Implementasi Metasploit Framework Pada Platform Android Dalam Satu Jaringan

Muhammad Fitra Gemilang, Arif Senja Fitrani, Mochamad Alfan Rosid, Sumarno

Program Studi Informatika, Universitas Muhammadiyah Sidoarjo, Indonesia
Email Penulis Korespondensi: arifsenjafitrani@umsida.ac.id

Abstract. *This study explores the implementation of the Metasploit Framework on Android platforms within a single network. The aim is to analyze the vulnerability of Android systems against backdoor-based attacks using penetration testing tools. The study used msfvenom to generate a malicious APK and tested it within a LAN environment. The results showed successful exploitation, including access to sensitive data like SMS, call logs, and device location. This highlights the importance of Android security awareness and proactive prevention strategies..*

Keywords - *Metasploit; Android; Penetration Testing; Backdoor; Payload*

Abstrak. Penelitian ini membahas implementasi Metasploit Framework terhadap platform Android dalam satu jaringan. Tujuan penelitian ini adalah untuk menganalisis kerentanan perangkat Android terhadap serangan backdoor menggunakan tools penetration testing. Payload dalam bentuk file APK dibuat menggunakan msfvenom dan diuji pada perangkat Android dalam jaringan lokal. Hasil menunjukkan eksploitasi berhasil, termasuk akses ke SMS, log panggilan, dan lokasi perangkat. Penelitian ini menunjukkan perlunya kesadaran keamanan pada pengguna Android dan pentingnya langkah pencegahan.

Kata Kunci - *Metasploit; Android; Penetration Testing; Backdoor; Payload*

I. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mendorong meningkatnya penggunaan perangkat berbasis sistem operasi Android di berbagai aspek kehidupan, mulai dari komunikasi, transaksi digital, hingga sistem kendali perangkat pintar[1]. Android, sebagai sistem operasi dengan lisensi terbuka (open source), memberikan fleksibilitas tinggi bagi para pengembang dan produsen perangkat. Namun, keterbukaan sistem ini juga menjadikannya sebagai sasaran empuk bagi berbagai jenis serangan siber (cyber attack) yang memanfaatkan celah keamanan aplikasi dan sistem[2].

Menurut laporan dari Symantec dan Badan Siber dan Sandi Negara, Indonesia menempati peringkat tinggi dalam jumlah insiden serangan siber di kawasan Asia Tenggara, termasuk serangan yang melibatkan teknik backdoor[3]. Backdoor merupakan metode serangan yang memberikan akses tersembunyi kepada penyerang untuk mengendalikan sistem tanpa sepengetahuan pengguna, sering kali melalui aplikasi yang telah dimodifikasi atau disusupi. Teknik ini berbahaya karena mampu menghindari deteksi dan memberikan kontrol penuh atas perangkat korban[4].

Salah satu framework yang umum digunakan dalam pengujian penetrasi dan eksploitasi sistem Android adalah Metasploit Framework. Metasploit adalah alat bantu dalam bidang ethical hacking yang mendukung berbagai teknik serangan, termasuk pembuatan dan penyisipan payload ke dalam perangkat target[5]. Dengan alat ini, penyerang dapat memperoleh akses sistem, mengunduh data, atau mengaktifkan mikrofon dan kamera secara diam-diam. Pengetahuan tentang bagaimana serangan ini bekerja sangat penting untuk meningkatkan ketahanan siber dan kesadaran pengguna dalam mengelola keamanan perangkatnya.

Berbagai penelitian sebelumnya telah membahas pemanfaatan Metasploit untuk simulasi serangan terhadap sistem Android. Penelitian Nugroho et al. [6] menunjukkan efektivitas teknik reverse TCP payload dalam mengakses sistem Android dari jarak jauh, sementara studi oleh Pratiwi dan Miarsa menyoroti pentingnya edukasi pengguna dalam mendeteksi aplikasi berbahaya[7]. Meski demikian, masih dibutuhkan kajian lebih lanjut yang fokus pada pemetaan tingkat akses yang diperoleh melalui serangan backdoor dan langkah mitigasi yang dapat dilakukan.

Penelitian ini bertujuan untuk mengetahui proses eksploitasi perangkat Android menggunakan Metasploit Framework, menggambarkan sejauh mana akses yang dapat diperoleh melalui backdoor, serta meningkatkan kesadaran akan pentingnya pengamanan perangkat Android dari akses tidak sah. Dengan adanya penelitian ini, diharapkan dapat memberikan kontribusi terhadap pengembangan strategi pencegahan dan deteksi dini terhadap ancaman siber yang menargetkan sistem operasi Android.

