

TUGAS AKHIR

**ANALISIS *MALWARE* BACKDOOR-APK
MENGUNAKAN METODE *REVERSE*
*ENGINEERING***



**AUFA SALSABILA NAHROWI
20102040**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2024**

TUGAS AKHIR

**ANALISIS *MALWARE* BACKDOOR-APK
MENGUNAKAN METODE *REVERSE*
*ENGINEERING***

***BACKDOOR-APK MALWARE ANALYSIS USING
REVERSE ENGINEERING METHOD***

Disusun Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Komputer



**AUFA SALSABILA NAHROWI
20102040**

**PROGRAM STUDI S1 TEKNIK INFORMATIKA
FAKULTAS INFORMATIKA
INSTITUT TEKNOLOGI TELKOM PURWOKERTO
2024**

LEMBAR PERSETUJUAN PEMBIMBING

**ANALISIS *MALWARE* BACKDOOR-APK
MENGUNAKAN METODE *REVERSE*
*ENGINEERING***

***BACKDOOR-APK MALWARE ANALYSIS USING
REVERSE ENGINEERING METHOD***

Dipersiapkan dan Disusun oleh

AUFA SALSABILA NAHROWI

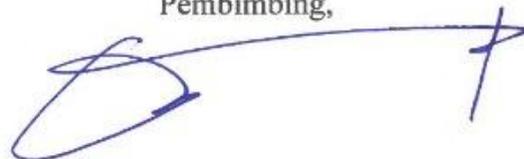
20102040

Fakultas Informatika

Institut Teknologi Telkom Purwokerto

Pada Tanggal: 1 April 2024

Pembimbing,



(Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom.)

NIDN. 0613038503

LEMBAR PENGESAHAN TUGAS AKHIR

**ANALISIS *MALWARE* BACKDOOR-APK
MENGUNAKAN METODE *REVERSE*
*ENGINEERING***

***BACKDOOR-APK MALWARE ANALYSIS USING
REVERSE ENGINEERING METHOD***

Disusun oleh

AUFA SALSABILA NAHROWI

20102040

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tugas Akhir
Pada Hari Kamis, 25 April 2024

Penguji I,



Bitu Parga Zen, S.Kom.,
M. Han.
NIDN. 0603089202

Penguji II,



Cahyo Priantoro, S.Kom.,
M.Eng.
NIDN. 0221019002

Penguji III,



Iqsyahiro Kresna A, S.T.,
M.T.
NIDN. 0616068903

Pembimbing Utama,



Wahyu Adi Prabowo, S.Kom., M.B.A., M.Kom
NIDN. 0613038503

Dekan,



Auliya Burhanuddin, S.Si., M.Kom
NIK. 19820008

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Afa Salsabila Nahrowi
NIM : 20102040
Program Studi : SI Teknik Informatika

Menyatakan bahwa Tugas Akhir dengan judul berikut:

ANALISIS *MALWARE* BACKDOOR-APK MENGGUNAKAN METODE *REVERSE ENGINEERING*

Dosen Pembimbing Utama : Wahyu Adi Prabowo, S.Kom., M.B.A.,
M.Kom.

Dosen Pembimbing Pendamping : -

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Institut Teknologi Telkom Purwokerto maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan, dan penelitian Saya Sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing.
3. Dalam Karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggungjawab Saya, bukan tanggungjawab Institut Teknologi Telkom Purwokerto.
5. Pernyataan ini Saya buat dengan sesungguhnya, apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka Saya bersedia menerima Sanksi Akademik dengan pencabutan gelar yang sudah diperoleh serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Purwokerto, 1 April 2024,

Yang Menyatakan,



(Afa Salsabila Nahrowi)

KATA PENGANTAR

Puji syukur peneliti panjatkan kehadirat Allah SWT yang telah memberikan skripsi dengan judul “Analisis *Malware* Backdoor-Apk Menggunakan Metode *Reverse Engineering*” sebagai salah satu persyaratan yang harus dipenuhi untuk menyelesaikan Pendidikan tingkat Sarjana Komputer pada Fakultas Informatika Institut Teknologi Telkom Purwokerto.

