JRKT (Jurnal Rekayasa Komputasi Terapan)
Vol 02 No 02 Tahun 2022 e-ISSN : 2776-5873

ANALISIS KEAMANAN INFORMASI *MALWARE* TERHADAP APLIKASI APK DENGAN METODE *STATIC ANALYSIS* MENGGUNAKAN *MOBSF*

Imam Himawan[1], Kevin Septianzah[2], Irawan Setiadi[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer,
Universitas Indraprasta PGRI
Jalan Raya Tengah No 80, Kelurahan Gedong, Pasar Rebo, Jakarta Timur
imamhimawann@gmail.com[1], kevin.septianzah24@gmail.com[2],
irawan.setiadi91@gmail.com[3]

Abstrak

Tujuan Penelitian ini adalah untuk menghasilkan analisis informasi aplikasi file yang berkesktensi APK (*Application Package File*), Aplikasi yang diadopasi adalah aplikasi sistem pakar penceranaan berbasis android, mengingat banyaknya aplikasi yang terproduksi oleh pengelola perusahaan yang bergerak di bidang IT (*Information Technology*) khususnya perangkat lunak, Metode yang digunakan peneliti adalah memanfattkan Aplikasi Mobsf (*Mobile Sequrity Framework*) yang berjenis static, aplikasi Mobsf (*Mobile Sequrity Framework*) cukup banyak digunakan oleh para peneliti mengingat Aplikasi ini berbasis open source, bahasa pemrograman yang digunakan oleh aplikasi ini adalah *powerfull pyton*, Aplikasi Mobsf (*Mobile Sequrity Framework*) itu sendiri bersifat AI (*Artificial Intelligency*). Permasalahan yang dihadapi adalah apakah semua Aplikasi yang sudah terproduksi sudah dinyatakan layak atau tidak khususnya dari sisi keamanan bagi pengguna (*user*) dari segi malware mengingat saat ini banyaknya kasus pencurian data. Aplikasi Mobsf (*Mobile Sequrity Framework*) juga memberikan penilaian lebih tepat karena didasarkan pada nilai kriteria dari bobot preferensi yang sudah di tentukan. Selain itu, peneliti juga melakukan penelitian dengan metode pengumpulan data dengan cara Observasi aplikasi yang akan di jadikan sebagai topic utama penelitian. Analisis Informasi Keamanan Aplikasi Berbasis Android dengan Aplikasi Mobsf telah berhasil menghasilkan informasi keamanan terhadap aplikasi android berjenis APK (*Application Package File*), dari segi malware. sehinga proses penilaian dan penentuan bobot nilai dilakukan secara sistematis. Hasil pengujian fungsional menunjukan bahwa fungsi-fungsi yang terdapat pada aplikasi berjalan dengan baik dan sesuai dengan kebutuhan.

Kata Kunci : Mobsf (*Mobile Sequrity Framework*), Aplikasi Android, *Pyton*.

Abstract

The purpose of this research is to produce an information analysis of file applications with the extension APK (Application Package File), considering the number of applications produced by managers of companies engaged in IT (Information Technology), especially software tools, the method used by researchers is to utilize the dynamic type Mobsf application (*Mobile Sequrity Framework*), the Mobsf application (*Mobile Sequrity Framework*) is quite widely used by researchers considering that This application is based on open source, the programming language used by this application is powerful python, the Mobsf application (*Mobile Sequrity Framework*) itself is AI (Artificial Intelligence). The problem faced is whether all applications that have been produced have been declared feasible or not, especially in terms of security for users, considering that there are currently many cases of data theft. The Mobsf application (*Mobile Sequrity Framework*) also provides a more precise assessment because it is based on the criterion value of a predetermined preference weight. In addition, the author also conducts research with data collection methods by observing the application that will be used as a topic of discussion and making reports. Analysis of Android-Based Application Security Information with the Mobsf Application has succeeded in producing security information for Android applications of the APK (Application Package File) type, especially in the security field. until the process of evaluating and determining the weight of the value is carried out systematically. The results of functional testing show that the functions contained in the application are running well and in accordance with the needs and design. Report generation.

Keywords : Mobsf (*Mobile Sequrity Framework*), Android Application, Python.

