ANALISIS MEKANISME PAYLOAD METASPLOIT MELALUI JARINGAN PUBLIK MENGGUNAKAN TUNNELING TERHADAP KEAMANAN SISTEM OPERASI ANDROID 13

TUGAS AKHIR
SKRIPSI

MUHAMAD FADLY RAEHAN
41522010222

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2026

ANALISIS MEKANISME PAYLOAD METASPLOIT MELALUI JARINGAN PUBLIK MENGGUNAKAN TUNNELING TERHADAP KEAMANAN SISTEM OPERASI ANDROID 13

TUGAS AKHIR
SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana

MUHAMAD FADLY RAEHAN
41522010222

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2026

HALAMAN PERNYATAAN KARYA SENDIRI

Saya yang bertanda Tangan di bawah Ini:

Nama	: Muhamad Fadly Raehan
NIM	: 41522010222
Fakultas/Program Studi	: Ilmu Komputer / Teknik Informatika

Menyatakan dengan sebenar-benarnya bahwa Tugas Akhir berjudul:
"Analisis Mekanisme Payload Metasploit Melalui Jaringan Publik Menggunakan Tunneling Terhadap Keamanan Sistem Operasi Android 13" adalah hasil karya saya sendiri, tidak mengandung unsur plagiarisme, pelanggaran hak cipta, atau konten ilegal dalam bentuk apapun dan tidak melanggar hukum atau hak pihak manapun.

Apabila di kemudian hari ditemukan pelanggaran terhadap pernyataan ini, saya bersedia menanggung seluruh konsekuensi hukum dan membebaskan Universitas Mercu Buana dari segala bentuk tuntutan hukum dan saya siap mendapatkan sanksi akademis yang berlaku di Universitas Mercu Buana.

Demikian pernyataan ini saya buat dengan sebenar-benarnya untuk digunakan sebagaimana mestinya.

Jakarta , 27 Juli 2026

Muhamad Fadly Raehan

HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN

072.423.4.03.01

UNIVERSITAS
MERCU BUANA
AKREDITASI UNGGUL

PERNYATAAN SIMILARITY CHECK
/SIMILARITY CHECK STATEMENT

Saya yang bertanda tangan dibawah ini menyatakan, bahwa karya ilmiah yang ditulis oleh
/The undersigned, hereby declare that the scientific work written by

Nama /Name	: Muhamad Fadly Raehan
NIM /Student ID Number	: 41522010222
Program Studi /Study Program	: Teknik Informatika

Dengan Judul Tugas Akhir
/The title:

"ANALISIS MEKANISME PAYLOAD METASPLOIT MELALUI JARINGAN PUBLIK MENGGUNAKAN TUNNELING TERHADAP KEAMANAN SISTEM OPERASI ANDROID 13"

telah dilakukan pengecekan *similarity* dengan sistem Turnitin pada tanggal:
/Similarity checks have been carried out with the Turnitin system on the date:

5 Juni 2026

dengan nilai persentase sebesar :
/with a percentage value of:

13%

dinyatakan memenuhi standar sesuai dengan ketentuan berlaku di **Fakultas Ilmu Komputer** Universitas Mercu Buana. */declared to meet standards in accordance with applicable regulations at the Faculty of Computer Science, Universitas Mercu Buana.*

File hasil cek similarity turnitin:
/Turnitin similarity report file

https://drive.google.com/file/d/1nd3l0gPtwmgW9P9HjhJhQm9OKestCn_S/view?usp=drive_link

Jakarta, 5 Juni 2026
Admin Turnitin Fasilkom UMB

Agung Prawoto

Agung Prawoto, S.Kom., B.Sc
NIK : 322970503

Fakultas Ilmu Komputer
KAMPUS MENARA BHAKTI
Jl. Raya Meruya Selatan No. 1 Kembangan, Jakarta Barat 11650
Telp. 021-5840816 (Hunting), Psw : 5700 Fax. 021-5840813
http://www.mercubuana.ac.id, e-mail : fasilkom@mercubuana.ac.id

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan oleh:

Nama	:	Muhamad Fadly Raehan
NIM	:	41522010222
Fakultas/Program Studi	:	Fakultas Ilmu Komputer / Teknik Informatika
Judul Tugas Akhir	:	Analisis Mekanisme payload metasploit melalui Jaringan publik menggunakan tunneling terhadap keamanan sistem operasi android 13

Telah berhasil dipertahankan pada sidang tanggal 27 Juli 2026 dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer Universitas Mercu Buana.

Disahkan oleh:
Dosen Pembimbing

Muhammad Rifqi, S.kom., M.Kom.
NIDN/NUPTK: 0301067101

Jakarta, 27 Juli 2026
Mengetahui,

Dekan Fakultas Ilmu Komputer	Ketua Program Studi Teknik Informatika
Dr. Bambang Jokonowo, S.Si., MTI	Dr. Hadi Santoso, S.Kom., M.Kom
NIDN/NUPTK: 0320037002	NIDN/NUPTK: 0225067701

KATA PENGANTAR

Puji syukur kehadirat Tuhan yang Maha Esa, atas segala rahmat dan ridha-Nya sehingga penulis dapat menyelesaikan Tugas Akhir ini, yang merupakan salah satu persyaratan kelulusan Program Studi Strata Satu (S1) pada jurusan Teknik Informatika, Universitas Mercu Buana.

