

**ANALISIS SERANGAN *FILELESS MALWARE* PADA LINUX
BERBASIS *LINUX SECURITY MODULE* (LSM)
(Studi Kasus Aplikasi Web Berbasis PHP)**

TUGAS AKHIR



**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

**ANALISIS SERANGAN *FILELESS MALWARE* PADA LINUX
BERBASIS *LINUX SECURITY MODULE* (LSM)
(Studi Kasus Aplikasi Web Berbasis PHP)**

Tugas Akhir

Skema Skripsi

Tugas Akhir diajukan sebagai salah satu persyaratan memperoleh gelar Sarjana

Teknik pada Program Studi Teknik Informatika



Zacky Santoso

2101020123

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2026**

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “Analisis Serangan *Fileless Malware* Pada Linux Berbasis *Linux Security Module* (Lsm) (Studi Kasus Aplikasi Web Berbasis Php)” adalah benar karya saya dengan arahan dari komisi pembimbing dan belum diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir skripsi ini.

Apabila di kemudian hari terbukti pernyataan saya tidak benar dan melanggar peraturan yang berlaku dalam karya tulis dan hak intelektual, maka saya bersedia ijazah yang telah saya terima untuk ditarik kembali oleh Universitas Maritim Raja Ali Haji dan menerima sanksi lainnya sesuai dengan peraturan yang berlaku. Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Universitas Maritim Raja Ali Haji.

Tanjungpinang, Januari 2026



Zacky Santoso
2101020123



© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2026

Hak Cipta Dilindungi Undang- Undang

Dilarang mengutip sebagian atau seluruh karya tulis ini tanpa mencantumkan atau menyebutkan sumbernya. Pengutipan hanya untuk kepentingan pendidikan, penelitian, penulisan karya ilmiah, penyusunan laporan, penulisan kritik, atau tinjauan suatu masalah; dan pengutipan tersebut tidak merugikan kepentingan Universitas Maritim Raja Ali Haji.

Dilarang mengumumkan dan memperbanyak sebagian atau seluruh karya tulis ini dalam bentuk apapun tanpa izin Universitas Maritim Raja Ali Haji.



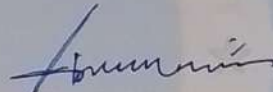
HALAMAN PERSETUJUAN

Judul : Analisis Serangan *Fileless Malware* Pada Linux
Berbasis *Linux Security Module* (LSM)
(Studi Kasus Aplikasi Web Berbasis PHP)
Nama : Zacky Santoso
NIM : 2101020123
Program Studi : Teknik Informatika
Tanggal Persetujuan : Januari 2026

Disetujui oleh,
Komisi Pembimbing



Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.
(Ketua)



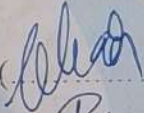
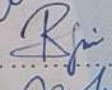
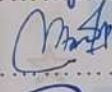
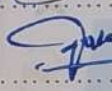
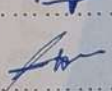
Berta Erwin Slam, S.T., M.Kom.
(Anggota)

HALAMAN PENGESAHAN

Judul : Analisis Serangan *Fileless Malware* Pada Linux
Berbasis *Linux Security Module* (LSM) (Studi
Kasus Aplikasi Web Berbasis Php)
Nama : Zacky Santoso
NIM : 2101020123

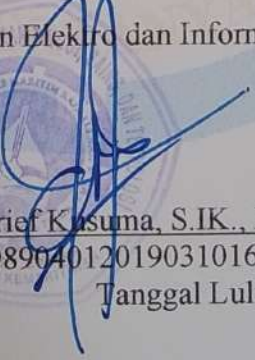
Telah berhasil dipertahankan di hadapan Komisi Penguji sebagai bagian persyaratan yang diperlukan dalam memperoleh gelar Sarjana Teknik pada Program Studi Teknik Informatika, Jurusan Teknik Elektro Dan Informatika, Fakultas Teknik dan Teknologi Kemaritiman, Universitas Maritim Raja Ali Haji.

KOMISI PENGUJI

Ketua	: Tekad Matulatan, S.Kom., M.Info., Tech.	()
Anggota I	: Rifaldi Herikson, M.Kom.	()
Anggota II	: Marisha Pertiwi, S.Tr. Kom., M.Kom.	()
Anggota III	: Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D.	()
Anggota IV	: Berta Erwin Slam, S.T., M.Kom.	()

Mengetahui,

Ketua Jurusan Elektro dan Informatika


Hollanda Arief Kusuma, S.IK., M.Si

NIP. 198904012019031016

Tanggal Ujian: 14 Januari 2026

Tanggal Lulus:

2026

PRAKATA

Puji syukur kehadiran Allah *subhanahu wa ta'ala* atas rahmat dan karunia-Nya, sehingga Skripsi Tugas Akhir dengan judul “**ANALISIS SERANGAN FILELESS MALWARE PADA LINUX BERBASIS LINUX SECURITY MODULE (LSM) (Studi Kasus Aplikasi Web Berbasis PHP)**” ini dapat diselesaikan.