Dalam penyusunan skripsi ini, tidak terlepas dari dukungan dan bantuan dari berbagai pihak selama ini. Oleh karena itu, pada kesempatan ini peneliti mengucapkan terima kasih kepada:

1. Allah SWT yang senantiasa melimpahkan rahmat dan karunia-Nya sehingga skripsi ini dapat terselesaikan dengan baik;
2. Kedua orang tua peneliti, Ibu Rossy Yulia Sari dan Bapak Achmad Nahrowi yang telah memberikan do'a, dukungan serta motivasi secara terus-menerus sehingga peneliti mampu menyelesaikan studinya sampai sarjana;
3. Dr. Tenia Wahyuningrum, S.Kom., M.T selaku Rektor Institut Teknologi Telkom Purwokerto;
4. Auliya Burhanuddin, S.Si., M.Kom selaku Dekan Fakultas Informatika Institut Teknologi Telkom Purwokerto;
5. Amalia Belandinna Arifa, S.Pd., M.Cs selaku Ketua Program Studi S1 Informatika;
6. Wahyu Adi Prabowo, S.Kom.,M.B.A.,M.Kom selaku dosen pembimbing pertama yang senantiasa memberikan pengarahan dan dukungan dalam menyelesaikan tugas akhir ini;
7. Seluruh dosen dan karyawan Institut Teknologi Telkom Purwokerto yang telah memberikan banyak kesempatan, tempat dan waktu pada peneliti dalam menyelesaikan studi di Institut Teknologi Telkom Purwokerto;
8. Adik peneliti, Umar Abdurrahman yang telah memberikan semangat dan menjadi *mood booster* peneliti;
9. Seluruh Keluarga Besar yang telah memberikan dukungannya;

10. Khusnul Fauziah yang telah menjadi partner dalam penyusunan skripsi dan memberikan motivasi serta dukungan;
11. Teman – teman dan rekan – rekan peneliti, terutama Niken Pratiwi, Alyssa Diva Risana Fauziah, dan Atifah Herawati yang telah memberikan dukungan dan semangat.

Peneliti menyadari bahwa masih banyak kekurangan dalam penyusunan skripsi ini, sehingga kritik dan saran yang membangun sangat diharapkan. Akhir kata, peneliti berharap semoga skripsi ini dapat bermanfaat dan membantu menambah pengetahuan bagi yang membutuhkan.

Purwokerto, 1 April 2024



Aufa Salsabila Nahrowi

DAFTAR ISI

TUGAS AKHIR.....	ii
LEMBAR PERSETUJUAN PEMBIMBING.....	iii
LEMBAR PENGESAHAN TUGAS AKHIR	iv
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	v
KATA PENGANTAR	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR	x
DAFTAR TABEL.....	xi
DAFTAR SINGKATAN	xii
DAFTAR LAMPIRAN.....	xiii
ABSTRAK.....	xiv
ABSTRACT.....	xv
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Pertanyaan penelitian	3
1.4. Tujuan.....	3
1.5. Batasan masalah	3
1.6. Manfaat.....	4
BAB II TINJAUAN PUSTAKA.....	5
2.1. Penelitian Terkait	5
2.2. Dasar Teori	14
2.2.1. <i>Malware</i>	14
2.2.2. Backdoor	17
2.2.3. Backdoor-apk	17
2.2.4. Turbo VPN.....	18
2.2.5. Reverse Engineering	18
2.2.6. MobSF.....	18
2.2.7. JADX	19

2.2.8.	Metasploit.....	19
2.2.9.	Payload.....	20
2.2.10.	Meterpreter.....	21
2.2.11.	Exploit.....	22
2.2.12.	Kali linux.....	23
BAB III METODOLOGI PENELITIAN.....		25
3.1.	Objek dan Subjek Penelitian	25
3.2.	Alat dan Bahan Penelitian	25
3.3.	Diagram Alur Penelitian.....	27
3.3.1.	Identifikasi Masalah.....	27
3.3.2.	Studi Literatur	28
3.3.3.	Tahap Pengujian.....	28
3.3.4.	Tahap Analisis <i>Malware</i>	33
3.3.5.	Dokumentasi	35
BAB IV HASIL DAN PEMBAHASAN		36
4.1.	Hasil Pengambilan Data	36
4.2.	Hasil Analisis Otomatis Menggunakan MoBSF	40
4.2.1.	Security Score	40
4.2.2.	Permission Analysis.....	41
4.2.3.	Source Code Analysis	49
4.3.	Hasil Analisis Manual Menggunakan JADX	51
4.3.1.	Permission Analysis.....	51
4.3.2.	META-INF.....	52
4.3.3.	Source Code Analysis	53
4.4.	Perbandingan Otomatis MoBSF dan Manual JADX	59
BAB V PENUTUP.....		62
5.1.	Kesimpulan.....	62
5.2.	Saran	62
DAFTAR PUSTAKA		64
LAMPIRAN.....		69

