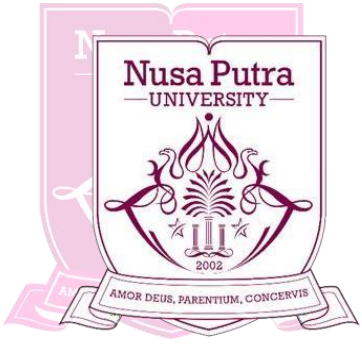
ANALISIS KEAMANAN DAN EKSPLOITASI KERNEL *ANDROID* 13 MENGGUNAKAN *METASPLOIT REVERSE TCP*

SKRIPSI

SALMAN ALHIDAMKARA
20200040122



PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN

SUKABUMI

JUNI 2024

ANALISIS KEAMANAN DAN EKSPLOITASI KERNEL *ANDROID* 13 MENGGUNAKAN *METASPLOIT REVERSE TCP*

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat Dalam Menempuh

Gelar Sarjana Teknik Informatika

Salman Alhidamkara
20200040122

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK, KOMPUTER DAN DESAIN

SUKABUMI

JUNI 2024

PERNYATAAN PENULIS

JUDUL : ANALISIS KEAMANAN DAN EKSPLOITASI KERNEL ANDROID 13 MENGGUNAKAN *METASPLOIT REVERSE TCP*
NAMA : SALMAN ALHIDAMKARA
NIM : 20200040122

"Saya menyatakan dan bertanggungjawab dengan sebenarnya bahwa Skripsi ini adalah hasil karya saya sendiri kecuali cuplikan dan ringkasan yang masing-masing telah saya jelaskan sumbernya. Jika pada waktu selanjutnya ada pihak lain yang mengklaim bahwa Skripsi ini sebagai karyanya, yang disertai dengan bukti-bukti yang cukup, maka kami bersedia untuk dibatalkan gelar Sarjana Teknik Informatika saya beserta segala hak dan kewajiban yang melekat pada gelar tersebut".

Sukabumi, 25 Juni 2024

Salman Alhidamkara
Penulis

PENGESAHAN SKRIPSI

JUDUL : ANALISIS KEAMANAN DAN EKSPLOITASI KERNEL *ANDROID* 13 MENGGUNAKAN *METASPLOIT REVERSE TCP*
NAMA : SALMAN ALHIDAMKARA
NIM : 20200040122

Skripsi ini telah diujikan dan dipertahankan di depan Dewan Penguji pada Sidang Skripsi tanggal 21 Juni 2024. Menurut pandangan kami, Skripsi ini memadai dari segi kualitas untuk tujuan penganugerahan gelar Sarjana Teknik Komputer (S.Kom)

Sukabumi, 21 Juni 2024

Pembimbing I

Ir. Somantri, S.T, M.Kom
NIDN. 0419128801

Pembimbing II

Ivana Lucia Kharisma, M.Kom
NIDN. 0429038002

Ketua Penguji

Hermanto, S.T, M.Kom
NIDN. 0402027401

Ketua Program Studi

Ir. Somantri, S.T, M.Kom
NIDN. 0419128801

PLH Dekan Fakultas Teknik Komputer dan Desain

Ir. Paikun, ST., MT., IPM., ASEAN Eng
NIDN. 0402037401

ABSTRAK

Perkembangan teknologi informasi, terutama di bidang *mobile*, telah mengubah cara kita berinteraksi dengan perangkat secara substansial. *Android*, sebagai sistem operasi *mobile* yang paling dominan digunakan di seluruh dunia, menarik perhatian yang signifikan terhadap aspek keamanannya. Meskipun telah ada peningkatan dalam keamanan perangkat *Android*, upaya eksploitasi terus dilakukan oleh para peneliti keamanan dan peretas dengan menggunakan berbagai metode, termasuk eksploitasi melalui *Reverse_TCP* dengan alat bantu seperti *Metasploit*. Penelitian ini bertujuan untuk menganalisis keamanan perangkat *Android* 13 menggunakan metode *Reverse_TCP* melalui *Metasploit*. Metode yang digunakan melibatkan eksploitasi dengan mengirim aplikasi *backdoor*, membuka sesi *Meterpreter*, dan mencuri data seperti SMS dan log panggilan. Hasil penelitian menunjukkan bahwa *Google Play Protect* mendeteksi aplikasi berbahaya, namun aplikasi tersebut masih dapat diinstal dan dijalankan, menunjukkan kelemahan dalam sistem deteksi keamanan. Eksploitasi *Reverse_TCP* dapat menyebabkan akses tidak sah ke data pribadi dan kontrol penuh atas perangkat, menimbulkan risiko signifikan bagi pengguna. Selain itu, hasilnya juga menunjukkan bahwa data sensitif seperti *SMS, log* panggilan, dan lokasi dapat berhasil diambil oleh penyerang melalui sesi *Meterpreter*, menyoroti celah keamanan yang kritis. Langkah pencegahan yang diusulkan termasuk penggunaan *Mobile Security Framework (MobSF)*, pengaktifan *Google Play Protect*, dan menonaktifkan izin aplikasi yang tidak diperlukan. Penelitian ini menyarankan penelitian lebih lanjut untuk mengatasi keterbatasan dan mengeksplorasi lebih dalam aspek keamanan *Android*.