PENDAHULUAN

Perkembangan Sistem Informasi, perkembangan teknologi semakin pesat. Pemanfaatan alat *technologi* seperti *computer* dan ponsel lebih banyak digunakan oleh masrayakat, khususnya ke dua alat tersebut mempunyai kekurangan dan kelebihan, baik dari sisi pengguna yang di manfaatkan oleh masyarakat guna mendukung menyelesaikanya pekerjaan [1]. Terdapat berbagai jenis sistem operasi yang digunakan seperti, IOS, Windows Phone, Windows Operating dan Andorid *Smartphone* dengan sistem operasi android merupakan *smartphone* yang paling banyak digunakan saat ini di seluruh dunia, dalam kasus ini peneliti mengangkat topic pembahasan mengenai aplikasi android yang berjenis APK (Application Package File) [2]. Pada aplikasi sistem pakar pecernaan berbasis android, Dengan begitu banyaknya aplikasi *mobile* yang tersedia oleh pengembang perusahaan dibidang perangkat lunak, yang mudah diakses masyarakat melalui aplikasi tersedia seperti IOS Store dan Play Store apakah aplikasi tesebut dapat dinyatakan aman dari segi malware, sebagai contoh aplikasi baterai palsu, aplikasi memori palsu, antivirus palsu, dan aplikasi pihak ketiga lainnya yang banyak tersebar di google [3]. Alasan mengapa aplikasi tersebut termasuk berbahaya karena aplikasi tersusupi malware yang dapat merusak perangkat maupun mencuri data pengguna. *Mobile Security Framework* (MobSF) adalah framework pengujian otomatis bersifat *open source*, yang mampu melakukan analisis statis dan dinamis [4]. Dalam melakukan proses analisis menggunakan metode static analysis di dapat hasil berupa laporan mengenai aplikasi android dengan berjenis file APK (Application Package File). Berdasarkan hal tersebut peneliti akan menganalisis sistem pakar penceranaan berbasis android dengan menggunakan *Mobile Security Framework* (MobSF) untuk dapat mengetahui adanya *malware* berbahaya pada aplikasi android [5]. Dengan menggunakan *Mobile Security Framework* (MobSF) akan dilakukan analisis statis dan dinamis pada beberapa aplikasi android yang ada di Web dan sampel yang sudah mengandung malware, yang kemudian akan dianalisis lebih lanjut mengenai hasilnya yang berupa source code program [6].

.

METODE PENELITIAN

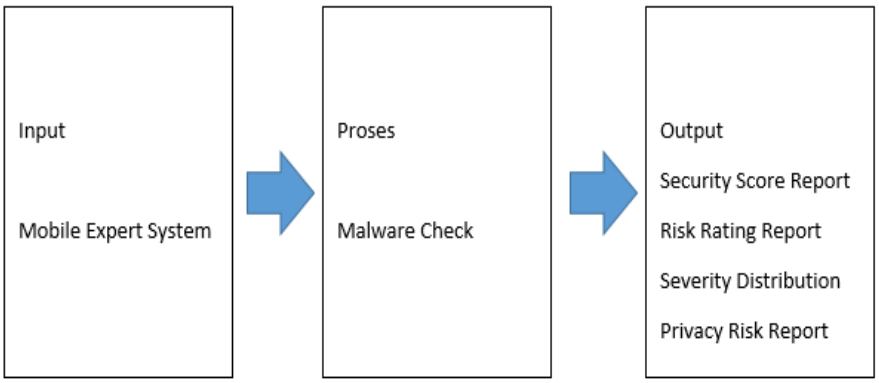
1. Pengamatan (Observation) peneliti mempelajari dan mengamati sistem pakar pecernaan berbasis android Selaras serta keterkaitan antara sub sistem satu dengan yang lainnya dengan meninjau tentang keamanaan sistem.
2. Wawancara (Interview) Wawancara merupakan proses tanya jawab secara langsung dengan pihak terkait. Teknik wawancara ini peneliti gunakan untuk mendapatkan data dan informasi yang berkaitan dengan keamanan.
3. Studi Pustaka Pengumpulan data yang bersumber dari berbagai buku maupun jurnal yang menjadi referensi, pedoman penulisan riset, penelitian, skripsi atau diklat yang menunjang pemecahan permasalahan yang tidak didapatkan dalam penelitian lainnya.

