessnya. Admin menganggap jaringannya sudah aman dengan sistem keamanan yang tersedia sehingga tidak lagi memperhatikan lebih mendalam mengenai proteksi terhadap masalah keamanan.

Warnet Fortran pun sudah berupaya untuk meminimalkan kelemahan teknologi tersebut, yaitu dengan captive portal (*Open System Authentication*). Authentication pada metode ini terjadi pada saat user/pengguna melakukan pengaksesan internet untuk pertama kali. Metode ini pun belum biasa di jadikan pedoman bahwa jaringan wireless aman dari serangan attacker. Maka dari itu diperlukan percobaan untuk mengetahui celah keamanan yang masih ada, sehingga dapat mencegah terjadinya kerugian pada Warnet Fortran, serta dapat digunakan untuk meningkatkan kualitas sistem wireless pada Warnet Fortran.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka permasalahan yang ada dalam Skripsi ini yaitu

- a. Bagaimana kondisi sistem wireless pada Warnet Fortran?
- b. Bagaimana sistem keamanan wireless yang ada di dalamnya?
- c. Bagaimana cara untuk mengamankan sistem wireless tersebut dari serangan?

## 1.3 Batasan Masalah

- a. Penelitian hanya membahas mengenai kondisi serta keamanan wireless di Warnet Fortran.
- b. Implementasi terbatas pada peningkatan keamanan sistem jaringan wireless captive portal di Warnet Fortran

## 1.4 Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengetahui keadaan sistem wireless pada Warnet Fortran, serta mengetahui celah – celah keamanan pada sistem wireless captive portal, yang nanti dapat digunakan untuk meningkatkan keamanan sistem.

## 1.5 Manfaat Penelitian

Penelitian yang dilakukan memberikan beberapa manfaat antara lain :

1. Bagi Penulis

- a. Memperoleh gelar sarjana komputer STMIK Amikom Yogyakarta.
- b. Mengembangkan ilmu serta teori yang telah didapatkan selama masa perkuliahan untuk persiapan dunia kerja.

## 2. Bagi Obyek Penelitian

- a. Diketahuinya informasi mengenai sistem wireless, penyedia jasa wireless dapat lebih meningkatkan kinerja jaringan wireless di Warnet Fortran.

### 1.6 Metodologi Pengumpulan Data

#### a. Ujicoba

Peneliti menggunakan 2 perangkat laptop untuk melakukan percobaan. Satu perangkat bertindak sebagai client resmi dan perangkat yang lain sebagai penyerang. Perangkat yang bertindak sebagai *client* resmi untuk terhubung ke internet harus membeli voucher, sedangkan perangkat yang bertindak sebagai penyerang tidak menggunakan voucher tetapi menunggu client resmi yang terhubung ke internet. *Client* resmi terhubung dengan *Acces point* dan mulai mengakses internet, pada saat itu penyerang konek ke *Acces point* dan mulai melakukan serangan. Metode Penyerangan menggunakan Mac spoofing. Metode ini penyerang melakukan scanning pada jaringan wireless untuk mendapatkan mac address client resmi, setelah mendapat mac address penyerang melakukan *cloning mac address client* resmi, penyerang pun

dapat mengakses internet tanpa memasukkan login. Metode lainnya menggunakan tool wireshark untuk mendapatkan informasi *username* dan *password client* resmi.

b. Studi Pustaka

Studi pustaka dilakukan dengan membaca buku untuk mendapatkan menunjang laporan yang berkaitan dengan topik yang diambil serta pemecahan masalah yang ada.

### 1.7 Sistematika Penulisan

Penyusunan laporan skripsi ini dibagi ke dalam beberapa bagian pada tiap bab yang ada. Penjelasan dari masing – masing bab dijelaskan sebagai berikut:

#### BAB I : PENDAHULUAN

Membahas mengenai dasar pemikiran diambilnya judul tugas akhir ini. Berisi sub bab antara lain, Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metodologi Penelitian.

#### BAB II : LANDASAN TEORI

Membahas landasan teori yang dijadikan sumber acuan dalam penulisan laporan tugas akhir. Terdapat beberapa subbab dalam bab ini, diantaranya yaitu, pembahasan mengenai Internet, Jaringan Komputer Wireless LAN, Protokol TCP/IP.

### BAB III: ANALISA DAN PERANCANGAN

Membahas mengenai metodologi penelitian. Terdapat beberapa subbab dalam bab ini, diantaranya yaitu Waktu dan Tempat Pelaksanaan Percobaan, Profil Warnet sebagai objek penelitian, Peralatan – peralatan yang dibutuhkan dalam Proses Penelitian, Tahap Analisis dan Perancangan

### BAB IV : IMPLEMENTASI DAN PEMBAHASAN

Merupakan bab inti dari penyusunan laporan tugas akhir. Terdapat beberapa subbab pada bab ini, yaitu subbab yang membahas mengenai Implementasi keamanan, pengujian serta pembahasannya.

### BAB V : PENUTUP

Merupakan bab penutup dari penyusunan laporan tugas akhir. Pada bab ini diuraikan mengenai kesimpulan dan saran dari percobaan yang telah dilaksanakan

## 1.8 Jadwal Penelitian

Tabel 1.1 Jadwal penelitian

No	Kegiatan	Bulan/Tahun					
		Sep '12	Okt '12	Nov '12	Des '12	Jan '13	Feb'13
1	Studi Pustaka						
2	Pengumpulan Data/Analisis						
3	Implementasi						
4	Penulisan Skripsi						
5	Penyerahan Skripsi						