II. METODE

Penelitian ini menggunakan pendekatan **eksperimen** dengan metode **studi kasus** pada perangkat Android yang berada dalam satu jaringan lokal. Tujuan dari metode ini adalah untuk mensimulasikan proses serangan *backdoor* menggunakan *Metasploit Framework*, guna mengamati secara langsung tahapan eksploitasi dan tingkat akses yang dapat diperoleh oleh penyerang.

2.1 Perangkat dan Alat

Penelitian dilakukan menggunakan satu perangkat komputer sebagai **attacker** dan satu perangkat Android sebagai **target/victim**. Komputer penyerang menjalankan sistem operasi Kali Linux yang telah terinstal *Metasploit Framework* dan *msfvenom*, sedangkan perangkat target menggunakan sistem operasi Android versi 8.0 (Oreo) ke atas. Koneksi antara kedua perangkat dilakukan melalui jaringan Wi-Fi lokal (*Local Area Network*).

2.2 Langkah-Langkah Eksperimen

Tahapan eksperimen dalam penelitian ini meliputi:

1. **Pembuatan Payload**
   Peneliti menggunakan perintah msfvenom untuk membuat payload dengan tipe android/meterpreter/reverse_tcp. Payload tersebut dikemas dalam format file .apk (Android Package) dan disamarkan agar menyerupai aplikasi yang sah, sehingga dapat dijalankan pada perangkat target tanpa menimbulkan kecurigaan[8]..
2. **Distribusi Payload**
   File APK hasil kompilasi didistribusikan secara manual ke perangkat Android untuk tujuan simulasi (bukan melalui Play Store atau media sosial, demi menjaga etika eksperimen).
3. **Penyisipan dan Eksekusi Payload**
   Setelah aplikasi terinstal dan dijalankan pada perangkat Android, *Metasploit Handler* akan mendengarkan koneksi dari perangkat target. Jika berhasil, sesi Meterpreter akan terbuka, menandakan bahwa perangkat telah berhasil dieksploitasi[9].
4. **Observasi dan Dokumentasi Akses**
   Peneliti mengamati fitur-fitur yang dapat dikendalikan dari jarak jauh melalui sesi Meterpreter, seperti mengambil gambar, membaca file, mengakses lokasi, merekam audio, hingga membuka kamera.
5. **Analisis Keamanan dan Potensi Kerentanan**
   Hasil eksploitasi kemudian dianalisis untuk mengidentifikasi potensi risiko keamanan dan sejauh mana kontrol yang dapat diperoleh oleh penyerang melalui *backdoor* ini.[10]

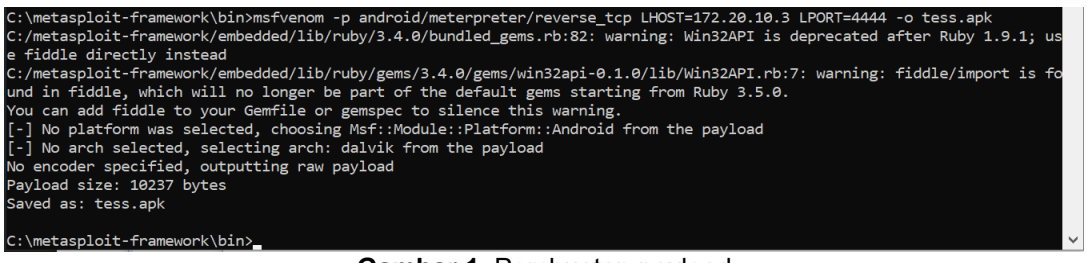
2.3 Etika dan Keamanan Penelitian

Seluruh proses eksperimen dilakukan dalam lingkungan tertutup dan terkendali, tanpa melibatkan perangkat pihak ketiga atau individu lain. Penelitian ini murni bersifat edukatif dan bertujuan untuk meningkatkan kesadaran akan pentingnya keamanan perangkat Android. Tidak ada data pribadi yang disalahgunakan selama proses penelitian.