Metode Pengembangan Sistem

Sesuai dengan metode pengembangan yang dilakukan, terdapat kebutuhan sotware yang akan di instalasi sesusi dengan documentasi yang sudah terdapat dalam paket source code aplikasi MobSF, meliputi;

a. Install Git
b. Install Pyton 3.8 – 3.9
c. Install JDK 8+
d. Install Microsoft Visual c++ Build Tools
e. Install OpenSSl (Non-light)
f. Install wkhtmltopdf

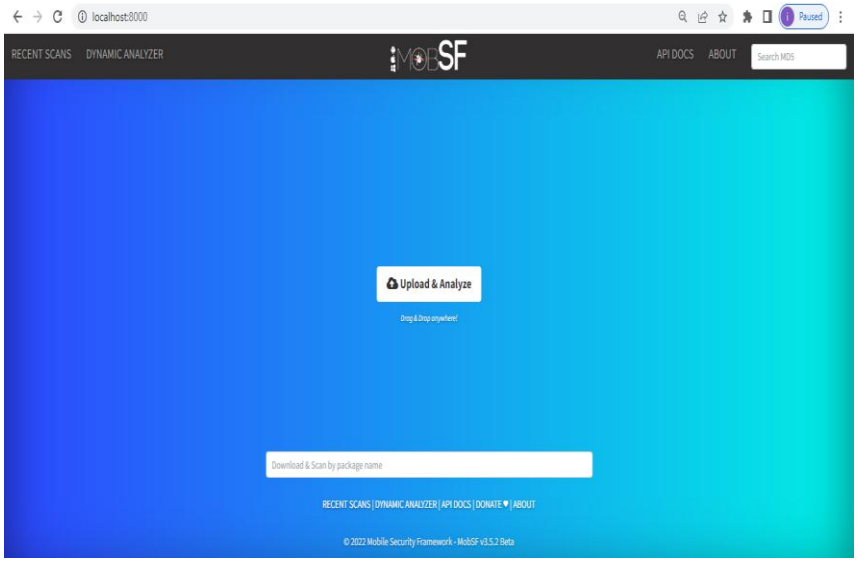
Proses kebutuhan diatas harus terpenuhi untuk melakukan pengujian. Dalam penelitian ini peneliti memanfaatkan salah satu aplikasi opensource yang biasa digunakan untuk melakukan pengukuran terhadap aplikasi mobile sistem pakar pencernaan yaitu MobSF [7].



Gambar 1. Desain Analisis Statis Menggunakan MobSF

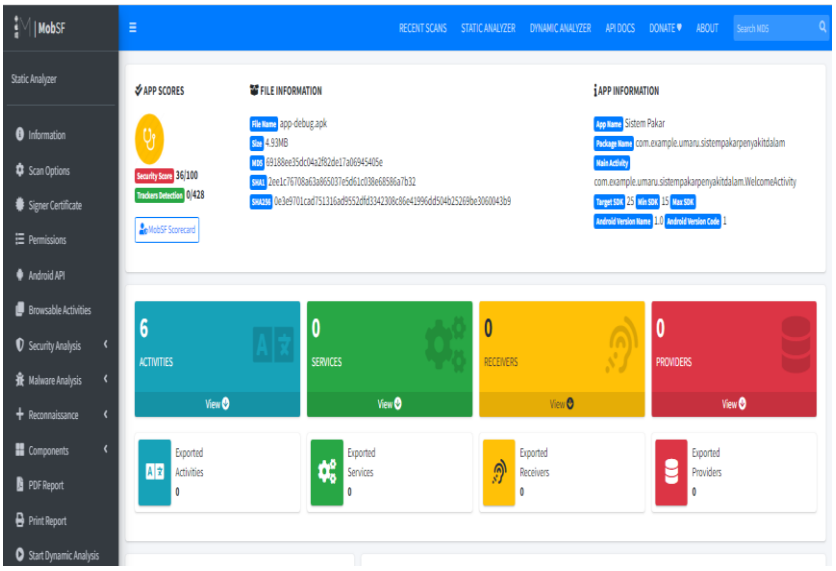
HASIL DAN PEMBAHASAN

Dalam tahapan proses analisis statis menggunakan MobSF, diantaranya file yang dapat digunakan adalah berjenis APK/APKS/XAPK/IPA/ZIPA/APPX. Adapun peneliti melakukan uji coba menggunakan jenis APK. Setelah berhasil instalasi kebutuhan MobSF, metode Implementasi dengan menginput localhost/8000/ seperti pada gambar dibawah ini.



