BAB I
PENDAHULUAN

1.1. Latar Belakang

Internet merupakan jaringan komunikasi global yang menghubungkan komputer dan jaringan komputer di seluruh perangkat yang ada di dunia . Singkatan dari *Interconnected Network* ini memungkinkan kita dapat berbagi informasi dan berkomunikasi dengan keluarga, rekan kerja dan lain sebagainya. Internet di zaman sekarang ini sangat erat kaitanya dalam kehidupan sehari-hari. Mulai dari kalangan muda hingga kalangan dewasa, kebanyakan masyarakat menggunakan internet sebagai media bantu dalam mengerjakan dan menghubungkan berbagai aktivitas manusia secara efektif, akurat dan efisien.

Teknologi merupakan sebuah terobosan baru yang diciptakan manusia dari beberapa generasi ke generasi selanjutnya. *Internet Of Things* merupakan penemuan baru yang dikembangkan karena memiliki kelebihan yang mampu mendukung kinerja tanpa menggunakan bantuan kabel dan menggunakan cara *wireless*. Jenis perangkat *internet of things* (IoT) yang paling banyak diketahui oleh masyaralat pengguna yaitu *Smart home, Smart city, smart campus dan smart industrial*. *Internet Of Things* mendeskripsikan jaringan fisik yang dilengkapi dengan sensor, perangkat lunak, dan teknologi lain untuk tujuan saling terhubung dan bertukar data dengan perangkat dan *system* lain melalui internet.

Salah satu tantangan yang harus diatasi untuk mendorong implementasi IoT secara luas adalah factor keamana. IoT merupakan sebuah *system* majemuk. Kemajemukannya buka hanya karena keterlibatan berbagai entitas seperti data, mesin, RFID, sensor dan lain-lain, tetapi juga karena melibatkan berbagai peralatan dengan kemampuan komunikasi dan pengolahan data. Banyaknya entitas dan data

yang terlibat, membuat IoT menghadapi resiko keamanan yang dapat mengancam dan membahayakan konsumen. Ancaman ini utamanya dilakukan dengan cara memungkinkan orang yang tidak berhak untuk mengakses data dan menyalah gunakan informasi personal, memfasilitasi serangan terhadap *system* yang lain, serta mengancam keselamatan personal penggunanya (Arini et al., 2022).

System kendali dan pemantauan perangkat ruangan pada *smart home* merupakan sebuah bentuk kendali dan dipantau secara otomatis terhadap alat-alat listrik, *system* penerangan atau *system* keamanan rumah yang semuanya mampu dikendalikan dan dipantau secara langsung oleh pemilik. *System smart home* saat ini ada yang menggunakan instalasi kabel dan tanpa kabel. Sehingga pemantauan dan implementasi untuk instalasi secara nirkabel di realisasikan. Tingkat frekuensi kerja, efektivitas, dan beberapa kelebihan serta keunggulan lainnya dari komunikasi nirkabel ini, sangat cocok terhadap *system smart home* yang mendukung teknologi *modern* (Rachman, 2017).

Penulis menggunakan metode SQUARE *(Security Quality Requirements Engineering)* yang menyediakan identifikasi dan analisis kebutuhan dengan pendekatan masalah non-fungsional yang artinya kebutuhan yang menitik beratkan pada *property* perilaku yang dimiliki oleh sistem dan kebutuhan fungsional yang artinya berisi proses-proses apa saja yang nantinya dilakukan oleh sistem dan memberikan hasil keluaran berupa kategori dan prioritas keamanan jaringan. Metode *SQUARE* ini juga merupakan metode yang mencakup beberapa metode analisis keamanan jaringan. Hal ini menjadikan metode *SQUARE* sebagai metode yang mampu diterapkan dalam ruang lingkup masalah yang beragam (Mead & Stehney, 2005).

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, maka penulis merumuskan masalah penelitian Bagaimana menganalisis keamanan jaringan dalam *smart home* dengan metode *SQUARE* yang di rekomendasikan untuk mencari kerentanan dan memberikan kategori dan prioritas keamanan dalam jaringan *smart home*?

1.3. Batasan Masalah

Batasan masalah pada analisi keamanan jaringan ini penulis membatasi masalah dalam penelitian ini yaitu :

1. Infrastruktur yang digunakan merupakan Simulasi *Smart Home Internet of Things (IoT)* yang dibangun menggunakan *Cisco Packet Tracer* Versi 7.3.
2. Metode yang digunakan dalam penelitian ini adalah metode SQUARE (*Security Quality Requirements Engineering)*
3. Jenis serangan yang disimulasikan sebanyak 4 ancaman, yaitu , Reveal SSID, *MAC Address Spoofing*, *Rogue Access Point*, Dan DDOS.
4. Penulis tidak melakukan implementasi peningkatan keamanan pada *smart home* dan hanya memberikan solusi yang sebaiknya dilakukan untuk mengantisipasi terjadinya serangan dari kerentanan yang ditemukan seperti yang dilakukan penulis.

1.4. Tujuan Penelitian

Tujuan merupakan konsep untuk mencapai sesuatu yang di inginkan, tujuan yang di rancang yaitu Membantu menganalisis keamanan jaringan dalam *smart*

home yang di rekomendasikan untuk mencari kerentanan dan memberikan kategori dan prioritas keamanan dalam jaringan *Smart home.*

1.5. Manfaat Penelitian

Manfaat yang di harapkan dalam penelitian ini dibagi menjadi 2 bagian yaitu sebagai berikut:

a. Bagi Penulis

1. Sebagai sarana penelitian untuk menyelesaikan Skripsi
2. Diharapkan hasil analisis keamanan jaringan yang dikembangkan di Indonesia khususnya *Internet Of Things* dapat dikembangkan oleh penulis.
3. Indonesia merupakan negara dengan pengguna internet yang terus berkembang saat ini, dalam hal ini menjadikan suatu kehormatan dapat berpartisipasi dalam keamanan jaringan.
4. Sebagai sarana belajar untuk peneliti dalam mengembangkan keamanan jaringan *smart home* .

b. Bagi Universitas

1. Mengetahui kemampuan mahasiswa dalam menganalisi dan menerapkan imunya sebagai bahan Evaluasi.
2. Menambah referensi kepustakaan Universitas Teknokrat Indonesia.
3. Dapat di jadikan sebuah referensi dalam melakukan analisis keamanan jaringan untuk keperluan Universitas atau Akademik.

1.6. Keaslian Penelitian

Untuk menentukan keaslian penelitian penulis dengan judul " Analisis Keamanan Jaringan *Internet Of Things* (IoT) Dalam *Smart Home* Dengan Metode *SQUARE* Menggunakan *Cisco Packet Tracer* ". Adapun beberapa hal yang menjadi pembeda antara penelitian yang dilakukan penulis dengan penelitian yang sudah pernah dilakukan sebelumnya.

Perbedaan penelitian ini dengan penelitian yang akan dilakukan :

1. Lokasi, fungsi dan model infrastruktur *smart home* yang akan digunakan.
2. Menggunakan *cisco packet tracer* versi 7.3
3. Menggunakan 4 (empat) scenario uji coba serangan yaitu, Reveal SSID, *Rogue Access Point*, MAC *Address Spoofing* dan DDOS.
4. Implementasi, Teknik pengolahan data, dan tahapan penelitian
5. Dari segi manfaat penelitian, batasan penelitian, rumusah masalah dan tujuan penelitian.

Penelitian ini diharapkan dapat digunakan untuk perbaikan dan melengkapi penelitian-penelitian sebelumnya, sehingga keaslian penelitian ini dapat dijaga.