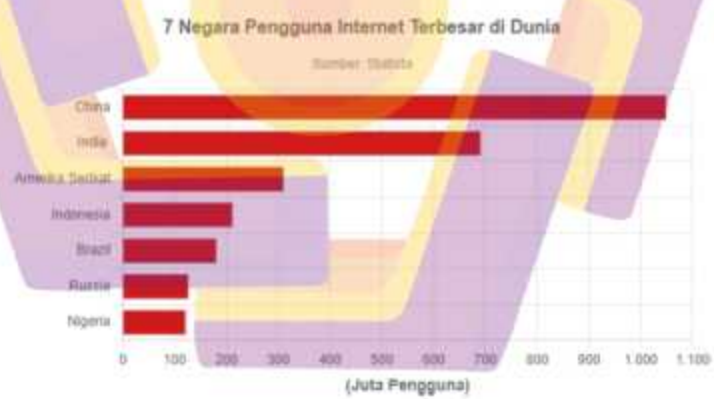
BAB I
PENDAHULUAN

1.1 Latar Belakang

Jumlah pengguna internet di dunia terus meningkat seiring dengan kebutuhan pendidikan, hiburan, media sosial, hingga bisnis. Menurut Statista, jumlah pengguna internet global diperkirakan mencapai 5 miliar pada tahun 2023. Asia Tenggara sendiri memiliki 1,24 miliar pengguna, sedangkan Afrika dan Timur Tengah relatif lebih sedikit. China menempati peringkat pertama dengan lebih dari 1 miliar pengguna internet, yaitu sekitar 75% dari total populasinya. Fenomena ini menunjukkan bahwa perkembangan teknologi digital semakin pesat dan tidak dapat dipisahkan dari kehidupan masyarakat. [1].

China sekarang memiliki pengguna internet terbanyak di dunia. Mengingat populasinya yang mencapai 1,4 miliar orang, 1,05 miliar dari mereka yang dapat mengakses internet, yang merupakan 75% dari total populasinya [2].



Gambar 1.1 Pertumbuhan pengguna internet menurut survei Statista

Di Indonesia, berdasarkan survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) tahun 2024, tingkat penetrasi internet meningkat hingga 79,5%, atau setara dengan 221,5 juta orang dari total populasi 278,6 juta jiwa [3]. Kementerian Komunikasi dan Informatika (Kominfo) menegaskan bahwa peningkatan tersebut menjadi landasan dalam memperkuat kerja sama lintas sektor untuk memperbaiki kualitas layanan internet. Perkembangan ini sekaligus menuntut adanya perhatian serius terhadap keamanan jaringan di Indonesia [4].

Gambar 1.2 Pertumbuhan internet di Indonesia menurut survei APJII.

Salah satu paradigma baru dalam perkembangan teknologi adalah *Smart Home*, yang menghubungkan berbagai perangkat ke internet. Konsep rumah pintar (*smart home*) menghadirkan efisiensi energi, kenyamanan, serta keamanan melalui integrasi perangkat seperti kamera pengawas, kunci pintar, hingga sistem pencahayaan otomatis. Namun, seiring meningkatnya jumlah perangkat yang terhubung, tantangan keamanan jaringan juga semakin besar, termasuk ancaman peretasan, pencurian data, hingga kontrol ilegal oleh pihak tidak berwenang [5].

Risiko keamanan jaringan pada smart home perlu ditangani secara serius melalui metode analisis risiko yang sistematis. Salah satu metode yang dapat digunakan adalah *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)*, yang dikembangkan oleh Carnegie Mellon University. Metode ini menawarkan pendekatan terstruktur untuk mengidentifikasi aset kritis, mengevaluasi ancaman, serta mengelola kerentanan. Dengan demikian, *OCTAVE* relevan untuk diterapkan dalam konteks jaringan *smart home* IoT.

Salah satu metode yang dapat digunakan untuk menganalisis risiko adalah *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)* yang dikembangkan oleh Carnegie Mellon University. Metode ini menawarkan pendekatan sistematis dalam mengidentifikasi aset kritis, mengevaluasi ancaman, serta mengelola kerentanan [6]. Untuk mendukung analisis, penelitian ini juga menggunakan *Cisco Packet Tracer* sebagai alat simulasi jaringan, sehingga dapat dilakukan pemodelan skenario serangan serta evaluasi mitigasi.

1.2 Rumusan Masalah

berdasarkan latar belakang diatas, maka peneliti merumuskan suatu masalah dalam penelitian ini, Yaitu :

1. Bagaimana metode *OCTAVE* digunakan dalam menganalisis risiko keamanan jaringan smart home IoT?
2. Bagaimana simulasi Packet Tracer dapat digunakan untuk menguji keamanan jaringan smart home?

1.3 Batasan Masalah

Berdasarkan permasalahan yang ada, maka peneliti membatasi masalah dalam penelitian ini, yaitu :

1. Metode yang di gunakan adalah metode *OCTAVE* (*operational cyber threat analysis vulnerability evaluation*) sebagai kerangka kerja utama untuk menganalisis risiko keamanan jaringan smart home.
2. Metode pengumpulan data yang digunakan adalah studi literatur dan simulasi.
3. simulasi Packet Tracer akan digunakan untuk menguji dan memvalidasikeamanan jaringan sebelum diimplementasikan secara nyata.
4. Simulasi menggunakan Cisco Packet Tracer.
5. Cisco Packet Tracer memiliki keterbatasan fitur, sehingga simulasi serangan aktif seperti Denial of Service (DoS) dan MAC Spoofing tidak dapat dilakukan secara langsung.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah menganalisis risiko keamanan jaringan smart home berbasis IoT dengan menggunakan metode *OCTAVE* serta mendukung analisis tersebut melalui simulasi jaringan pada *Cisco Packet Tracer*.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan manfaat bagi masyarakat dalam meningkatkan kesadaran akan pentingnya keamanan jaringan IoT, bagi akademisi sebagai referensi penelitian selanjutnya, serta bagi penulis memperdalam pemahaman mengenai analisis risiko keamanan jaringan.

1.6 Sistematika Penulisan

Beberapa pokok bahasan yang dibahas penulis dalam penyusunan skripsi ini termasuk:

BAB I PENDAHULUAN

Bab ini memberikan penjelasan tentang latar belakang penelitian, perumusan masalah, batasan dan tujuan penelitian, metode penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Bab ini membahas konsep dan teori yang mendasari penelitian ini. Literatur yang digunakan mencakup buku dan penelitian sejenis yang mendukung.

BAB III METODOLOGI PENELITIAN

Bab ini memberikan uraian lengkap tentang teknik penelitian yang digunakan, termasuk teknik pengumpulan data, teknik implementasi, dan teknik pengujian.

BAB IV HASIL DAN PEMBAHASAN

Bab ini mencakup analisis keamanan jaringan rumah pintar (Smart Home) dengan simulator *Cisco Packet tracer*, yang digunakan metode *OCTAVE* berdasarkan landasan teori yang telah diuraikan sebelumnya.

BAB V KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan penulis dan saran untuk pengembangan penelitian selanjutnya.