

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang sangat maju mengakibatkan tingkat kebutuhan akan internet sebagai sistem komunikasi semakin meningkat.

Salah satu sistem internet sebagai alat komunikasi adalah jaringan LoRa. Jaringan LoRa merupakan sistem internet yang mampu menjangkau jarak jauh dan sangat hemat baterai. Namun jaringan LoRa mudah dikuping atau disamarkan oleh para penjahat untuk pencurian sinyal dan paket data yang berbasis informasi pribadi, seperti kredensial login, detail akun dan nomor kartu kredit. Target biasanya adalah pengguna aplikasi keuangan, bisnis SaaS, situs e-niaga dan situs web lain yang memerlukan login.

Hal ini menjadi hal penting bagi para teknisi jaringan untuk memberikan keamanan terhadap pengguna internet. Langkah Langkah keamanan tersebut adalah mencari tahu dan memahami cara kerja keamanan jaringan dan mencuri informasi dengan berbagai cara, salah satunya adalah memantau jaringan dengan software dan mencatat informasi yang jelas. Teknik yang digunakan pada langkah langkah diatas adalah *MITM (Man in the Middle) Attack*.

MITM (Man in the Middle) Attack juga dapat digunakan untuk menguping atau menyamarkan sinyal dan paket data seolah pertukarannya berlangsung normal. *MITM (Man in the Middle) Attack* dapat digunakan untuk mendengar percakapan pribadi, melihat berbagai informasi yang ada di dalam perangkat yang digunakan dan mengubah percakapan antara kedua belah pihak serta masih banyak fungsi lainnya.

Pada dasarnya langkah *MITM (Man in the Middle) Attack* digunakan untuk menentukan langkah keamanan. Langkah ini dapat diperoleh selama tahap infiltrasi seragan ancaman

yang persisten (APT) pada tingkat lanjut.

Atas dasar hal di atas, maka pada pengujian ini penulis ingin melakukan Man In The Middle (MITM) Attack untuk menunjukkan kerentanan jaringan LoRa dan mengidentifikasi kemungkinan jika terjadi serangan yang dilakukan ke jaringan dengan menggunakan sniffing dan/replay. Serangan pada jaringan dilakukan dengan mengimplementasikan protocol analyser (sniffer) untuk menangkap paket data. Sedangkan langkah sniffing diimplementasikan menggunakan perangkat keras RTL-SDR dan divisualisasikan melalui GNU-Radio.

Judul dalam penulisan buku ini adalah “Reverse Engineering LoRa Menggunakan GNURadio LoRa”.

1.2 Rumusan Masalah

Berikut rumusan masalah yang disampaikan oleh penulis dalam penelitian adalah sebagai berikut.

1. Cara melakukan Man In The Middle Attack yaitu sinyal LoRa ditangkap oleh antena RTL-SDR. Kemudian, diteruskan ke gnu radio untuk dilakukan sniffing, encoding, parsing, dan decoding.
2. Cara sinyal ditangkap oleh antena RTL-SDR yang berasal dari komunikasi antara transmitter dan receiver. Kemudian, untuk menerjemahkan sinyal dapat dilakukan dengan menggunakan blok yang ada di GNU Radio. Sehingga membentuk text dari sinyal LoRa yang dipancarkan.

1.3 Tujuan

Tujuan dari perancangan sistem tersebut adalah sebagai berikut :

1. Melakukan komunikasi data pada suhu dan kelembapan menggunakan LoRa, RTL-SDR, dan GNURadio.
2. Melakukan sniffing pada jaringan LoRa menggunakan GNURadio.

3. Melakukan pengujian Kuat Sinyal, Packet loss, dan akurasi bit yang diterima.

1.4 Batasan Masalah

Berikut adalah batasan masalah pada proyek akhir adalah sebagai berikut :

1. Melakukan komunikasi data suhu dan kelembapan menggunakan LoRa, RTL-SDR dan GNURadio.
2. Menampilkan data suhu dan kelembapan menggunakan Arduino Uno, SX1276, LCDI2C.
3. Software menggunakan GNURadio untuk melakukan sniffing dan decoding sinyal LoRa
4. Penangkapan sinyal LoRa menggunakan antena RTL-SDR.