BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Teknologi Informasi saat ini berkembang sangat pesat yang salah satunya yaitu penggunaan perangkat *mobile* saat ini. Dalam beberapa tahun terakhir, penggunaan aplikasi *mobile* telah meningkat di berbagai bidang kehidupan masyarakat Indonesia. Berdasarkan Data Report pada laporan Digital 2022: Indonesia, jumlah pengguna internet di Indonesia mencapai 204,7 juta dengan tingkat penetrasi sebanyak 73,7 persen. Angka tersebut meningkat dibandingkan dengan tahun lalu sebesar 1 persen (DataReportal, 2022). Namun, peningkatan jumlah pengguna internet di Indonesia tidak berbanding lurus dengan tingkat keamanan siber yang baik.

Keamanan siber di Indonesia menjadi masalah yang serius dengan kebocoran data yang sering terjadi. Menurut laporan dari *National Cyber Security Index (NCSI)* pada tahun 2022, Indonesia memiliki skor indeks keamanan siber sebesar 38,96 poin dari 100. Penilaian ini maksudnya ialah mengukur kesiapan negara dalam mencegah ancaman siber dan mengelola insiden keamanan siber. Hal tersebut menempatkan Indonesia pada peringkat 83 dari 160 negara di dunia dan peringkat 6 se-ASEAN serta menjadi peringkat ke-3 terendah dibanding negara-negara G20 (National CyberSecurity Index, 2022).

Berdasarkan *Statcounter Global Stats* yaitu sebuah *website* perhitungan pengguna jenis sistem operasi *mobile* yang digunakan di Indonesia saat ini tercatat sebanyak 89,29 persen menggunakan sistem operasi *Android* (Statcounter, 2022). Namun, sebagian pengguna *smartphone* Android tidak mengetahui apakah aplikasi yang mereka pasang telah teruji keamanannya. Pengguna *smartphone* kurang mengetahui bahwa suatu aplikasi dapat menggunakan informasi pribadinya, atau memberikan informasi pribadi pengguna untuk tujuan lain (Akraman et al., 2018).

Hal tersebut menyebabkan munculnya banyak masalah keamanan dan ancaman privasi dari peretas untuk melakukan tindak kejahatan siber dari sebuah aplikasi. Dalam laporan *Vulnerabilities and Threats in Mobile Application* 2019 pada situs *ptsecurity.com*,

menyatakan sebanyak 43 persen aplikasi Android memiliki kerentanan keamanan dengan risiko yang tinggi. Sebagian besar disebabkan karena kelemahan mekanisme keamanan sejak pembuatan aplikasi dan juga pada pemberian hak istimewa yang tidak tepat dimanfaatkan oleh penyerang (Kurniawan & Trianto, 2021).

Meningkatnya kejahatan siber seperti kebocoran data berturut-turut terjadi di Indonesia. Salah satunya yaitu kasus pencurian data pada aplikasi *mobile commerce* di Indonesia, dalam penelitian (Parulian et al., 2021) sebanyak 91 juta data pengguna aplikasi Tokopedia diperjualbelikan oleh peretas secara ilegal di situs *Dark Web*. Data pengguna yang mungkin terekspos yaitu data personal seperti *email*, nama, alamat, tanggal lahir, dan nomor telepon. Pelaku menjual data tersebut seharga $5.000 atau sekitar Rp 74 juta (Fathur, 2020). Hal tersebut tidak terlepas dari kecerobohan dan lemahnya sistem keamanan teknologi *online* sehingga menyebabkan dampak yang sangat buruk bagi pengguna serta pemilik platform. Penyedia aplikasi atau dalam kasus tersebut aplikasi *mobile commerce* pada umumnya sering meminta izin terkait data-data pribadi dari penggunanya. Data- data tersebut digunakan untuk mendukung proses bisnis aplikasinya. Identitas utama pengguna seperti email, alamat, dan nomor telepon bersifat unik dan rentan untuk disalahgunakan (Indarta et al., 2022). Menurut Surfshark, Indonesia memiliki kasus kebocoran akun yang meningkat lebih dari 100% pada tahun 2022 dibandingkan pada tahun 2021. Indonesia menempati tingkat pertama di mana negara yang memiliki peningkatan kasus terhadap kebocoran akun dari tahun 2021 dengan tahun 2022 (Surfshark, 2023).

Ancaman serangan siber tidak terlepas dari kecerobohan dan lemahnya sistem keamanan teknologi *online* sehingga menyebabkan dampak yang sangat buruk bagi pengguna aplikasi maupun pemilik platform (Fathur, 2020) . Menurut Kotler dan Armstrong dalam (Rohmah, 2022), *mobile commerce* merupakan saluran online yang dapat dijangkau sescorang melalui perangkat selular yang digunakan oleh penjual dan pelanggan untuk melakukan transaksi secara *online*. Peningkatan jumlah pengguna *electronic commerce* di Indonesia telah diprediksi akan mencapai 189,6 juta pengguna pada tahun 2024 (Rohmah, 2022). Oleh karena itu, penting bagi semua pihak yang terlibat dalam transaksi secara *online* harus mempertimbangkan ancaman terhadap keamanan informasi dan harus dilengkapi dengan pengetahuan yang relevan dan terkini untuk meminimalkan risikonya (Domenig et al., 2022).