Kata Kunci : Analisis keamanan, *Android* 13, Eksploitasi, *Metasploit*, *Reverse TCP*

ABSTRACT

The development of information technology, especially in the mobile sector, has substantially changed the way we interact with devices. Android, as the most dominantly used mobile operating system worldwide, attracts significant attention to its security aspects. Despite improvements in Android device security, exploitation efforts continue to be carried out by security researchers and hackers using various methods, including *exploitation through Reverse_TCP with tools such as Metasploit. This study aims to analyze the security of Android 13 devices using the Reverse_TCP method through Metasploit. The method used involves exploitation by sending a backdoor application, opening a Meterpreter session, and stealing data such as SMS and call logs. The research results show that Google Play Protect detects malicious applications; however, these applications can still be installed and run, indicating weaknesses in the security detection system. Reverse_TCP exploitation can lead to unauthorized access to personal data and full control over the device, posing significant risks to users. Additionally, the results also show that sensitive data such as SMS, call logs, and location can be successfully retrieved by attackers through the Meterpreter session, highlighting critical security gaps.Proposed preventive measures include the use of the Mobile Security Framework (MobSF), enabling Google Play Protect, and disabling unnecessary app permissions. This study suggests further research to address limitations and explore deeper aspects of Android security.*

***Keywords**: Android 13, Exploitation, Metasploit, Reverse TCP, Security Analysis*

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT, berkat rahmat dan karunia- Nya penulis dapat menyelesaikan penulisan skripsi dengan judul "ANALISIS KEAMANAN DAN EKSPLOITASI KERNEL *ANDROID* 13 MENGGUNAKAN *METASPLOIT REVERSE TCP*". Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik di Program Studi Teknik Informatika Universitas Nusa Putra.

Dalam proses penyelesaian Skripsi ini, penulis banyak mendapatkan bimbingan, dorongan, dukungan dan bantuan baik secara moril maupun materiil dari berbagai pihak, oleh sebab itu peneliti ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Kurniawan, ST., M.Si., MM selaku Rektor Universitas Nusa Putra Sukabumi
2. Dekan Fakultas Teknik, Komputer dan Desain Bapak Ir. Paikun, ST., MT., IPM., Asean Eng
3. Ketua Program Studi Teknik Informatika Universitas Nusa Putra Sukabumi Bapak Ir. Somantri, S.T, M.Kom
4. Dosen pembimbing I Bapak Ir. Somantri, S.T, M.Kom dan dosen pembimbing II Ibu Ivana Lucia Kharisma, M.Kom yang telah memberikan dorongan, saran dan bimbingan sehingga skripsi ini dapat selesai dengan baik.
5. Para Dosen Program Studi Teknik Informatika Universitas Nusa Putra Sukabumi yang telah memberikan ilmu yang bermanfaat bagi kami selama menempuh pendidikan di Program Studi Teknik Sipil
6. Orang tua dan keluarga kami yang tidak henti-hentinya memberikan doa dan juga dukungan yang sangat membantu untuk menyelesaikan skripsi ini
7. Seluruh teman-teman seperjuangan kami yang telah memberikan semangat dari awal sampai akhir

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, oleh karena itu kritik dan saran yang membangun dari berbagai pihak sangat kami harapkan demi perbaikan.

