



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

**TUGAS AKHIR
SKRIPSI**

**MUHAMAD FADLY RAEHAN
41522010222**

**UNIVERSITAS
MERCU BUANA**

**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**

**UNIVERSITAS
MERCU BUANA**

**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


F51EEAKX803049660
Muhamad Fadly Raehan

HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN



072.423.4.03.01

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/1nd3l0gPtwmgW9P9HjUjHqM9OKestCn_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

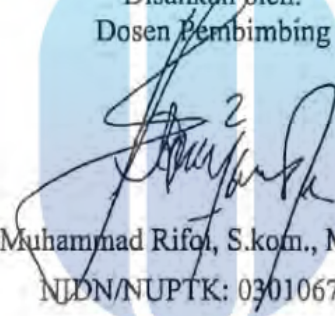
HALAMAN PENGESAHAN

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 Rifol, S.kom., M.Kom.
NIDN/NUPTK: 0301067101

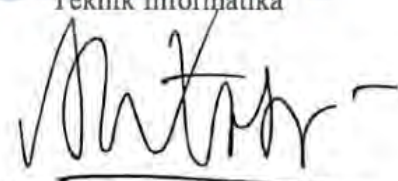
Jakarta, 27 Juli 2026

Mengetahui,

Dekan Fakultas Ilmu Komputer

Ketua Program Studi
Teknik Informatika


Dr. Bambang Jokonowo, S.Si., MTI
NIDN/NUPTK: 0320037002


Dr. Hadi Santoso, S.Kom., M.Kom
NIDN/NUPTK: 0225067701

KATA PENGANTAR

Puji syukur kehadiran 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 mensupport 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 Royalty-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.

MERCU BUANA

Jakarta, 27 Juli 2026

Yang menvatakan,


MEYERAI
TEMPEL
B8FD1AMX333089125

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.

UNIVERSITAS
MERCU BUANA

**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.

U N I V E R S I T A S
M E R C U B U A N A

DAFTAR ISI

HALAMAN SAMPUL.....	i
HALAMAN JUDUL	i
HALAMAN PERNYATAAN KARYA SENDIRI.....	ii
HALAMAN SURAT KETERANGAN HASIL UJI TURNITIN	iii
HALAMAN PENGESAHAN	iv
KATA PENGANTAR.....	v
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR DI REPOSITORI UMB	vi
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI.....	ix
DAFTAR TABEL	xi
DAFTAR GAMBAR.....	xii
DAFTAR LAMPIRAN	xiii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian	2
1.4 Batasan penelitian	2
1.4.1 Batasan Platform dan Perangkat.....	2
1.4.2 Batasan Jaringan dan Konektivitas.....	2
1.4.3 Batasan Teknik Penelitian.....	3
1.5 Manfaat Penelitian	3
1.5.1 Manfaat Akademis.....	3
1.5.2 Manfaat Praktis.....	3
BAB II TINJAUAN PUSTAKA.....	4
2.1 Penelitian Terdahulu	4
2.2 Teori Pendukung	9
2.2.1 Keytool.....	9
2.2.2 Metasploit Framework	9
2.2.3 Apksigner	9

2.2.4	Apktool.....	9
2.2.5	Ngrok	10
2.2.6	Mekanisme Keamanan Sistem Operasi Android 13	10
2.2.7	Konsep Komunikasi Reverse HTTPS Payload	11
2.2.8	Layanan Proteksi Google Play Protect	11
2.3	Gap penelitian	12
BAB III METODE PENELITIAN		13
3.1	Jenis Penelitian.....	13
3.2	Tahapan Penelitian	14
BAB IV HASIL DAN PEMBAHASAN		16
4.1.	Analisis Infrastruktur dan Lingkungan Pengujian	16
4.1.1	Analisis Performa Attacker Machine (Live USB Persistence)	16
4.1.2	Analisis Tunneling Ngrok.....	16
4.2.	Analisis Modifikasi APK Kalkulator	17
4.2.1	Analisis Proses Injeksi Payload Menggunakan Msfvenom	17
4.2.2	Analisis Proses Dekompilasi dan Rekompilasi APK (Apktool)	18
4.2.3	Proses Pembuatan Keytool.....	21
4.2.4	Analisis Proses Penandatanganan Digital dengan Apksigner	22
4.3	Analisis Pengujian Penetrasi Dengan Msfconsole.....	22
4.3.1.	Analisis Instalasi Aplikasi Hasil Modifikasi Pada Perangkat Target ...	23
4.3.2.	Pengujian Penyembunyian Ikon Aplikasi (Hide App Icon).....	24
4.4	Analisis Keberhasilan Ekstraksi Data (SMS_DUMP)	25
4.5.	Pembahasan Temuan Teknis	27
BAB V KESIMPULAN DAN SARAN		31
5.1	Kesimpulan.....	31
5.2	Saran.....	31
DAFTAR PUSTAKA.....		33
LAMPIRAN		36
Lampiran 1 Sertifikasi Coursera.....		36
Lampiran 2 Sertifikat BNSP		38
Lampiran 3 Curriculum Vitae (CV)		40
Lampiran 4 Surat Pernyataan & Pengalihan HAKI.....		41
Lampiran 5 Surat keterangan Bebas Perpustakaan.....		42
Lampiran 6 Transkrip Student Academy HackTheBox (HTB)		43
Lampiran 7 Logbook Bimbingan Akhir		45

DAFTAR TABEL

Tabel 2.1 Penelitian Terkait	4
Tabel 4.1 Perbandingan Temuan Penelitian Ini dengan Penelitian Terkait	28



DAFTAR GAMBAR

Gambar 4.1 Ngrok port forwarding	16
Gambar 4.2 melihat Ip Ngrok.....	17
Gambar 4.3 Msfvenom.....	18
Gambar 4.4 Analisis Proses Dekompilasi (Apktool).....	19
Gambar 4.5 membuka file kalkulator_fix	19
Gambar 4. 6 Modifikasi file AndroidManifest.xml	20
Gambar 4. 7 Rekompilasi file apk	20
Gambar 4.8 membuat keytool	21
Gambar 4.9 Analisis Penandatanganan Digital dengan Apksigner	22
Gambar 4.10 Pengujian Penetrasi dengan Msfconsole	23
Gambar 4.11 menunjukan perangkat Android dengan Sercpy.....	24
Gambar 4.12 menyembunyikan Aplikasi Kalkulator	25
Gambar 4.13 pengambilan pesan dengan meterpreter	26
Gambar 4.14 melihat isi pesan pada sms_dump.txt.....	26

DAFTAR LAMPIRAN

Lampiran 1 Sertifikasi Coursera.....	36
Lampiran 2 Sertifikat BNSP	38
Lampiran 3 Curriculum Vitae (CV)	40
Lampiran 4 Surat Pernyataan & Pengalihan HAKI.....	41
Lampiran 5 Surat keterangan Bebas Perpustakaan.....	42
Lampiran 6 Transkrip Student Academy HackTheBox (HTB)	43
Lampiran 7 Logbook Bimbingan Akhir	45