III. HASIL DAN PEMBAHASAN

A. Pembuatan payload

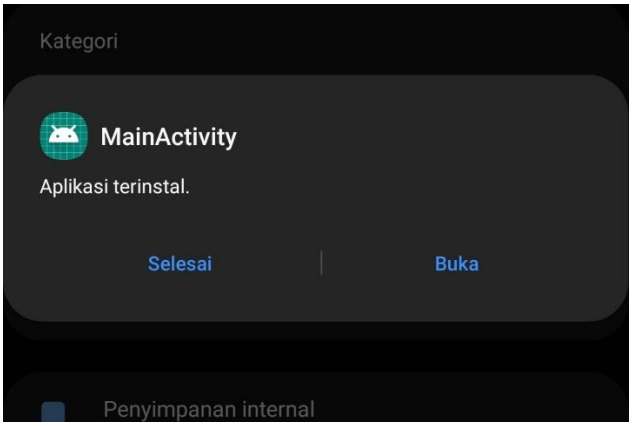
Payload dibuat menggunakan perintah msfvenom -p android/meterpreter/reverse_tcp LHOST=172.20.10.3 LPORT=4444 -o tess.apk, yang ditunjukkan pada Gambar 1. Perintah ini menghasilkan file tess.apk yang berisi payload dengan konfigurasi alamat host lokal (LHOST) 172.20.10.3 dan port (LPORT) 4444 sebagai jalur komunikasi balik ke perangkat penyerang. Perintah tersebut menghasilkan file *tess.apk* yang berisi payload dengan ukuran sebesar 10.237 byte, yang nantinya digunakan untuk mengeksploitasi perangkat Android target melalui koneksi balik (*reverse connection*).



Gambar 1. Pembuatan payload

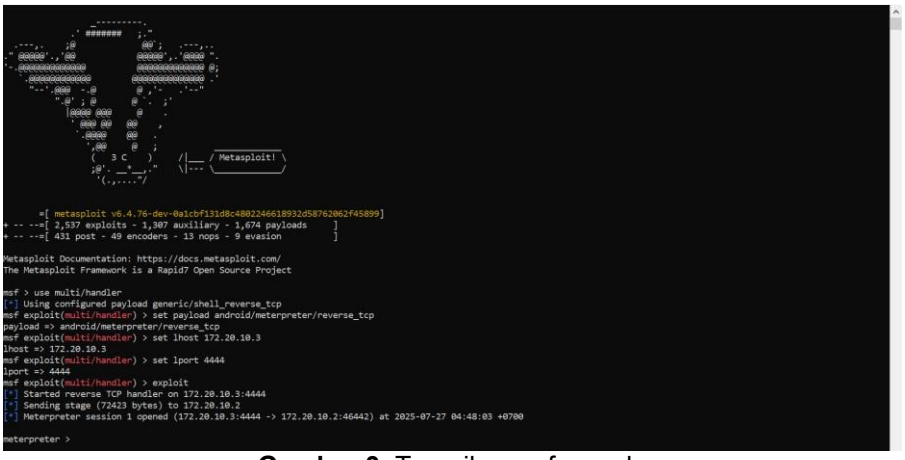
B. Instalasi pada perangkat android

File APK dikirim ke perangkat Android melalui sambungan kabel USB karena metode ini menawarkan kecepatan transfer yang lebih tinggi, koneksi yang lebih stabil, serta risiko deteksi yang lebih rendah dibandingkan dengan koneksi nirkabel. Pengujian dilakukan dengan menjalankan aplikasi pada perangkat Android dan memantau sesi koneksi Meterpreter melalui perangkat laptop penyerang, seperti ditunjukkan pada Gambar 2



Gambar 2. APK telah terinstall

C. Buat apk backdoor dengan msfvenom



Gambar 3. Tampilan msfconsole

Msfconsole merupakan alat yang digunakan untuk menjalankan Meterpreter dan mengeksekusi payload yang telah dibuat sebelumnya. Proses ini dimulai dengan perintah use multi/handler untuk mempersiapkan listener, diikuti dengan konfigurasi parameter Local Host (LHOST) dan Local Port (LPORT). Setelah konfigurasi selesai, perintah exploit dijalankan untuk menunggu koneksi dari perangkat target, seperti ditunjukkan pada Gambar 3

D. Perintah-perintah eksploitasi

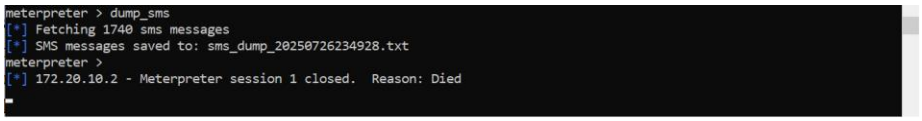
Eksploitasi dapat dilakukan dengan menjalankan sejumlah perintah tertentu melalui sesi Meterpreter. Beberapa di antaranya adalah sysinfo, yang digunakan untuk menampilkan informasi sistem seperti versi Android dan arsitektur CPU; dump_sms untuk mengambil data pesan SMS dari perangkat; dump_calllog untuk memperoleh riwayat panggilan; app_list untuk menampilkan seluruh aplikasi yang terinstal pada perangkat; serta geolocate, yang digunakan untuk mengambil koordinat GPS dari lokasi perangkat target.

