

# BAB 1

## PENDAHULUAN

---

### 1.1 Latar Belakang

Internet of Things (IoT) merupakan sebuah inovasi teknologi yang sudah banyak digunakan untuk mengembangkan perangkat menjadi lebih efisien dengan memanfaatkan konektivitas internet. Dalam konteks ini, Telkom IoT Platform hadir sebagai platform yang diproduksi oleh ITDRI (Indonesia Telecommunication Digital Research Institute) yang juga merupakan bagian PT Telkom Indonesia untuk mengelola dan mengintegrasikan perangkat IoT yang terhubung. Namun, semakin banyaknya perangkat yang terhubung meningkatkan risiko keamanan yang harus diatasi.

Pada saat ini, serangan terhadap sistem IoT semakin kompleks dan sering terjadi. Keberhasilan serangan dapat mengakibatkan kerugian finansial yang signifikan, kebocoran data sensitif, atau bahkan mengancam nyawa manusia. Oleh karena itu, sangat penting untuk secara teratur melakukan uji kerentanan atau penetration test pada sistem IoT.

Penelitian ini bertujuan untuk melakukan penetration test pada Telkom IoT Platform untuk mengidentifikasi dan menguji kerentanan yang mungkin ada dalam sistem. Dengan melakukan serangan simulasi dan menganalisis respons sistem, dapat diidentifikasi kerentanan yang perlu diperbaiki. Penelitian ini akan memberikan rekomendasi perbaikan keamanan yang efektif untuk meningkatkan keamanan Telkom IoT Platform.

Dengan mengintegrasikan praktik penetration test dalam siklus pengembangan dan pemeliharaan Telkom IoT Platform, PT Telkom Indonesia dapat memastikan bahwa platform mereka aman dari serangan dan menjaga kepercayaan pengguna serta integritas data. Penelitian ini juga memberikan kontribusi dalam memperkuat pemahaman umum tentang keamanan IoT dan praktik penetration test yang relevan.

### 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka berikut adalah beberapa masalah yang akan dibahas. Potensi kerentanan apa saja yang mungkin terdapat dalam Telkom IoT Platform. Teknik apa saja yang akan digunakan untuk mengidentifikasi kerentanan dan mengeksploitasi kerentanan tersebut.

### 1.3 Tujuan

Berikut adalah tujuan dari penteration testing yang dilakukan.

1. Menganalisis kerentanan keamanan yang mungkin ada di Telkom IoT Platform.
2. Melakukan implementasi penetration test menggunakan metode dan teknik yang sesuai untuk mengidentifikasi dan mengeksploitasi kerentanan tersebut.

### 1.4 Batasan Masalah

1. Penetration test difokuskan pada Telkom IoT Platform (console.telkomiot.id)
2. Penetration test yang dilakukan penulis hanya mencakup scanning port dan direktori, SQL injection, cross site scripting, dan clickjacking.
3. Pengujian ini tidak akan membahas aspek implementasi atau pengembangan Telkom IoT Platform itu sendiri, tetapi akan difokuskan pada pengujian keamanan.

### 1.5 Jadwal Pengerjaan

Berikut adalah tabel penjadwalan pengerjaan *penetration test*.

No	Deskripsi Kerja	September			
		1	2	3	4
1	Diskusi				
2	Perancangan				
3	Pengujian				

Tabel 1. 1 Penjadwalan Kerja