BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi *ICT (Information Communication Technology)* telah mempengaruhi perkembangan pada pola pembelajaran, pola interaksi dan cara pengelolaan sistem Perguruan Tinggi. Suatu Perguruan Tinggi dikatakan bisa bersaing bila dilihat dari fasilitas penunjang kampus. Layanan yang baik tersebut dinamakan *Smart Campus* yang menjadikan suatu kampus terhubung secara *online*, seperti pertukaran data, aktifitas pendidikan, riset dan lainnya. Untuk menunjang *Smart Campus* diperlukan layanan yang lebih efisien, seperti absensi yang berbasis *ICT* misalnya sistem *RFID (Radio Frequency Identification)* untuk melakukan absensi. Tetapi untuk menunjang *Smart Campus*, berbagai perangkat harus saling terhubung, termasuk dengan perangkat *mobile* yang digunakan setiap mahasiswa.

Dengan sistem *Smart Identification,* server akan mengintegrasikan *access point* dengan perangkat *mobile.* Server akan mendapatkan data dari perangkat *mobile* yang terhubung dengan *access point*. Data yang didapat berupa MAC *address* dari setiap perangkat *mobile* yang terhubung. Setiap perangkat yang terhubung pada jaringan tidak selamanya aman, sisi keamanan jaringan pada sistem sangat penting untuk melakukan validitas dan integritas serta menjamin layanan bagi penggunanya.

Banyak masalah yang terjadi pada keamanan MAC *address* adalah sering terjadinya penyerangan pada server, *access point*, serangan ARP *spoofing* dan ARP *poisoning*. Masalah tersebut terjadi karena lemahnya sistem keamanan jaringan. Untuk mengatasi keamanan jaringan pada sistem perlu adanya pendeteksi dalam suatu jaringan. Arpon adalah *software* untuk mendeteksi dan mencegah sistem dari serangan ARP *spoofing* dan ARP *poisoning.* Arpon mempunyai fungsionalitas untuk menghindari *Man In The Middle (MITM)* serangan melalui ARP *spoofing,* ARP *cache poisoning* atau ARP *poison routing*. Cara kerja Arpon adalah ketika arpon dijalankan, arpon mulai bekerja untuk mengecek apakah ada serangan atau tidak, jika ada

serangan masuk, makan arpon akan mendeteksi serangan tersebut dan mengeluarkan notifikasi berupa *log file*, bila serangan tidak terdeteksi maka serangan berhasil masuk.

Oleh karena itu, dalam proyek akhir ini akan diimplementasikan keamanan MAC *address* di *access point* pada sistem *smart identification*. Untuk menunjang layanan *Smart Campus* yang saling terhubung.

1.2 Rumusan Masalah

Rumusan masalah dalam proyek akhir ini adalah sebagai berikut:

1. Bagaimana mengimplementasikan keamanan MAC *address* dari serangan ARP *spoofing* dan ARP *poisoning* di *access point* pada sistem *smart identification* ?
2. Bagaimana cara memberikan notifikasi serangan berupa *log file* jika terjadi penyerangan ?
3. Bagaimana mengintegrasikan hasil *log file* arpon ke *web interface* ?

1.3 Tujuan

Berdasarkan rumusan masalah, tujuan proyek akhir ini adalah sebagai berikut:

1. Implementasi Keamanan MAC *Address* di *access point* pada sistem *smart identification* menggunakan Arpon.
2. Dapat memberikan notifikasi berupa *log file* ketika terjadi penyerangan.
3. Dapat mengintegrasikan hasil *log file* berupa tampilan web interface.

1.4 Batasan Masalah

Ruang lingkup proyek akhir ini dibatasi sebagai berikut :

1. Implementasi Server menggunakan sistem operasi Ubuntu,
2. Implementasi MAC *Address* untuk mengetahui setiap perangkat yang terhubung pada *access point*,

3. Implementasi *access point* menggunakan *Linksys Wireless-G Broadband Router,*
4. Pendeteksi serangan menggunakan aplikasi ArpOn,
5. Pencegahan serangan menggunakan aplikasi ArpOn,
6. Jenis serangan yang digunakan adalah serangan yang berupa ARP *spoofing* dan ARP *poisoning,*
7. Serangan hanya dilakukan oleh satu penyerang, dan satu kali penyerangan,
8. Layanan yang diberikan server berupa *DNS Server, Web server* dan *MySQL*,
9. Satu server mempunyai dua fungsi sebagai server arpon dan *monitoring*,
10. Menggunakan jaringan *WLAN (Wireless Local Area Network)*.

1.5 Definisi Operasional

Smart identification menurut terjemahan bahasa inggris *smart* artinya pintar atau cerdas, sedangkan *identification* artinya identifikasi. Identifikasi menurut Kamus Besar Bahasa Indonesia diartikan tanda kenal diri atau menetapkan identitas. *Smart Identification* dapat diartikan sebagai identitas yang dikenali secara otomatis oleh sistem dan memanfaatkan teknologi *wireless* untuk menghubungkannya. Perangkat *mobile* akan digunakan sebagai identitas pengguna untuk melakukan identifikasi yang terhubung dengan *access point* yang menampilkan MAC *address* di *database* server. *Access point* sebagai jembatan *(bridge)* antara server dengan perangkat *mobile*. Sistem Operasi yang akan digunakan sistem operasi Ubuntu pada sisi server.

1.6 Metode Pengerjaan

Metode pengerjaan yang digunakan adalah *NDLC (Network Development Life Cycle)* dengan tahapan studi literatur, perancangan sistem, konfigurasi sistem, implementasi, pengujian dan penyusunan laporan.

1. Studi Literatur

Mencari informasi dan mempelajari hal yang berkaitan dengan proyek akhir, seperti Keamanan Jaringan yang mengamankan MAC *Address* dari serangan terhadap server.

2. Perancangan Sistem

Langkah ini dilakukan untuk melakukan perancangan sistem jaringan berbasis *client* server.

3. Konfigurasi Sistem

Pembangunan sistem dengan melakukan konfigurasi arpon pada server agar membangun sistem keamanan dengan tingkat yang baik.

4. Implementasi

Langkah selanjutnya adalah implementasi. Implementasi memuat hal mengenai instalasi dan konfigurasi semua layanan yang dibutuhkan.

5. Pengujian

Pengujian dilakukan setelah instalasi dan konfigurasi berjalan dengan baik, berupa simulasi *Smart Identification* untuk mengamankan MAC *address* yang terhubung ke *access point.*

6. Penyusunan Laporan

Pada langkah ini semua metode yang telah dilakukan dan data uang terkumpul dibuat dokumentasi berupa laporan proyek akhir dalam kaidah penulisan yang telah ditentukan.

1.7 Jadwal Pengerjaan

Tabel 1- 1 Jadwal Pengerjaan

No	Kegiatan	Waktu Pelaksanaan Tahun 2016																					
		Januari		Februari				Maret				April				Mei				Juni			
		3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																						
2	Perancangan Sistem																						
3	Konfigurasi Sistem																						
4	Implementasi																						
5	Pengujian																						
6	Penyusunan Laporan																						