E. Visualisasi hasil

Gambar 4 menampilkan keluaran dari perintah sysinfo dalam lingkungan Metasploit Meterpreter. Informasi yang ditampilkan menggambarkan detail sistem dari perangkat Android yang berhasil diakses. Perangkat tersebut memiliki hostname localhost dan menjalankan sistem operasi Android 11 di atas kernel Linux versi 4.14.113 dengan nama Lengyue-beyond0lte-Kernel-V7. Arsitektur prosesor yang digunakan adalah aarch64, menunjukkan bahwa perangkat berbasis ARM 64-bit. Bahasa sistem yang terdeteksi adalah in_ID, yang mengindikasikan penggunaan bahasa Indonesia. Jenis Meterpreter yang aktif adalah dalvik/android, yang mengonfirmasi bahwa sesi eksploitasi ini terhubung ke perangkat Android.

Gambar 4. sysinfo

Gambar 5 memperlihatkan interaksi dalam lingkungan Meterpreter, yaitu sebuah payload canggih dari Metasploit Framework yang digunakan untuk melakukan aktivitas post-exploitation pada sistem yang telah berhasil dikompromikan. Dalam skenario ini, perintah dump_sms berhasil dijalankan dan menghasilkan ekstraksi sebanyak 1.740 pesan SMS dari perangkat target. Data tersebut kemudian disimpan secara otomatis ke dalam berkas sms_dump_20250726234928.txt. Namun, setelah proses pengambilan data selesai, sesi Meterpreter yang sebelumnya terhubung ke alamat IP 172.20.10.2 terputus secara tiba-tiba dengan status "Reason: Died". Hal ini mengindikasikan bahwa sesi eksploitasi berakhir secara tidak terduga, yang kemungkinan disebabkan oleh gangguan koneksi jaringan, crash pada agent Meterpreter di sisi perangkat target, atau perangkat dimatikan secara paksa.

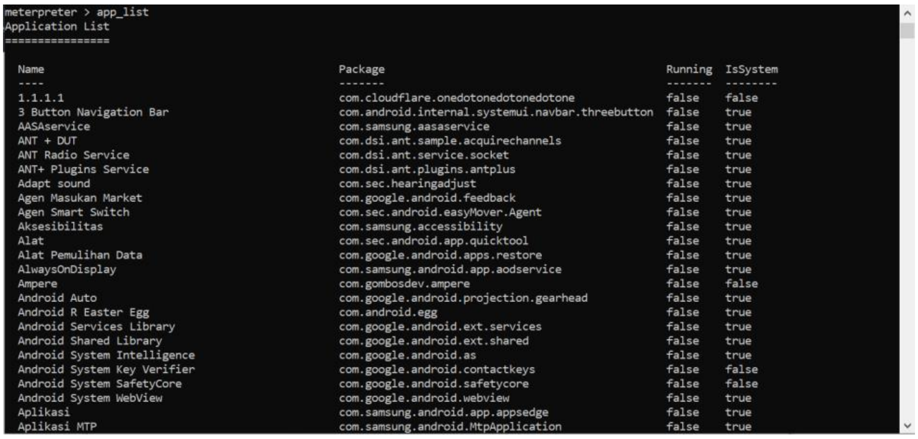


Gambar 5. dump_sms

Gambar 6 menunjukkan salah satu operasi dalam sesi Meterpreter, di mana perintah dump_calllog berhasil dijalankan untuk mengambil riwayat panggilan dari perangkat target. Hasil dari proses ini mencakup sebanyak 315 entri atau catatan panggilan yang berhasil diekstraksi. Setelah proses pengambilan selesai, seluruh data tersebut disimpan ke dalam sebuah berkas teks dengan nama calllog_dump_20250727081520.txt. Format penamaan berkas tersebut diduga mencakup informasi tanggal dan waktu saat proses dumping dilakukan, guna memudahkan identifikasi hasil ekstraksi berdasarkan waktu eksekusi.