Sukabum, 25 Juni 2024

Salman Alhidamkara

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI

SKRIPSI UNTUK KEPENTINGAN AKADEMIK

Sebagai civitas academica Universitas Nusa Putra, kami yang bertanda tangan di bawah ini:

Nama	: SALMAN ALHIDAMKARA
NIM	: 20200040122
Program Studi	: TEKNIK INFORMATIKA
Jenis Karya	: SKRIPSI

Demi perkembangan ilmu pengetahuan, dengan ini kami menyetujui untuk memberikan kepada Universitas Nusa Putra ***Hak Bebas Royalti Non eksekutif (Non Exlusive Royalty-Free Right)*** atas karya ilmiah kami yang berjudul:

"ANALISIS KEAMANAN DAN EKSPLOITASI KERNEL *ANDROID* 13 MENGGUNAKAN *METASPLOIT REVERSE TCP*"

Beserta perangkat yang ada (jika diperlukan). Dengan hak bebas *royalty Non-Ekslusif* ini Universitas Nusa Putra berhak menyimpan, mengalih media/format, mengolah dalam bentuk pangkalan data (*data base*), merawat dan mempublikasikan skripsi kami selama tetap mencantumkan nama kami sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini kami buat dengan sebenarnya.

Dibuat di: Sukabumi

Pada Tanggal: 25 Juni 2024

Yang Menyatakan

Salman Alhidamkara

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Dalam era digital yang terus berkembang, keamanan sistem operasi mobile menjadi semakin penting, khususnya dalam konteks *Android* yang merupakan sistem operasi yang paling banyak digunakan di seluruh dunia [1],[2]. *Kernel Android*, sebagai inti dari sistem operasi ini, memegang peranan krusial dalam mengelola sumber daya perangkat keras dan menyediakan antarmuka bagi aplikasi yang berjalan di atasnya [3]. Namun, dengan kemajuan teknologi juga muncul tantangan baru dalam hal keamanan [4]. Keberadaan kerentanan dalam *kernel Android* menjadi target utama bagi penyerang yang mencari celah untuk mengeksploitasi perangkat tersebut [5]. Dalam menghadapi kompleksitas dan luasnya penggunaan *Android*, diperlukan upaya yang sistematis untuk menganalisis keamanan *kernel Android versi* terbaru, dalam hal ini adalah *versi* 13 [6]. Dalam konteks penelitian ini, pemilihan *Kernel Android* 13 sebagai fokus utama adalah karena perbaikan signifikan dalam keamanan dibandingkan dengan versi sebelumnya. *Android* 13 menawarkan peningkatan keamanan yang lebih baik dalam mengelola sumber daya perangkat keras dan melindungi privasi pengguna. Dengan memilih *versi* terbaru ini, penelitian dapat mengungkapkan sejauh mana kemajuan keamanan yang telah dicapai dan mengidentifikasi potensi celah yang masih perlu ditangani.

Salah satu pendekatan yang umum digunakan dalam analisis keamanan sistem adalah penggunaan alat bantu seperti *Metasploit*, yang merupakan salah satu *Framework* pengujian penetrasi yang paling populer dan kuat [7]. Modul *Reverse_TCP* dalam *Metasploit* memungkinkan peneliti keamanan untuk membangun koneksi terbalik ke perangkat target, membuka peluang untuk mengeksplorasi potensi kerentanan dan rentang serangan yang mungkin [8].

Walaupun *kernel Android* 13 telah menerima perbaikan keamanan dari *versi* sebelumnya, namun demikian, tidak dapat dipungkiri bahwa masih

terdapat risiko keamanan yang perlu dipahami dan ditangani [9]. Keberadaan celah keamanan dalam *kernel Android* 13 dapat dimanfaatkan oleh penyerang untuk mendapatkan akses yang tidak sah ke perangkat pengguna, yang pada gilirannya dapat menyebabkan kerugian data pribadi atau bahkan kerugian finansial [10].

Oleh karena itu, perlu dilakukan analisis yang mendalam terhadap keamanan *kernel Android* 13 menggunakan *Metasploit Reverse_TCP* [11]. Dengan melakukan analisis ini, diharapkan dapat diidentifikasi dan dipahami kerentanan yang mungkin ada dalam *kernel Android* 13, sehingga langkah-langkah pencegahan dan perbaikan keamanan yang tepat dapat dirancang dan diimplementasikan [12]. Meskipun *Kernel Android* 13 telah mengalami perbaikan yang signifikan dalam keamanan, beberapa celah keamanan masih dapat dieksplorasi. Misalnya, celah-celah tersebut mungkin terletak pada manajemen hak akses yang tidak optimal atau kekurangan dalam penanganan *input* yang tidak sah, yang dapat dieksploitasi oleh penyerang untuk mendapatkan akses tidak sah ke perangkat.