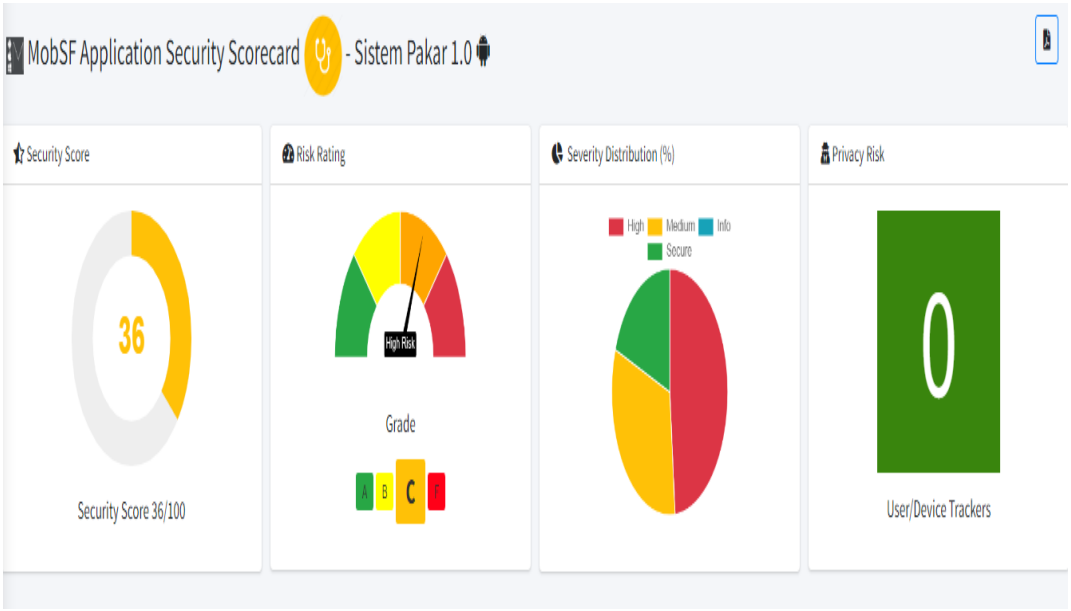
Gambar 2. Halaman Utama MobSF

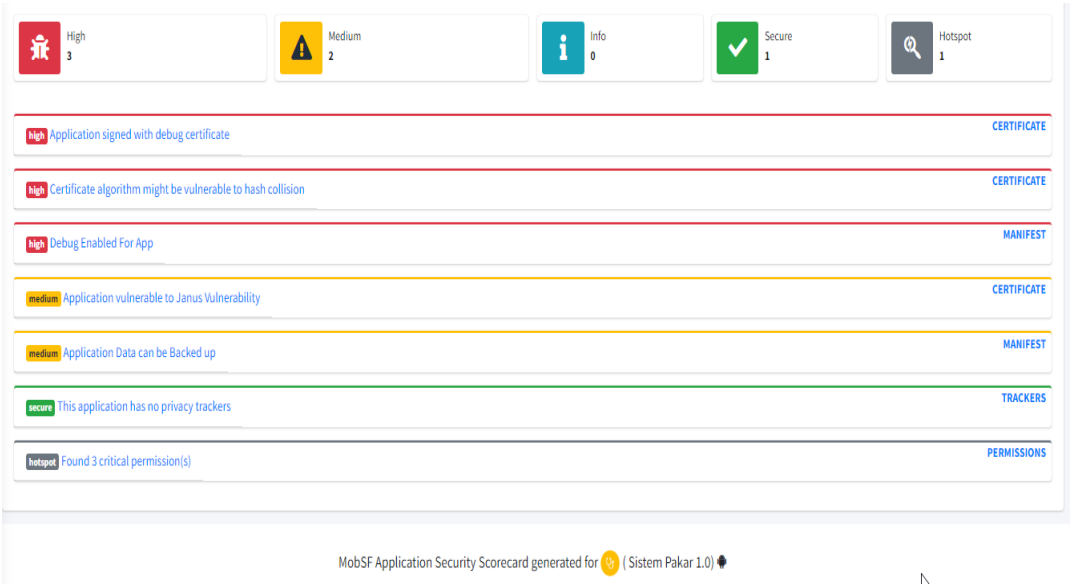
Setelah halaman page MobSf terlihat, maka implementasi prosesnya dengan cara mempersiapkan file APK sistem pakar pencernaan serta mengupload file terserbut ke halaman tersedia. Jika file yang terupload cukup besar maka waktu proses analisanya membutuhkan waktu yang cukup lama, jika sebaliknya maka proses analisis akan berlangsung cepat. Ada pun hasil proses selesai sepereti pada gambar dibawah ini.