Gambar 6. dump_callog

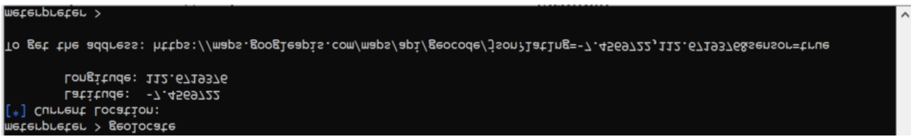
Gambar 7 menampilkan hasil eksekusi perintah app_list dalam sesi Meterpreter, yang digunakan untuk memperoleh daftar lengkap aplikasi yang terinstal pada perangkat Android target. Setiap entri dalam daftar mencakup beberapa kolom informasi penting, yaitu Name (nama tampilan aplikasi), Package (nama paket unik sebagai identitas aplikasi), Running (status apakah aplikasi sedang berjalan, ditandai dengan "true" atau "false"), dan IsSystem (indikasi apakah aplikasi tersebut merupakan bagian dari sistem operasi). Dari data yang ditampilkan, dapat diamati keberagaman aplikasi yang terinstal, mulai dari aplikasi utilitas seperti "1.1.1.1" (yang kemungkinan merupakan aplikasi VPN dari Cloudflare) dan "3 Button Navigation Bar", hingga layanan sistem Android seperti "ANT+ Plugins Service", "Android System Intelligence", serta aplikasi bawaan pabrikan seperti "AlwaysOnDisplay" dan "Aplikasi MTP". Informasi ini memberikan gambaran komprehensif mengenai ekosistem aplikasi yang berjalan pada perangkat yang berhasil dieksploitasi.


meterpreter > app_list
Application List
================

Name	Package	Running	IsSystem
1.1.1.1	com.cloudflare.onedotonedotonedotone	false	false
3 Button Navigation Bar	com.android.internal.systemui.navbar.threebutton	false	true
AASAservice	com.samsung.aasaservice	false	true
ANT + DUT	com.dsi.ant.sample.acquirechannels	false	true
ANT Radio Service	com.dsi.ant.service.socket	false	true
ANT+ Plugins Service	com.dsi.ant.plugins.antplus	false	true
Adapt sound	com.sec.hearingadjust	false	true
Agen Masukan Market	com.google.android.feedback	false	true
Agen Smart Switch	com.sec.android.easyMover.Agent	false	true
Aksesibilitas	com.samsung.accessibility	false	true
Alat	com.sec.android.app.quicktool	false	true
Alat Pemulihan Data	com.google.android.apps.restore	false	true
AlwaysOnDisplay	com.samsung.android.app.aodservice	false	true
Ampere	com.gombosdev.ampere	false	false
Android Auto	com.google.android.projection.gearhead	false	true
Android R Easter Egg	com.android.egg	false	true
Android Services Library	com.google.android.ext.services	false	true
Android Shared Library	com.google.android.ext.shared	false	true
Android System Intelligence	com.google.android.as	false	true
Android System Key Verifier	com.google.android.contactkeys	false	false
Android System SafetyCore	com.google.android.safetycore	false	false
Android System WebView	com.google.android.webview	false	true
Aplikasi	com.samsung.android.app.appsedge	false	true
Aplikasi MTP	com.samsung.android.MtpApplication	false	true

Gambar 7. App_list

Gambar 8 menampilkan hasil keluaran dari sesi Meterpreter yang terlihat tidak biasa, di mana teks tampak terbalik dan sulit dibaca. Hal ini mengindikasikan adanya kemungkinan gangguan pada orientasi tampilan terminal atau penggunaan encoding karakter yang tidak standar. Meskipun demikian, setelah dilakukan pembacaan terbalik secara manual, beberapa elemen dapat diidentifikasi, seperti frasa "current location" dan perintah geolocate, yang menunjukkan bahwa pengguna telah mengeksekusi fitur geolokasi dalam Meterpreter untuk memperoleh koordinat geografis dari perangkat target. Walaupun hasil yang ditampilkan tidak langsung terbaca dengan jelas, konteks perintah tersebut tetap menggambarkan upaya untuk mengambil data lokasi dari sistem yang telah dikompromikan.