Pentingnya analisis keamanan *kernel Android* 13 ini tidak hanya berkaitan dengan pengembangan sistem operasi itu sendiri, tetapi juga melibatkan privasi dan keamanan pengguna [1]. Dengan meningkatnya ancaman *cyber* yang ditujukan kepada perangkat *mobile*, langkah-langkah proaktif dalam meningkatkan keamanan *kernel Android* 13 akan memberikan manfaat yang signifikan bagi pengguna secara keseluruhan.

Dalam konteks pengembangan keamanan *cyber*, penelitian ini juga dapat memberikan panduan yang berguna bagi pengembang dan peneliti keamanan untuk mengembangkan strategi yang lebih efektif dalam mengatasi ancaman siber terhadap sistem operasi *Android* [13]. Dengan demikian, analisis keamanan dan eksploitasi *kernel Android* 13 menggunakan *Metasploit Reverse_TCP* menjadi topik yang relevan dan perlu untuk diteliti lebih lanjut guna meningkatkan keamanan *cyber* secara keseluruhan [14].

Dalam memilih judul "Analisis Keamanan dan Eksploitasi *Kernel Android* 13 Menggunakan *Metasploit Reverse_TCP*", relevansi dan urgensi

topik tersebut sangat jelas. Mengingat pentingnya keamanan sistem operasi *mobile*, khususnya *Android* yang mendominasi pasar global, fokus pada analisis keamanan *kernel Android versi* terbaru, yaitu *versi* 13, menjadi langkah yang tepat. *Metasploit Reverse_TCP* dipilih sebagai alat analisis karena popularitasnya dan kemampuannya dalam mendeteksi kerentanan serta rentang serangan yang mungkin terjadi. Dengan demikian, judul ini mencerminkan kebutuhan akan penelitian yang sistematis dan mendalam untuk menghadapi ancaman *cyber* yang semakin kompleks terhadap sistem operasi *Android*, sambil memberikan kontribusi pada pengembangan strategi keamanan *cyber* yang lebih efektif secara keseluruhan.

1.2 Rumusan Masalah

Dalam konteks analisis keamanan perangkat *Android* dengan metode *Reverse_TCP*, beberapa permasalahan yang akan diidentifikasi meliputi:

1. Bagaimana proses analisis dan eksploitasi dilakukan dengan menggunakan *Metasploit Reverse TCP* pada perangkat *Android* 13?
2. Apa dampak dan potensi risiko yang mungkin timbul akibat eksploitasi menggunakan metode *Reverse_TCP* pada perangkat *Android* 13?
3. Apa saja langkah-langkah pencegahan yang dapat dirancang dan diimplementasikan untuk meningkatkan keamanan *kernel Android* 13?

1.3 Batasan Masalah

Penelitian ini memiliki batasan pada:

1. Jenis perangkat *Android* yang akan diuji coba adalah *Android* 13 *Xiaomi Redmi 12*, *Infinix Smart 8* dan *Samsung M12*.
2. Metode yang digunakan untuk mengeksploitasi *Android* 13 adalah Metode *Reverse_tcp* dengan menggunakan *Metasploit Framework*
3. *Attacker* dan target berada pada jaringan intranet.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk:

1. Mengeksplorasi proses eksploitasi keamanan menggunakan *Metasploit* pada perangkat *Android.*
2. Mengidentifikasi dampak dan potensi risiko yang mungkin timbul akibat eksploitasi menggunakan metode *Reverse_TCP* pada perangkat *Android.*
3. Merancang langkah-langkah pencegahan yang efektif untuk meningkatkan keamanan *kernel Android* 13.

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam pemahaman lebih lanjut tentang kerentanan keamanan perangkat *Android* dan metode *Reverse_TCP*. Manfaatnya antara lain:

1. Sebagai referensi bagi peneliti dan praktisi keamanan informasi.
2. Menyediakan wawasan tentang pentingnya perlindungan terhadap perangkat *Android.*
3. Memberikan informasi kepada pengguna perangkat *Android* untuk meningkatkan kesadaran keamanan.

