

DAFTAR PUSTAKA

- [1] “Sejarah Android|S1 Sistem Informasi S.Kom.” Diakses: 21 Juli 2023. [Daring]. Tersedia pada: <https://sistem-informasi-s1.stekom.ac.id/informasi/baca/Sejarah-Android/fc5ab04944f17da73bb33362fb70110494afb251>
- [2] “Apa itu Android? Berikut Pengertian, Kelebihan, serta Kekurangannya! - Bitlabs Blog.” Diakses: 21 Juli 2023. [Daring]. Tersedia pada: <https://bitlabs.id/blog/android-adalah/>
- [3] “+65 Statistik Malware untuk tahun 2024.” Diakses: 1 Juni 2024. [Daring]. Tersedia pada: <https://www.stationx.net/malware-statistics/>
- [4] “√Pengertian Metasploit, fungsi dan cara kerjanya lengkap - FHXPloit.” Diakses: 21 Juli 2023. [Daring]. Tersedia pada: <https://fhxexploit.com/pengertian-metasploit-fungsi-dan-cara-kerjanya-lengkap/>
- [5] “Apa itu Exploit? Penjelasan, Jenis dan Pencegahannya • Widya Security.” Diakses: 1 Juni 2024. [Daring]. Tersedia pada: <https://widyasecurity.com/2024/01/09/apa-itu-exploit-penjelasan-jenis-dan-pencegahannya/>
- [6] R. Sajeev, S. Joseph, S. Biju, dan M. Manoj, “A Collaborative Approach for Android Hacking by Integrating Evil-Droid, Ngrok, Armitage and its Countermeasures”, Diakses: 21 Juli 2023. [Daring]. Tersedia pada: <https://github.com/M4sc3r4no/Evil-Droid.git>
- [7] “Analisis Malware Pada Sistem Operasi Android Menggunakan Permission-based.” Diakses: 1 Juni 2024. [Daring]. Tersedia pada: <https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/10644/10502>
- [8] I. Putu, A. Eka Pratama, dan R. R. Daniswara, “Pengujian dan Analisa Reverse Engineering Pada Platform Android (Studi Kasus: Tebak_Gambar.apk),” vol. 8.
- [9] M. Hazri, “Analisis Malware PlasmaRAT dengan Metode Reverse Engineering,” *JURTI*, vol. 4, no. 2, 2020.
- [10] “Analisis Malware Android Menggunakan Metode Reverse Engineering.” Diakses: 4 Juni 2024. [Daring]. Tersedia pada: <https://ejournal.umm.ac.id/index.php/repositor/article/view/31842/13797>
- [11] “Analisis Malware Ahmyth pada Platform Android Menggunakan Metode Reverse Engineering.” Diakses: 4 Juni 2024. [Daring]. Tersedia pada: <https://ojs.unpkediri.ac.id/index.php/gj/article/view/17749/2910>

- [12] “Analisis Malicious Software Trojan Downloader Pada Android Menggunakan Teknik Reverse Engineering (Studi Kasus: Kamus Kesehatan v2.apk).” Diakses: 1 Juni 2024. [Daring]. Tersedia pada: <https://ejurnal.seminar-id.com/index.php/bits/article/view/1515/1089>
- [13] “ANALISIS MALWARE ANDROID MENGGUNAKAN METODE REVERSE ENGINEERING.” Diakses: 4 Juni 2024. [Daring]. Tersedia pada: <https://jurnal.itbsemarang.ac.id/index.php/JIKMA/article/view/169/183>
- [14] “√ Urutan Versi Android dari Awal Hingga Android 14.” Diakses: 10 Juni 2024. [Daring]. Tersedia pada: <https://www.bhinneka.com/blog/urutan-android/>
- [15] “Apa Itu Malware: Pengertian, Jenis, serta Cara Mengatasinya.” Diakses: 21 Juli 2023. [Daring]. Tersedia pada: <https://cloudmatika.co.id/blog-detail/apa-itu-malware>
- [16] R. Dwiananda, L. Putra, dan I. Mardianto, “JEPIN (Jurnal Edukasi dan Penelitian Informatika) Exploitation with Reverse_tcp method on Android Device Using Metasploit,” *Universitas Trisakti Jl. Letjen S. Parman*, no. 1, hlm. 11440, 2019.
- [17] “What is Meterpreter ? - Security Wiki.” Diakses: 3 Juni 2024. [Daring]. Tersedia pada: <https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/>
- [18] “jadX : Android Reverse Engineering dari Android Dex ke File Java - alfach.com.” Diakses: 4 Juni 2024. [Daring]. Tersedia pada: <https://alfach.com/2020/11/05/jadx-android-reverse-engineering-dari-android-dex-ke-file-java/>