

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan sebagai berikut:

1. Penelitian ini menggunakan dua alat utama dalam proses analisis keamanan aplikasi gratis berbasis Android dari Play Store kategori game dan productivity, yaitu Mobile Security Framework (MobSF) dan JADX-GUI, yang masing-masing memiliki fungsi spesifik. MobSF digunakan untuk melakukan analisis statis guna mendeteksi *Security Score*, *Tracker Detection*, dan SSL Certificate Pinning secara otomatis, sedangkan JADX-GUI dimanfaatkan untuk menganalisis source code aplikasi secara manual guna mengidentifikasi izin-izin berbahaya yang diminta oleh aplikasi.
2. Melalui teknik analisis statis dan dinamis menggunakan MobSF dan JADX-GUI, sejumlah informasi keamanan penting berhasil diperoleh dari sepuluh aplikasi yang dianalisis, seperti tingkat keamanan aplikasi (*Security Score*), keberadaan pelacak (*tracker*), peringkat risiko (*Risk Rating*), serta jenis-jenis izin berbahaya yang diminta aplikasi seperti `ACCESS_NETWORK_STATE`, `ACCESS_WIFI_STATE`, `READ_PHONE_STATE`, `WRITE_EXTERNAL_STORAGE`, `ACCESS_COARSE_LOCATION`, `CAMERA`, `CALL_PHONE`, dan `WRITE_SETTINGS`. Temuan ini menunjukkan bahwa mayoritas aplikasi gratis memiliki potensi risiko keamanan data dan privasi yang signifikan.
3. Di antara sepuluh sampel aplikasi yang dianalisis, beberapa aplikasi menunjukkan tingkat implementasi keamanan yang jauh lebih unggul, yang ditandai dengan *Security Score* yang tinggi dan *Risk Rating* yang rendah. Secara spesifik, aplikasi seperti Google Gemini dan Identitas

Kependudukan Digital (IKD) terbukti memiliki kerentanan yang paling rendah, terutama google gemini yang sama sekali tidak memiliki izin berbahaya satupun.

4. Perbedaan mendasar antara kedua analisis ini terletak pada objek dan metode pemeriksaannya. Analisis statis melalui MobSF ibarat melakukan scan otomatis pada aplikasi untuk melihat struktur keamanannya secara keseluruhan seperti skor keamanan dan adanya pelacak tanpa harus menjalankan aplikasi tersebut. Sebaliknya, analisis dinamis yang peneliti lakukan menggunakan JADX-GUI berfungsi sebagai tahap pembuktian manual di sini peneliti meneliti langsung isi *source code* nya untuk memvalidasi apakah izin-izin berbahaya yang terdeteksi benar-benar digunakan secara tidak wajar. Jadi, jika analisis statis memberikan gambaran risiko secara cepat dan otomatis, maka analisis dinamis di skripsi peneliti memberikan kepastian dan detail melalui pengecekan manual yang lebih akurat terhadap perilaku aplikasi.
5. Penggunaan dua pendekatan sekaligus dalam skripsi ini sangat penting karena keduanya saling melengkapi untuk menutupi kelemahan satu sama lain, sehingga hasil penelitian peneliti menjadi jauh lebih akurat dan kredibel. MobSF itu ibarat pemeriksaan awal yang serba otomatis dan cepat untuk memetakan risiko di banyak aplikasi sekaligus, namun yang namanya alat otomatis terkadang hanya melihat "kulit luar" saja dan sering kali salah menebak atau memberikan laporan yang meleset. Di sinilah pendekatan kedua melalui JADX-GUI berperan sangat penting peneliti melakukan investigasi mendalam terhadap *source code* untuk memastikan apakah izin berbahaya yang terdeteksi benar-benar ada dan bagaimana fungsinya dijalankan. Dengan menggabungkan keduanya, peneliti tidak hanya sekadar memberikan angka skor keamanan, tetapi juga memberikan bukti nyata berbasis kode yang membuat kesimpulan skripsi peneliti sulit untuk dibantah secara ilmiah.

5.2 Saran

1. Masyarakat perlu lebih diberikan edukasi mengenai pentingnya memahami izin aplikasi yang diminta sebelum menginstal aplikasi gratis dari Play Store, terutama terkait risiko privasi dan keamanan data pribadi. Disarankan untuk menyelenggarakan pelatihan atau seminar yang berfokus pada penggunaan teknik-teknik dasar analisis keamanan aplikasi mobile seperti membaca izin aplikasi, memahami indikator keamanan, dan melakukan pemeriksaan manual terhadap aplikasi yang akan diinstal guna meningkatkan kesadaran publik terhadap potensi ancaman siber.
2. Diperlukan kebijakan yang lebih ketat dari pihak Google Play Store dan pengembang aplikasi terkait pengelolaan izin aplikasi dan transparansi penggunaan data pribadi pengguna. Penelitian ini menunjukkan bahwa banyak aplikasi gratis meminta izin yang tidak relevan dengan fungsi utama aplikasi, sehingga berpotensi menimbulkan penyalahgunaan data. Oleh karena itu, disarankan agar Google Play Store memperketat proses review aplikasi sebelum publikasi dan pengembang aplikasi meningkatkan transparansi dengan menyediakan kebijakan privasi yang jelas serta mengurangi permintaan izin yang tidak diperlukan. Selain itu, pengembang juga disarankan untuk melakukan pengujian keamanan secara berkala menggunakan *tools* seperti MobSF dan JADX-GUI agar aplikasi yang dirilis lebih aman dan terpercaya bagi pengguna.