1.6 Sistematika Penulisan

Penulis membuat suatu sistematika penulisan yang dibagi atas beberapa bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini menjelaskan Latar Belakang Masalah, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, dan Sistematika Penulisan yang bertujuan untuk memberikan gambaran awal mengenai konteks penelitian, masalah yang dihadapi, serta tujuan dan manfaat yang ingin dicapai dari penelitian ini.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan Landasan Teori, Tinjauan Pustaka, dan Kerangka Pemikiran yang bertujuan untuk memberikan dasar teoritis yang relevan dan mendukung penelitian ini, serta menyusun kerangka pemikiran yang akan digunakan dalam analisis penelitian.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan Tahapan Penelitian, Metode Penelitian, Metode Pengumpulan Data dan Analisis Kebutuhan yang bertujuan untuk menguraikan langkah-langkah penelitian yang dilakukan, metode yang digunakan dalam pengumpulan dan analisis data.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan Implementasi dan Hasil yang bertujuan untuk memaparkan hasil dari penelitian yang telah dilakukan, termasuk implementasi dari metode yang digunakan dan pembahasan mengenai temuan yang diperoleh.

BAB V PENUTUP

Bab ini menjelaskan Kesimpulan dan Saran yang bertujuan untuk menyimpulkan hasil penelitian yang telah dilakukan dan memberikan saran-saran untuk pengembangan selanjutnya, agar dapat dilakukan perbaikan-perbaikan di masa yang akan datang

Nusa Putra
UNIVERSITY
2002
AMOR DEUS, PARENTIUM, CONCERVIS

BAB V
PENUTUP

5.1 Kesimpulan

Penelitian ini mengimplementasikan dan menganalisis keamanan perangkat *Android* 13 dengan menggunakan metode *Reverse_TCP* melalui *Metasploit*. Diantaranya:

1. Terkait proses analisis dan eksploitasi menggunakan *Metasploit Reverse TCP* pada perangkat *Android* 13, penelitian ini menunjukkan bahwa langkah- langkah eksploitasi termasuk pengiriman aplikasi *backdoor*, pembukaan sesi *Meterpreter*, dan manipulasi data seperti pencurian *SMS*, *log* panggilan, dan informasi lokasi. Meskipun *Google Play Protect* dapat mendeteksi aplikasi berbahaya, aplikasi tersebut masih bisa diinstal dan dijalankan, menunjukkan kelemahan dalam sistem deteksi keamanan.
2. Mengenai dampak dan potensi risiko dari eksploitasi menggunakan metode *Reverse_TCP* pada perangkat *Android* 13, penelitian ini menemukan bahwa eksploitasi ini dapat menyebabkan berbagai risiko, seperti akses tidak sah ke data pribadi dan kontrol penuh atas perangkat. Penyerang bisa memanfaatkan kerentanan ini untuk mencuri informasi sensitif, mengendalikan fungsi perangkat, dan menyebabkan kerugian yang signifikan bagi pengguna.
3. Untuk langkah-langkah pencegahan yang bisa dirancang dan diterapkan untuk meningkatkan keamanan *kernel Android* 13, penelitian ini menekankan pentingnya langkah-langkah pencegahan untuk mengurangi risiko eksploitasi. Penggunaan *Mobile Security Framework (MobSF)* terbukti efektif dalam mengevaluasi dan mengidentifikasi kerentanan dalam aplikasi backdoor. Mengaktifkan *Google Play Protect* membantu dalam mendeteksi dan mencegah instalasi aplikasi berbahaya. Selain itu, menonaktifkan izin aplikasi yang tidak diperlukan secara signifikan mengurangi risiko eksploitasi, karena aplikasi

backdoor tidak bisa mengakses data atau menjalankan perintah berbahaya tanpa izin yang memadai.

4. Pengujian juga berhasil dilakukan pada beberapa android 13 seperti *Infinix Smart 8*, *Samsung M12* dan *Xiaomi Redmi 12*. Dan berhasil membuka sesi meterpreter dari ketiga android tersebut.

5.2 Saran

Saran untuk penelitian ini mencakup peningkatan analisis terhadap metode eksploitasi selain *Reverse_TCP*, evaluasi lebih lanjut terhadap efektivitas langkah- langkah pencegahan yang diidentifikasi, analisis mendalam terhadap dampak jangka panjang dari serangan yang berhasil, perbandingan dengan metode eksploitasi lainnya, dan eksperimen dengan berbagai konfigurasi perangkat *Android* 13 untuk memahami kerentanan yang mungkin terjadi pada konfigurasi tertentu. Penelitian dan pengembangan lebih lanjut pada *Android* 14, termasuk analisis terhadap perubahan keamanan yang diperkenalkan pada versi ini, serta eksperimen dengan berbagai konfigurasi perangkat *Android* 14 untuk mengidentifikasi dan memahami kerentanan baru yang mungkin muncul.

