DAFTAR PUSTAKA

[1] R. D. Putra and I. Mardianto, “Exploitation with Reverse_tcp Method on Android Device using Metasploit,” *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 106, 2019, doi: 10.26418/jp.v5i1.26893.

[2] StatCounter, “Mobile Android Version Market Share in Indonesia - March 2024.”

[3] R. Akraman, C. Candiwan, and Y. Priyadi, “Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia,” *J. Sist. Inf. Bisnis*, vol. 8, no. 2, p. 115, 2018, doi: 10.21456/vol8iss2pp115-122.

[4] A. KIVVA, “IT threat evolution in Q3 2023. Mobile statistics.”

[5] T. P. Setia, N. Widiyasono, and A. P. Aldya, “Analysis Malware Flawed Ammyy RAT Dengan Metode Reverse Engineering,” *J. Inform. J. Pengemb. IT*, vol. 3, p. 371, 2018.

[6] P. P. ROMADHON, “Analisis Pendeteksian dan Pencegahan Serangan Backdoor Pada Layanan Server,” no. 12, p. 102, 2014.

[7] F. Akbar, Hanafi, and A. Fauziah, “Evaluasi Serangan Exploit Terhadap Sistem Operasi Android Pada Jaringan Internet,” *J. TEKTRO*, vol. 5, no. 2, pp. 144–152, 2021, [Online]. Available: http://e-jurnal.pnl.ac.id/TEKTRO/article/view/3094

[8] A. N. Iman, M. T. Avon Budiyono, S.T., and M. T. Ahmad Almaarif, S.Kom., “Analisis Malware Pada Sistem Operasi Android Menggunakan Permission-Based Malware Analysis in Android Operation System Using Permission-Based,” *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 6, no. Mi, pp. 5–24, 1967.

[9] M. Santonario, Frenvol De. Moises, “Analisis Malware Android

Menggunakan Reverse Engineering," vol. 1, no. 2, pp. 41–53, 2023.

[10] N. Widiyasono, H. Mubarok, and A. Fatwa MF, "Analisis Malware Ahmyth pada Platform Android Menggunakan Metode Reverse Engineering," *Gener. J.*, vol. 6, no. 2, pp. 73–82, 2022, doi: 10.29407/gj.v6i2.17749.

[11] T. Pajar Setia, N. Widiyasono, and A. Putra Aldya, "Analysis Malware Flawed Ammyy RAT Dengan Metode Reverse Engineering," *J. Inform. J. Pengemb. IT*, vol. 3, no. 3, pp. 371–379, 2018, doi: 10.30591/jpit.v3i3.1019.

[12] M. Hazri, "Analisis Malware PlasmaRAT dengan Metode Reverse Engineering," *J. Rekayasa Teknol. Inf.*, vol. 4, no. 2, p. 192, 2020, doi: 10.30872/jurti.v4i2.4131.

[13] B. A. Saputro, L. I. Alfitra, and R. B. Oktaviaji, "Analisis Malware Android Menggunakan Metode Reverse Engineering," *J. Repos.*, vol. 2, no. 10, pp. 1331–1337, 2020, doi: 10.22219/repositor.v2i10.1061.

[14] S. Megira, A. R. Pangesti, and F. W. Wibowo, "Malware Analysis and Detection Using Reverse Engineering Technique," *J. Phys. Conf. Ser.*, vol. 1140, no. 1, 2018, doi: 10.1088/1742-6596/1140/1/012042.

[15] Y. P. Heru Ari Nugroho, "Penggunaan Teknik Reverse Engineering Pada Malware Analysis Untuk Identifikasi Serangan Malware," in *KNSI*, 2014.

[16] C. Le Roy, "sensepost /kwetza." [Online]. Available: https://github.com/sensepost/kwetza

[17] T. P. Setia, A. P. Aldya, and N. Widiyasono, "Reverse Engineering untuk Analisis Malware Remote Access Trojan," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 40, 2019, doi: 10.26418/jp.v5i1.28214.

[18] A. Abraham, "MobSF /Mobile-Security-Framework-MobSF." [Online]. Available: https://github.com/MobSF/Mobile-Security-Framework-MobSF

[19] Danar Cahyo Prakoso, "Investigasi Forensik RAM untuk Mendeteksi Serangan Exploit Framework Metasploit," *Univ. Islam Indones.*, pp. 7–14, 2019, [Online]. Available: https://dspace.uii.ac.id/bitstream/handle/123456789/17442/01 cover.pdf?sequence=2&isAllowed=yhttps://dspace.uii.ac.id/bitstream/handle/123456789/17442/05.2 bab 2.pdf?sequence=6&isAllowed=y

[20] L. Bruno, "Sistem Monitoring Dan Pencegahan Dengan Rules Penanganan Spesifik Serangan Scanning, Dos, Exploit Pada Komputer Server Menggunakan Suricata," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2019.

[21] D. Teori *et al.*, "Actual Exploit," no. 4, pp. 1–10.

[22] Ferdiansyah, "Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware," *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018, [Online]. Available: http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

[23] I. M. Rizky Dwiananda Lukita Putra, "Exploitation with Reverse_tcp method on Android Device Using Metasploit," *JEPIN (Jurnal Edukasi dan Penelit. Inform.*, vol. 5, p. 107, 2019.

[24] M. R. Kurian, E. Thoppil, S. Sibichan, and V. Viswanath, "Android Device Hacking: TheFatRat and Armitage," *Natl. Conf. Emerg. Comput. Appl.*, vol. 2, no. 1, 2020.

[25] F. L. Nafila and Y. Prayudi, "Analisis Digital Artifak Aplikasi Signal Messenger Pada Sistem Operasi Android Menggunakan metode NIST," *J. Sains Komput. Inform.*, vol. 6, no. 1, pp. 532–543, 2022, [Online]. Available: http://ejurnal.tunasbangsa.ac.id/index.php/jsakti/article/view/466

[26] M. A. Rahmadani, M. F. Rizal, T. Gunamawan, F. I. Terapan, U. Telkom, and H. Wireless, "Implementasi Hacking Wireless dengan Kali Linux

Menggunakan Kali Nethunter," *e-Proceedings Appl. Sci.*, vol. 3, no. 3, pp. 1767–1774, 2017.

[27] A. Setiyadi, "Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Pengguna dalam Mengakses Internet Seminar Nasional Komputer dan Informatika," *Implementasi Modul Netw. MITM Pada Websploit sebagai Monit. Aktifitas Pengguna dalam Mengakses Internet Semin. Nas. Komput. dan Inform.*, vol. 2017, pp. 113–120, 2017, [Online]. Available: https://ojs.unikom.ac.id/index.php/senaski/article/view/934

[28] D. Hindarto, "Perbandingan Kinerja Akurasi Klasifikasi K-NN, NB dan DT pada APK Android," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 1, pp. 486–503, 2022, doi: 10.35957/jatisi.v9i1.1542.