Penulis menyadari bahwa Tugas Akhir ini masih jauh dari sempurna, karena kesempurnaan sejatinya hanya milik Tuhan yang Maha Esa. Oleh karena itu kritik, saran dan masukan yang membangun senantiasa penulis terima dengan senang hati. Serta berkat dukungan, motivasi, bantuan, bimbingan, dan doa dari banyak pihak, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. Andi Adriansyah, M.Eng. selaku Rektor Universitas Mercu Buana.
2. Bapak Dr. Bambang Jokonowo, S.SI., MTI selaku Dekan Fakultas Ilmu Komputer.
3. Bapak Dr. Hadi Santoso, S.Kom., M.Kom. selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana.
4. Bapak Muhammad Rifqi, S.Kom, M.Kom. selaku dosen pembimbing MPTI yang telah memberikan pengarahan, motivasi, menyediakan waktu, tenaga, dan pikiran sehingga selama pembuatan proposal penelitian ini terjadwal dengan baik.
5. Kedua Orang Tua saya yang selalu mensuport dan mendukung saya selama menjalani masa studi sebagai mahasiswa Universitas Mercubuana..
6. Semua teman kuliah yang selalu berbagi informasi dan memberikan dukungan dalam bentuk yang berbeda-beda.

Akhir kata, penulis berharap semoga Tuhan yang Maha Esa membalas kebaikan dan selalu mencurahkan rahmat, hidayah, serta panjang umur kepada kita semua, aamiin. Terima Kasih.

Jakarta, 27 Juli 2026

Muhamad Fadly Raehan

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB

Sebagai sivitas akademik Universitas Mercu Buana, saya bertanda tangan di bawah ini:

Nama	: Muhamad Fadly Rachan
NIM	: 41522010222
Fakultas/Program Studi	: Fakultas Ilmu Komputer / Teknik Informatika
Judul Laporan Skripsi	: Analisis Mekanisme Payload Metasploit Melalui Jaringan Publik Menggunakan Tunneling Terhadap Keamanan Sistem Operasi Android 13

Demi Pengembangan ilmu Pengetahuan, dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Non-Eksklusif** (***Non-exclusive Royality-Free Right***) atas karya ilmiah saya yang berjudul di atas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/format-kan, mengelolah dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 27 Juli 2026

Yang menyatakan,

Muhamad Fadly Rachan

ANALISIS MEKANISME PAYLOAD METASPLOIT MELALUI JARINGAN PUBLIK MENGGUNAKAN TUNNELING TERHADAP KEAMANAN SISTEM OPERASI ANDROID 13

MUHAMAD FADLY RAEHAN

ABSTRAK

Seiring dirilisnya versi baru android, evaluasi keamanan terhadap Android 13 menjadi sangat krusial. Penelitian ini bertujuan untuk menganalisis mekanisme dan resistensi keamanan sistem operasi tersebut terhadap ancaman siber yang direplikasi menggunakan alat standar industri. Secara spesifik, penelitian ini mengevaluasi tingkat keberhasilan penetrasi Metasploit yang dikirimkan melalui jaringan publik menggunakan teknik *tunneling* terhadap sistem operasi Android 13 pada perangkat fisik. Berbeda dengan pengujian berbasis simulasi, seluruh pengujian dalam penelitian ini dilakukan menggunakan lingkungan perangkat keras langsung (*native*) melalui Kali Linux *Live USB Persistence* dan perangkat smartphone fisik untuk menjamin akurasi data empiris. Metode yang digunakan adalah Eksperimental Murni dengan skema *Penetration Testing*. Hasil penelitian ini diharapkan dapat mendokumentasikan tingkat ketahanan Android 13 terhadap serangan *payload* di jaringan publik, serta menjadi referensi penting bagi pengembang dan pengguna dalam memahami risiko keamanan spesifik pada platform tersebut.

Kata kunci: Android 13, Metasploit, Kali Linux, Payload, Penetration Testing, Tunneling.

ANALISIS MEKANISME PAYLOAD METASPLOIT MELALUI JARINGAN PUBLIK MENGGUNAKAN TUNNELING TERHADAP KEAMANAN SISTEM OPERASI ANDROID 13

MUHAMAD FADLY RAEHAN

ABSTRACT

As new versions of Android are released, security evaluations of android 13 have become increasingly crucial. This research aims to analyze the mechanism and security resistance of the operating system against cyber threats replicated using industry-standard tools. Specifically, this study evaluates the success rate of Metasploit payload penetration delivered via public networks using tunneling techniques against the Android 13 operating system on physical devices. Unlike simulation-based testing, all experiments in this study were conducted using a native hardware environment via Kali Linux Live USB Persistence and physical smartphone devices to ensure empirical data accuracy. The method employed is Pure Experimental with a Penetration Testing scheme. The results are expected to document the resilience level of Android 13 against payload attacks over public networks, serving as a vital reference for developers and users in understanding specific security risks on the platform.

Keywords: Android 13, Metasploit, Kali Linux, Payload, Penetration Testing, Tunneling.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN