# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Dalam era digital yang semakin berkembang pesat, penggunaan perangkat *mobile* dan aplikasi berbasis *android* telah menjadi bagian tidak terpisakan dari kehidupan masyarakat Indonesia. Bedasarkan laporan *Statcounter Global Stasts*, Android mendominasikan penggunaan sitem operasi *mobile* di Indonesia dengan persentase sebesar 87,56 persen pada tahun 2023 [1]. Bahkan, Indonesia menjadi salah satu negara dengan jumlah unduhan aplikasi terbanyak kelima di dunia pada tahun 2021, dengan total unduhan sebesar 230 milliar aplikasi yang diunduh oleh pengguna *mobile* [2].

Hal tersebut menyebabkan munculnya banyak masalah dan ancaman privasi dan mendorong para peretas untuk melakukan kejahatan siber. Berdasarkan laporan *Vylnerabilitie and Therats in Mobile Application* tahun 2019 dari ptsecurity.com, sebanyak 43 persen aplikasi *android* memiliki kerentangan keamanan dengan resiko tinggi. Faktor utama yang menyebakan ini adalah kelemahan mekanisme keamanan sejak awal pengembangan aplikasi, serta adanya pemberihan hak istimewa yang tidak tepat dan sering dimanfaatkan oleh pihak yang tidak bertanggung jawab [3]

Di balik kemudahan dan fleksibiltas smarphone yang ditawarkan, terdapat juga risiko kemanan yang bisa dimanfaatkan untuk mencuri data dan informasi pengguna. Salah satunya aplikasi modifikasi (MOD) yang menyediakan fitur tambahan atau menghilangkan batasan dari aplikasi asli. Aplikasi ini sering kali disusupi malware atau virus, yang dapat menggancam keamanan data pengguna [4]. Aplikasi modifikasi (MOD) yang sering diunduh dan digunakan untuk mendapatkan fitur tambahan secara gratis. Aplikasi mod tersebut memiliki resiko yang tinggi terhadapat keamanan karna tidak melalui proses pemeriksaan yang ketat seperti aplikasi di *Google play store* [5] Penelitian kaspersky telah mengidentifikasikan bahwa ada aplikasi modifikasi yaitu aplikasi *whatsapp* mod

deangan versi terbarunya yang tidak hanya menawarkan tambahan seperti pesan terjadwal dan opsi yang dapat disesusaikan, namun juga berisi modul *spyware* yaitu jenis malware atau perangkat lunak berbahaya yang bertujuan mendapatkan informasi atau data sensitif, kaspersky mengidentifikasikan lebih dari 340 ribu serangan yang melibatkan mod ini [6].

Ancaman siber tidak telepas dari kecerobohan dan lemahnya sistem keamanan teknologi *online* sehingga menyebabkan dampak yang sangat buruk bagi pengguna aplikasi [7]. Oleh karna itu, jangan sampai melalaikan ancaman siber yang mungkin bisa terjadi tampa disadari.

Dengan banyaknya aplikasi mod yang tersedia diberbagai platfrom. Aplikasi-aplikasi ini menawarkan fitu-fitur unik yang tidak ditemukan di dalam versi resmi. Namun, seperti halnya aplikasi lainya, aplikasi ini rentan terhadap risiko *malware*. Dalam bidang forensic digital, terdapat berbagai metode dan analisis yang dapat dilakukan untuk menangani dan mengatasi ancaman tersebut.

Ada beberapa kerangkan kerja yang tersedia untuk membantu dalam pengujian keamanan aplikasi *android*, seperti *Mobile Security Framework* (MobSF), Mobile Security Framework (MobSF) adalah sebuah *framework open-soucer* yang digunakan untuk pengujian otomatis pada aplikasi seluler (Android, iOS, Windows) yang dapat melakukan pengujian penetrasi, analisis *malware*, dan mendeteksi kerentangan pada aplikasi mobile [8]

Dari uraian yang telah di jelaskan di atas, maka pada penelitian ini penulis ingin menggunakan *mobile security framework* (MOBSF) untuk melakukan analisis statik pada aplikasi modifikasi (MOD) dengan parameter analisis yang digunakan yaitu *dangerous permissions, weak crypto, root detection,* SSI *bypass* dan *domain malware check* dengan harapan penelitian ini dapat mendukung analisis sistem keamanan pada sebuah aplikasi modifikasi (MOD) yang dapat menjadi rujukan untuk menilai tingkat keamanannya.

## 1.2 Rumusan Masalah

1. Bagaimana menerapkan analisis statik keamanan menggunakan mobile security framework (MobSF) pada aplikasi modifikasi berbasis android sehingga didapatkan hasil presentasi tingkat keamananya?

## 1.3 Batasan Masalah

1. Penelitian ini menggunakan *framework* MobSF
2. Peneliti ini menggunakan tiga aplikasi modifikasi.
3. Peneliti ini berfokus menganalis keamanan aplikasi modifikasi
4. Sistem operasi yang digunakan pada penelitian ini adalah kali linux

## 1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitian ini adalah mendapatkan hasil persentase tingkat keamanan pada aplikasi modifikasi berbasis android melalui analisis statik menggunakan *framework* MobSF.

## 1.5 Manfaat Penelitian

1. Diharapkan dengan hasil penelitian ini dapat bermanfaat bagi pengguna *smartphone* agar lebih berhati-hati jika ingin menggunakan aplikasi modifikasi.
2. Mengetauhi tingkat keamanan pada aplikasi-aplikasi modifikasi

## 1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan meliputi:

1. BAB I PENDAHULUAN, berisi Latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan
2. BAB II TINJAUAN PUSTAKA, berisi tetang studi litereatur yang terkait dengan penelitian penulis dan dasat teori yang berkaitan dengan penulisan seperti teori teori yang akan dbahas oleh penulis yang mendukung peneltian

ini.

3. BAB III METODE PENELITIAN, berisi tentang objek penelitian yang diteliti oleh penulis, alur penlitian yang berisikan penjelasan atau langkah Langkah terhadapat objek yang diteliti, dan yang terakhir adalah alat dan bahan apa saja yang akan mendukung pada objek yang diteliti
4. BAB IV HASIL DAN PEMBAHASAN, bab ini berisi hasil dari peneltian yang dilakukan oleh penulis berdasarkan yang ada pada bab 3.
5. BAB V PENUTUP, merangkum hasil dari penelitian yang menjawab semua dari rumusan masalah yang sesuai dengan tujuan penelitian. Dan berikan saran yang akan berguna untuk penetian selanjutnya