Pembayaran digital merupakan suatu hal yang lumrah dalam perkembangan pembayaran di masa kini, sudah bukan hal asing apabila kita melihat orang mengarahkan handphone ke barcode untuk melakukan transaksi pembayaran. Ada aplikasi mobile fintech yang paling populer yaitu *Ovo*, *Shopeepay*, *Link* Aja, dan Bayarind.

Aplikasi tersebut tentu saja sudah lulus uji dan bisa digunakan dengan aman. Namun seperti kebanyakan sistem yang lain, dalam aplikasi diatas tentu terdapat malware. Dalam dunia forensic terdapat cara dan analisis dalam menangani hal tersebut.

Ada beberapa kerangka kerja atau *framework* yang dapat membantu kita dalam melakukan pengujian keamanan terhadap aplikasi Android. Di antaranya yakni *Mobile Security Framework (MOBSF)* dan *Open Web Application Security Project Mobile Application Security Testing Guide (OWASP MASTG)* yang dapat memberikan hasil analisis keamanan yang jelas untuk menjadi bahan perbaikan keamanan bagi para pengembang aplikasi *Android* (Alanda et al., 2020; Joseph et al., 2021). *Mobile Security Framework* (MobSF) merupakan *framework* yang digunakan sebagai pengujian otomatis terhadap aplikasi seluler (Android, iOS, Windows) berbasis *open-source* yang melakukan pengujian penetrasi, analisis *malware* dan mampu mendeteksi kerentanan yang dapat dieksploitasi oleh penyerang di aplikasi *mobile* (Hanifurohman & Hutagalung, 2020). Menurut penelitian oleh (Negi et al., 2021) melakukan analisis statis menggunakan *framework* MOBSF dengan menghasilkan *True Positive* hingga 97%. Validitas dari hasil analisis tersebut dilakukan pembuktian validitas yang terbukti tidak ada perubahan dari nilai *True Positive* yang dihasilkan. Dalam MobSF mencakup beberapa *framework*, salah satunya ialah *framework Open Web Application Security Project* (OWASP) *Mobile Application Security. Framework* OWASP MASTG membantu MobSF dalam melakukan analisis dan mengkategorikan risiko keamanan *mobile* berdasarkan panduannya. Pada tahun 2018, OWASP membuat panduan tentang pengujian keamanan pada aplikasi *mobile* yang dikemas dalam OWASP MASTG. OWASP MASTG merupakan standar keamanan yang digunakan pada aplikasi *mobile* disertai dengan

panduan pengujian komprehensif yang mencakup proses, teknik, alat, dan studi kasus terkait pelaksanaan uji keamanan aplikasi *mobile*. Menurut penelitian (Yumnun et al., 2020) menyebutkan bahwa OWASP MASTG dapat menemukan kerentanan aplikasi android lebih banyak dari hasil analisis pada *framework* AndroBugs.

Dari hasil penelitian sejenis yang telah dijelaskan di atas, maka penulis ingin melakukan analisis keamanan pada aplikasi Android dengan menggunakan *framework* MOBSF. Hal tersebut diharapkan untuk mendapatkan hasil analisis keamanan yang mendekati sempurna serta dapat melakukan evaluasi ulang setelah adanya perbaikan yang sudah dilakukan terhadap sistem. Penulis mendapatkan temuan urgensi dan melakukan penelitian skripsi ini dengan judul "Statis Analisis Keamanan Aplikasi E-Wallet menggunakan Framework MobsF". Peran *tools MobsF* untuk menganalisis keamanan dan virus malware yang ada di dalam aplikasi tersebut. Penelitian menggunakan *framework MobsF* ini berfungsi untuk menganalisis perizinan dan akses yang dilakukan oleh aplikasi terhadap aplikasi yang ter-*install* di ponsel.

1.2 Rumusan Masalah

1. Bagaimana menganalisis keamanan aplikasi e-wallet berbasis android menggunakan tools framework MobSf sehingga didapatkan hasil persentase tingkat keamanannya?

1.3 Batasan Masalah

1. Sistem operasi yang digunakan pada penelitian ini adalah *Windows 10 Pro*.
2. *Tools* yang digunakan *MOBSF*.
3. Penelitian ini menggunakan metode *static forensic* pada file apk.
4. Penelitian ini berfokus melakukan analisis keamanan pada apk.
5. Penelitian ini menggunakan 4 apk android sebagai uji coba sistem.

1.4 Tujuan Penelitian

Tujuan yang akan dicapai oleh peneliti dalam penelitian ini adalah

mendapatkan hasil persentase tingkat keamanan pada aplikasi android yang dimana dianalisis secara statik menggunakan perangkat lunak MobSF.

1.5 Manfaat Penelitian

1. Membuktikan hasil Analisa keamanan menggunakan sistem *MobSF*.
2. Menambah wawasan dan pemahaman mengenai *cyber system*.
3. Memberikan pemahaman tentang bagaimana melakukan pemeriksaan keamanan jaringan menggunakan sistem *MobSF*.

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 : literature review, tinjauan pustaka, dasar-dasar teori yang digunakan terkait MobSF.
3. BAB III METODE PENELITIAN, berisi : penjelasan tentang tahapan pada penelitian, gambaran umum
4. BAB IV HASIL DAN PEMBAHASAN, berisi : membahas hasil kinerja beberapa tools yang digunakan untuk
5. BAB PENUTUP, berisi : kesimpulan yang diambil berdasarkan hasil dan pembahasan yang telah diuraikan dan menjawab pertanyaan dari rumusan masalah, serta rekomendasi untuk pengembanganan.