BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi merupakan hal yang sangat penting bagi masyarakat saat ini. Dengan adanya internet membuat komunikasi dan informasi mudah didapatkan. Kemudahan ini yang menyebabkan terjadinya kejahatan *cyber* di dunia maya. Ancaman *cyber* terus berkembang dan menjadi lebih komplek seiring berjalannya waktu. Serangan seperti *Deathentication* tidak hanya meningkat dalam skala tetapi juga dalam tingkat kecerdasan dan kreativitas penyerang. Serangan *deauthentication* adalah jenis serangan yang bertujuan untuk memaksakan perangkat yang terhubung ke jaringan untuk terputus secara paksa[2]. Serangan ini dapat dilakukan dengan mengirimkan paket palsu yang menyebabkan gangguan layanan dan kehilangan konektivitas bagi pengguna yang terkena dampak. Serangan *beacon spam* melibatkan pengiriman sinyal palsu yang mencoba menarik perangkat untuk terhubung ke jaringan yang sebenarnya tidak ada[2]. Hal ini mengakibatkan pengguna mengalami gangguan karena perangkat mereka otomatis mencoba terhubung ke jaringan yang sebenarnya tidak berfungsi. Ancaman serangan seperti *deauthentication* dan *beacon spam* menunjukkan bagaimana teknologi yang seharusnya memberikan kemudahan akses juga dapat disalahgunakan. Penjahat *cyber* dapat memanfaatkan kelemahan dalam protokol jaringan nirkabel untuk menciptakan gangguan atau mengumpulkan informasi secara tidak sah. Potensi serangan *deauthentication* dan *beacon spam* dapat digunakan sebagai bagian dari serangan seperti *Man-In The-Middle* (MITM) atau pencurian data sensitif.

Maka untuk mengatasi masalah tersebut, pada penelitian ini dikembangkan sebuah sistem yang dapat mendeteksi adanya serangan. Alat ini dilengkapi banyak fitur yang sangat mendukung untuk mendeteksi adanya serangan *DOS. Packet Monitor* memiliki fitur untuk menangkap dan menganalisis trafik jaringan secara berkala. *Wi-Fi Analyzer* dapat memindai jaringan *Wi-Fi* yang tersedia. *Beacon Spam* adalah alat simulasi serangan yang bertujuan untuk melihat cara kerja dari *Beacon Spam*. *Deauth detector* digunakan untuk mendeteksi adanya *deuthentication attack*.

1.2 Tujuan dan Manfaat

Adapun tujuan dari penulisan Proyek Akhir ini, sebagai berikut:

1. Merancang sistem pendeteksi serangan dengan menggunakan *esp32* secara real time.
2. Menemukan dan mengeksploitasi kerentanan dalam jaringan untuk memastikan jaringan dapat diatasi sebelum dieksploitasi oleh peretas.

Manfaat dari penulisan Proyek Akhir ini, sebagai berikut.

1. Menemukan kelemahan sebelum peretas dapat mengeksploitasi jaringan, sehingga memberikan waktu untuk memperbaikinya.
2. Sistem monitoring membantu dalam mendeteksi masalah yang mungkin timbul dengan cepat, sehingga mengurangi resiko diserang.
3. Bisa mengoptimalkan kinerja jaringan di beberapa tempat yang rawan terjadinya *cyber attack.*

1.3 Rumusan Masalah

Adapun rumusan masalah dari Proyek Akhir ini, sebagai berikut.

1. Bagaimana cara merancang sistem pendeteksi serangan *DoS?*
2. Bagaimana cara memanfaatkan alat pemantauan keamanan?
3. Fitur apa saja yang digunakan untuk mendeteksi serangan *DoS?*

1.4 Batasan Masalah

Adapun batasan masalah dari Proyek Akhir ini sebagai berikut.

1. Menggunakan *esp32* sebagai mikrokontroller untuk mendeteksi adanya serangan.
2. Kapasitas memori yang terbatas dari *esp32* yang membatasi ukuran program dan jumlah data yang dapat disimpan atau diproses.
3. Mengandalkan konektivitas *Wi-Fi* yang dipengaruhi oleh interferensi atau jangkauan jaringan.
4. Perancangan sistem ini diperuntukkan untuk mengukur parameter-parameter *RSI* disuatu jaringan jika terkena serangan seperti DoS.

1.5 Metodologi

Sistematika penulisan dari penulisan ini terdiri dari lima bab, adapun uraian dari keenam bab tersusun sebagai berikut:

1. Studi Literatur

   Studi literatur dilakukan dengan mengumpulkan literatur-literatur dan kajian-kajian yang berkaitan dengan permasalahan yang ada pada penelitian Proyek Akhir ini, baik berupa buku referensi, artikel, maupun *e-journal* yang berhubungan dengan perangkat pemantauan keamanan jaringan.

2. Perencanaan sistem

   Perencanaan sistem dilakukan untuk menentukan rancangan sistem dan kebutuhan sistem yang akan dibuat seperti apa berdasarkan studi literature yang sudah dilakukan.

3. Perakitan

   Pada tahap ini dilakukan perakitan alat dengan menghubungkan sensor-sensor yang digunakan untuk melakukan penetrasi jaringan *Wi-Fi*.

4. Pengujian Alat

   Setelah semua sensor terhubung dan dapat berkomunikasi dengan *Access Point*, dilakukan pengujian pada setiap sensor yang akan digunakan dalam proyek akhir ini.

5. Analisis dan Kesimpulan

   Tahap awal akan dilakukan analisa untuk membandingkan data yang dihasilkan sensor dan data ketika sebelum dan sesudah melakukan penyerangan.

1.6 Sistematika Penulisan

Dalam penulisan Proyek Akhir terdiri atas lima bab, dengan keterangan sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi latar belakang, rumusan masalah, tujuan dan manfaat, batasan masalah, metodologi penelitian, serta sistematika penulisan.

BAB II DASAR TEORI

Pada bab ini membahas tentang teori pendukung pengerjaan Proyek Akhir, seperti konsep *Network Security*, *Network Penetration Testing*, *Security Attack*, dan lain sebagainya.

BAB III PERANCANGAN SISTEM

Pada bab ini membahas tentang deskripsi Proyek Akhir, alur pengerjaan Proyek Akhir, dan identifikasi data serta hasil dari pemantau keamanan jaringan.

BAB IV HASIL DAN PENGUJIAN

Pada bab ini membahas tentang pengujian dan analisis dari pemantau keamanan jaringan.

BAB V KESIMPULAN DAN SARAN

Pada bab ini membahas tentang kesimpulan dari pengerjaan Proyek Akhir dan saran untuk pembaca yang akan mengambil penelitian dengan topik yang sama.