1. PENDAHULUAN

1.1 Latar Belakang

Lebih dari 3,73 milliar orang di seluruh dunia memanfaatkan akses internet dan memanfaatkannya dalam aktivitas sehari-hari [1], dengan itu ancaman serangan bisa saja terjadi ketika kita menggunakan jaringan *wireless* yang dapat menyebabkan data pengguna dicuri oleh pihak yang tidak bertanggung jawab, ancaman serangan *Spoofing* adalah termasuk salah satu serangan dengan frekuensi tertinggi [2] yang terjadi di jaringan *wireless*.

ARP (*Address Resolution Protocol*) adalah sebuah protokol dalam TCP/IP yang bertanggung jawab dalam menerjemahkan alamat IP ke alamat MAC (*Media Access Control*) Address, ARP *spoofing attack* alamat MAC dapat dimodifikasi oleh penyerang dengan menautkan alamat MAC-nya sendiri ke alamat IP yang diberikan [3], sehingga membuatnya rentan terhadap serangan *spoofing*. ARP spoofing adalah serangan yang mengirimkan ARP palsu yang sudah dimodifikasi untuk meracuni ARP cache table korban, serangan ini mendukung terjadinya serangan jaringan komputer lainnya seperti denial of service (DoS) attack, Man in the Middle Attack, dan lain-lain.

Penelitian yang dilakukan juga menggunakan aplikasi *nettcut* untuk melakukan serangan *spoofing* yang dilakukan pada jaringan WLAN (*Wireless Local Area Network*) juga mendapatkan persentase tinggi [4].

Salah satu upaya untuk meminimalkan kemungkinan adanya serangan yang terjadi dalam suatu jaringan komputer ketika terkoneksi internet yaitu dengan membangun suatu sistem yang nantinya mampu meningkatkan keamanan jaringan. Salah satu teknik yang digunakan untuk melindungi kemanan jaringan yaitu dengan membangun sistem yang menggunakan metode *string matching* dengan algoritma *boyer moore* dan *brute force*, *string matching* akan mencari MAC *address* yang mencurigakan, kemudian sistem yang dibangun akan memberikan laporan atau notifikasi bahwa komputer sedang disadap.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, rumusan masalah yang menjadi bahan kajian dalam penyusunan tugas akhir adalah:

1. Bagaimana cara kerja metode *string matching* untuk mendeteksi *ARP spoofing*?
2. Bagaimana kecepatan waktu deteksi pada *ARP spoofing* menggunakan metode *string matching* dengan algoritma *boyer moore* dan *brute force*?

1.3 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut :

1. Merancang *string matching* dengan algoritma *boyer moore* untuk mendeteksi perubahan MAC *address.*
2. Melakukan analisis waktu deteksi pada sistem yang dibangun dengan metode *string matching* dengan algoritma *boyer moore* dan *brute force*.

1.4 Rencana Kegiatan

Untuk menyelesaikan tugas akhir ini, maka perlu disusun rencana kegiatan sebagai berikut:

1. Studi Literatur

   Pada tahap ini dilakukan pencarian materi dalam tugas akhir terhadap masalah yang akan dibahas dengan mencari referensi sebanyak-banyaknya pada penelitian sebelumnya yang berkaitan dengan keamanan jaringan, ARP *Spoofing*, *String Matching Method*, *Boyer Moore*, *Brute Force*.

2. Perancangan dan Implementasi system

   Pada tahap ini akan dilakukan perancangan serta implementasi sistem keamanan dengan menggunakan *string matching* terhadap serangan *spoofing*.

3. Pengujian hasil dan analisis

   Pada tahap ini hasil dari impelementasi sistem yang dibangun menggunakan metode *string matching* akan diuji tingkat keakurasian waktu deteksi terhadap serangan *spoofing*, lalu akan dianalisis hasil pengujiannya.

4. Penyusunan Tugas Akhir

   Setelah melakukan Analisa hasil terhadap sistem yang dibangun, disusunlah laporan secara menyeluruh terhadap hasil yang telah didapat.

1.5 Jadwal Kegiatan

Kegiatan	Bulan					
	1	2	3	4	5	6
Studi literatur						
Perancangan dan implementasi sistem						
Pengujian hasil dan analisis						
Penulisan laporan						

Tabel 1. Jadwal Kegiatan