DAFTAR GAMBAR

Gambar 3.1. Diagram Alur Penelitian.....	27
Gambar 3. 2. <i>Exploit</i> Pada Meterpreter.....	30
Gambar 3. 3. Tahap MobSF.....	33
Gambar 3. 4. Tahap <i>Reverse Engineering</i> [1].....	34
Gambar 4. 1. Instalasi Pada Versi Android 13.....	37
Gambar 4. 2. Instalasi Rat.apk.....	37
Gambar 4. 3. <i>Security Score</i> TurboOri.apk.....	40
Gambar 4. 4. <i>Finding Severity</i> TurboOri.apk.....	41
Gambar 4. 5. <i>Security Score</i> Turbo.apk.....	41
Gambar 4. 6. <i>Finding Severity</i> Turbo.apk.....	41
Gambar 4. 7. <i>Permission</i> TurboOri.apk.....	42
Gambar 4. 8. <i>Permission</i> Turbo.apk.....	42
Gambar 4. 9. <i>Source Code Analysis</i> TurboOri.apk.....	49
Gambar 4. 10. <i>Source Code Analysis</i> Turbo.apk.....	50
Gambar 4. 11. <i>Code Analysis</i> TurboOri.apk.....	50
Gambar 4. 12. <i>Code Analysis</i> Turbo.apk.....	51
Gambar 4. 13. <i>Permission</i> TurboOri.apk.....	52
Gambar 4. 14. <i>Permission</i> Turbo.apk.....	52
Gambar 4. 15. Penambahan AndroidManifest.xml.....	53
Gambar 4. 16. <i>Import Statement</i> Turbo.apk.....	54
Gambar 4. 17. Memanggil <i>class</i> Dzlنز.....	55
Gambar 4. 18. <i>Source Code</i> aplikasi TurboOri.apk.....	55
Gambar 4. 19. <i>Source Code</i> Aplikasi Turbo.apk.....	55
Gambar 4. 20. <i>Class</i> Dzlنز memulai <i>Service</i>	56
Gambar 4. 21. <i>Class</i> Dzlنز mengirimkan Intent.....	56

DAFTAR TABEL

Tabel 3.1. Kebutuhan Perangkat Keras	25
Tabel 3.2. Kebutuhan Perangkat Lunak	26
Tabel 4. 1. Hasil Pengambilan Data <i>Malware</i>	38
Tabel 4. 2. Tabel Penambahan <i>Permission</i>	43
Tabel 4. 3. Tabel Perbandingan Hasil Analisis	60

DAFTAR SINGKATAN

MOBSF	= <i>Mobile Security Framework</i>
APK	= <i>Android Package Kit</i>
RAT	= <i>Remote Access Trojan</i>
TCP	= <i>Transmission Control Protocol</i>
HTML	= <i>HyperText Markup Language</i>
URL	= <i>Uniform Resource Locator</i>
SET	= <i>Social Engineering Toolkit</i>
ARP	= <i>Address Resolution Protocol</i>
XML	= <i>Extensible Markup Language</i>
API	= <i>Application Programming Interface</i>
Stdapi	= <i>Standard Application Programming Interface</i>
DEX	= <i>Dalvik Executable Format</i>
GPS	= <i>Global Positioning System</i>
ADB	= <i>Android Debug Bridge</i>
AES	= <i>Advanced Encryption Standard</i>
HTTP	= <i>Hypertext Transfer Protocol</i>
SSL/TLS	= <i>Secure Sockets Layer/Transport Layer Security</i>

DAFTAR LAMPIRAN

Lampiran 1. Pengiriman Aplikasi Melalui ADB	69
Lampiran 2. Proses Injeksi <i>Malware</i> Backdoor-apk.....	69
Lampiran 3. <i>Permission</i> MobSF Pada Aplikasi Sebelum Disisipi <i>Backdoor</i>	70
Lampiran 4. <i>Permission</i> MobSF Pada Aplikasi Setelah Disisipi <i>Backdoor</i>	70
Lampiran 5. <i>Permission</i> JADX Pada Aplikasi Sebelum Disisipi <i>Backdoor</i>	71
Lampiran 6. <i>Permission</i> Pada Aplikasi Setelah Disisipi <i>Backdoor</i>	71
Lampiran 7. Perubahan CERT.SF Menjadi SIGNING.SF	72
Lampiran 8. Perubahan Isi MANIFEST.SF	72
Lampiran 9. File Dzlz	72
Lampiran 10. File Lpmtc.....	73
Lampiran 11. File Hsfoy	73
Lampiran 12. File Kfyt.....	75
Lampiran 13. File <i>Main Activity</i> Rat.apk	83
Lampiran 14. File <i>Main Broadcast Receiver</i> Rat.apk.....	83
Lampiran 15. File <i>Main Service</i> Rat.apk	83
Lampiran 16. File <i>Payload</i> Rat.apk	84
Lampiran 17. Menu Meterpreter	92
Lampiran 18. Hasil Pengambilan Data Meterpreter	93
Lampiran 19. Hasil Analisis Manual JADX	100
Lampiran 20. Cek <i>Plagiarisme</i>	115