Gambar 3. Halaman Hasil Analisa Proses Pada MobSF

Terdapat beberapa informasi seperti terlihat pada menu *navigation* yang dapat di peroleh, diantaranya Menu Information, Scan Options, Signer Certificate, Permission, Android API, Browsable Activities, Security Analysis, Mailware Analysis, Reconnaissance, Components, PDF Report, Print Report. Selanjutnya menu yang disebutkan dapat dicetak atau dilihat secara detail dengan memanfaatkan menu pdf report. Serta mengenai analysis juga dapat di kembangkan menjadi metode analysis dinamic integrasikan terhadap menu yang tersedia seperti menu Start Dynamic Analysis sehingga dapat diperuntuk peneliti terhadap pengujian yang dibutuhkan, seperti terlihat pada gambar dibawah ini mengenai laporan detail MobSF application seperti terlihat pada gambar dibawah ini.





Gambar 4. Detail Report MobSF Sistem Pakar

SIMPULAN

Proses analisis yang dilakukan terhadap aplikasi sistem pakar pencernaan android menunjukan bahwa tingkat keamanan masih relatif sama adanya celah-celah kemanan yang ditemukan dapat menjadi security awareness untuk pengguna aplikasi tersebut yang jumlahnya cukup banyak di Indonesia, dan pengembangan aplikasi MobSF dapat digunakan untuk pengukuran terhadap aplikasi lainya, adapun penulis selanjutnya akan mengembangkan pengukuran terhadap comparasi dari beberapa aplikasi, peneliti hanya menggunakan analisis statis yang merupakan tahapan awal dalam analisis keamanan sehingga perlu dilanjutkan menggunakan analisis dinamis untuk mendapatkan hasil yang lebih lengkap dari analisis keamanan yang dilakukan dan perlu dibandingkan dengan metode analisis lainnya seperti Application Security Verification Standard untuk pengujian komprehensif yang mencakup proses, teknik, dan alat yang digunakan untuk keamanan aplikasi seluler. Melakukan pemantauan dan merekam aktivitas yang dilakukan pengguna smartphone android. Sedangkan malware memiliki karakteristik dalam mencuri data dengan menampilkan halaman informasi palsu. Kedua malware memiliki karakteristik yang sama, yaitu data akan dikirimkan ke server C&C(Command & Control Server). Upaya pencegahan yang dapat dilakukan untuk menghindari infeksi malware pada smartphone android yaitu dengan memastikan hanya memasang aplikasi android dari sumber terpercaya seperti Google Play Store, dan hiraukan SMS yang berisi tautan mencurigakan, serta pastikan selalu update firmware sistem android pada smartphone.

DAFTAR PUSTAKA

[1] R. Umar, I. Riadi, and E. Handoyo, “Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI),” *J. Sist. Inf. Bisnis*, vol. 9, no. 1, p. 47, 2019, doi: 10.21456/vol9iss1pp47-54.

[2] S. Sinambela, A. R. Pangestu, R. Feriyanto, and F. I. Komputer, “Analisis Aplikasi Malware pada Android dengan Metode Statik,” *J. Ilmu Komput. dan Inform.*, vol. 3, no. 2, pp. 2621–4970, 2020.

[3] S. D. S. K. Virgiawan A. Manoppo, Arie S. M. Lumenta, “Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi,” *J. Tek. Elektro Dan Komput.*, vol. 9, no. 3, pp. 181–188, 2020.

[4] A. Kartono, A. Sularsa, and S. J. I. Ismail, “Membangun Sistem Pengujian Keamanan Aplikasi Android Menggunakan Mobsf,” *e-Proceeding Appl. Sci.*, vol. 5, no. 1, pp. 146–151, 2019.

[5] A. S. Rusdi, N. Widiyasono, and H. Sulastri, “Analisis Infeksi Malware Pada Perangkat Android Dengan Metode Hybrid Analysis,” *Univ. Puter. Batam*, vol. 46115, no. 24, p. 107, 2019.

[6] B. Santoso, M. A. Ghofur, and J. Kuswanto, "Analysis of WhatsApp Mod User Awareness Information Security with Static Analysis Methods and Quantitative Methods," *Pros. Semin. Nas. Sains Teknol. dan Inov. Indones.*, vol. 3, no. November, pp. 213–222, 2021, doi: 10.54706/senastindo.v3.2021.128.

[7] Y. Dwi *et al.*, "Analisis Malware Menggunakan Metode Analisis Statis dan Dinamis untuk Pembuatan IOC Berdasarkan STIX Versi 2.1," *J. Info Kripto*, vol. 15, no. 3, pp. 105–111, 2017.