DAFTAR PUSTAKA

[1] P. Sharma, C. Lepcha, S. T. Bhutia, and A. Sharma, "CASE STUDY EXPLOIT OF *ANDROID* DEVICES USING PAYLOAD INJECTED APK," 2023, [Online]. Available: www.irjmets.com

[2] Deshinta. arrovadewi dan jelita. asian Somantri, "Implementasi Computer Based Test Pada SMP PGRI Se-Gugus V Kecamatan Cileungsi Kabupaten Bogor," 2023, Accessed: May 08, 2024. [Online]. Available: https://restikom.nusaputra.ac.id/issue/view/18

[3] D. Özdemir and H. Ç. Zaim, "INVESTIGATION OF ATTACK TYPES IN *ANDROID* OPERATING SYSTEM," 2021.

[4] S. Raj and N. K. Walia, "A Study on *Metasploit* Framework: A Pen-Testing Tool," in *2020 International Conference on Computational Performance Evaluation, ComPE 2020*, Institute of Electrical and Electronics Engineers Inc., Jul. 2020, pp. 296–302. doi: 10.1109/ComPE49325.2020.9200028.

[5] A. Dwivedi, "LAUNCHING AN ATTACK AND EXPLOITING THE *ANDROID* USING *METASPLOIT* FRAMEWORK," 2022. [Online]. Available: www.ijsrmst.com

[6] Mr. Gokul Reghu, Ms. Anjaly Prasad, Ms. Athira Prasad, and Ms. Grace Joseph, "Novel Approach For *Android* Hacking Using Bluesnarfer," 2023.

[7] T. Yerlikaya and S. Sen, "Hacking *Android* Mobile Phone with Phishing," 2021. [Online]. Available: http://10.40.48.145/police.apk

[8] I. Riadi, D. Aprilliansyah, and S. Sunardi, "Mobile Device Security Evaluation using Reverse TCP Method," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, Sep. 2022, doi: 10.22219/kinetik.v7i3.1433.

[9] S. Thomas, P. G. Scholar, and T. Bijimol, "Vulnerability Testing on Rooted *Android* Phones Using Msf Venom Payloads," vol. 3, no. 1, p. 27, 2021, doi: 10.5281/zenodo.5112704.

[10] R. Dwiananda, L. Putra, and 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, p. 11440, 2019.

[11] R. Satrio Hadikusuma and E. M. Rizaludin, "Methods of Stealing Personal Data on *Android* Using a Remote Administration Tool with Social Engineering Techniques," *Ultimatics : Jurnal Teknik Informatika*, vol. 15,

no. 1, 2023.

[12] K. Barapatre and P. Parkhi, "*Android* Spy Agent-Remote Access Trojan," *International Research Journal of Engineering and Technology*, 2020, [Online]. Available: www.irjet.net

[13] N. Kar Zuin and V. Selvarajah, "A Case Study: SYN Flood Attack Launched Through *Metasploit*," 2021.

[14] N. Jaswal, *Mastering Metasploit : exploit systems, cover your tracks, and bypass security controls with the Metasploit 5.0 framework*. 2020.

[15] S. Rahalkar, *Metasploit 5.0 for beginners : perform penetration testing to secure your IT environment against threats and vulnerabilities*. 2020.

[16] K. N. Isnaini and D. Suhartono, "Security Analysis of Simpel Desa using Mobile Security Framework and ISO 27002:2013," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 7, no. 1, pp. 84–105, Feb. 2023, doi: 10.29407/intensif.v7i1.18742.

[17] A. Arote and U. Mandawkar, "*Android* Hacking in Kali Linux Using *Metasploit* Framework," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 497–504, Jun. 2021, doi: 10.32628/cseit2173111.

[18] V. K. Velu and R. Beggs, *Mastering Kali Linux for advanced penetration testing secure your network with Kali Linux 2019.1 - the ultimate white hat hackers' toolkit, 3rd edition*. 2019.

[19] A. Sabbah, M. Kharma, and M. Jarrar, "Creating *Android* Malware Knowledge Graph Based on a Malware Ontology," Aug. 2023, [Online]. Available: http://arxiv.org/abs/2308.02640

[20] H. Singh and H. Sharma, *Hands-on web penetration testing with Metasploit : the subtle art of using Metasploit 5.0 for web application exploitation*. 2020.