Gambar 8. Geolocate

IV. Kesimpulan

Penelitian ini menunjukkan bahwa sistem operasi Android, meskipun bersifat terbuka dan fleksibel, sangat rentan terhadap serangan siber yang memanfaatkan teknik backdoor. Dengan memanfaatkan Metasploit Framework dan payload bertipe android/meterpreter/reverse_tcp, penyerang dapat memperoleh akses penuh ke perangkat target. Eksperimen yang dilakukan berhasil mendemonstrasikan bagaimana sebuah aplikasi berbahaya dapat dibuat, disamarkan, diinstal, dan dijalankan untuk membuka sesi Meterpreter yang memungkinkan pengambilan data sensitif seperti pesan SMS, riwayat panggilan, daftar aplikasi, dan bahkan lokasi geografis perangkat.

Ucapan Terima Kasih

Ucapan terima kasih disampaikan kepada Bapak Arif Senja Fitrani, M.Kom., selaku dosen pembimbing, serta kepada Laboratorium Informatika Universitas Muhammadiyah Sidoarjo atas dukungan fasilitas yang telah diberikan selama proses penelitian ini. Penelitian ini disadari masih memiliki sejumlah kekurangan. Oleh karena itu, masukan berupa kritik dan saran sangat diharapkan agar penelitian serupa di masa mendatang dapat dilakukan dengan lebih baik.

Referensi

[1] N. A. Pandusaputri, R. B. Ramadhan Mokodompit, and E. P. Simangunsong, “KENYAMANAN PENGGUNA IOS DAN ANDROID DI KALANGAN GENERASI Z.,” *J. Syntax Lit.*, vol. 9, no. 5, 2024, Accessed: Jul. 29, 2025. [Online]. Available: https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=2541

0849&AN=177805927&h=uksAeuWpjxLKL48E9O%2Fto7SdL8xkVBLco0X5X%2FEOyRvwH5Jruu%2BuqgaDJKekD2JdsFvYpsQDvNgIDykjqXhRGg%3D%3D&crl=c.
[2] L. D. Samsumar *et al.*, "Keamanan Sistem Informasi: Perlindungan Data dan Privasi di Era Digital." Hadla Media Informasi, 2025. Accessed: Jul. 29, 2025. [Online]. Available: http://pustakahadla.com/xmlui/handle/123456789/39
[3] R. Vice, N. C. Simaremare, and S. Manalu, "Perkembangan Cybercrime: Dampak Terhadap Keamanan dan Ketahanan Nasional serta Pencegahannya," *Mimb. KEADILAN J. Ilmu Huk.*, pp. 71–83, 2024.
[4] A. Ripaldi, "Jenis Serangan Siber Umum," Portal Jember, 2021. [Online]. Tersedia: https://portaljember.pikiran-rakyat.com
[5] Rapid7, "Metasploit Framework Documentation," 2022. [Online]. Tersedia: https://docs.rapid7.com/metasploit
[6] H. Ayasso and A. Mohammad-Djafari, "Joint NDT Image Restoration and Segmentation Using Gauss–Markov–Potts Prior Models and Variational Bayesian Computation," *IEEE Transactions on Image Processing*, vol. 19, no. 9, pp. 2265-77, 2010. [Online]. Available: IEEE Xplore, http://www.ieee.org. [Accessed Sept. 10, 2010].
[7] A. F. Ramadhan, A. D. Putra, and A. Surahman, "Aplikasi Pengenalan Perangkat Keras Komputer Berbasis Android Menggunakan Augmented Reality (AR)," J. Teknol. dan Sist. Inf., vol. 2, no. 2, pp. 24–31, 2021, [Online]. Available: http://jim.teknokrat.ac.id/index.php/JTSI.
[8] N. K. Ceryna Dewi, I. B. G. Anandita, K. J. Atmaja, and P. W. Aditama, "Rancang Bangun Aplikasi Mobile Siska Berbasis Android," SINTECH (Science Inf. Technol. J., vol. 1, no. 2, pp. 100–107, 2018, doi: 10.31598/sintechjournal.v2i1.291.
[9] T. Wijayanto and A. Susilo, "Implementasi Backdoor Scanner Tool Menggunakan Metode Carving File Pada Server Codepolitan," I-STATEMENT Inf. Syst. Technol. Manag., vol. 3, no. 2, 2017, [Online]. Available: http://journal.esqbs.ac.id/index.php/I-STATEMENT/article/view/64/66.
[10] M. R. Akhyari and A. R. Pratama, "Kesadaran akan Ancaman Serangan Berbasis Backdoor di Kalangan Pengguna Smartphone Android," Automata, vol. 2, no. 1, p. 7, 2021, [Online]. Available: https://journal.uii.ac.id/AUTOMATA/article/view/17317

Conflict of Interest Statement:
The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.