Terima kasih penulis ucapkan kepada Bapak Hendra Kurniawan, S.Kom., M.Sc.Eng., Ph.D. dan Bapak Berta Erwin Slam, S.T., M.Kom. yang telah banyak memberi saran. Di samping itu, Ungkapan terima kasih juga disampaikan kepada ayah, ibu, serta seluruh keluarga, atas segala doa dan kasih sayangnya. serta kepada teman-teman yang selalu memberikan semangat dan bantuan selama penelitian ini berlangsung.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk perbaikan di masa mendatang. Semoga skripsi ini dapat memberikan manfaat bagi penulis sendiri maupun bagi pembaca yang berminat dalam bidang keamanan sistem operasi Linux.

Tanjungpinang, Januari 2026



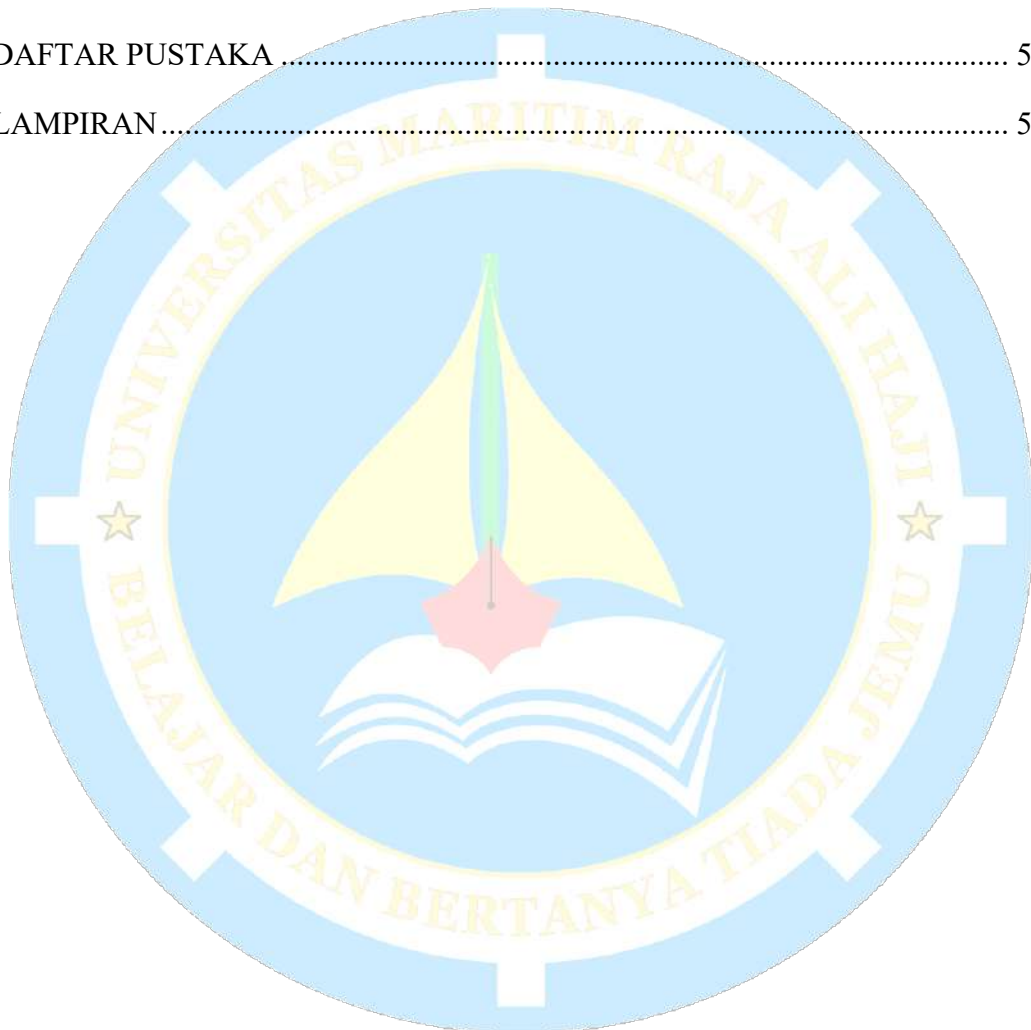
Zacky Santoso

DAFTAR ISI

HALAMAN PERSETUJUAN.....	iv
HALAMAN PENGESAHAN.....	v
ABSTRAK	vi
ABSTRACT.....	vii
PRAKATA.....	viii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN.....	xiv
BAB I PENDAHULUAN	1
A. Latar Belakang	1
B. Perumusan Masalah	3
C. Batasan Penelitian	3
D. Tujuan Penelitian	4
E. Manfaat Penelitian	4
BAB II KAJIAN LITERATUR	6
A. Tinjauan Pustaka	6
B. Landasan Teori.....	11
1. <i>Fileless malware</i>	11
2. Sistem Operasi Linux dan Model Keamanan <i>Default</i>	12
3. <i>Linux Security Module (LSM)</i>	13
4. SELinux (<i>Security-Enhanced Linux</i>).....	14
5. Landlock (<i>Sandbox</i> berbasis <i>Whitelist</i>).....	14
6. Aplikasi Web PHP.....	15

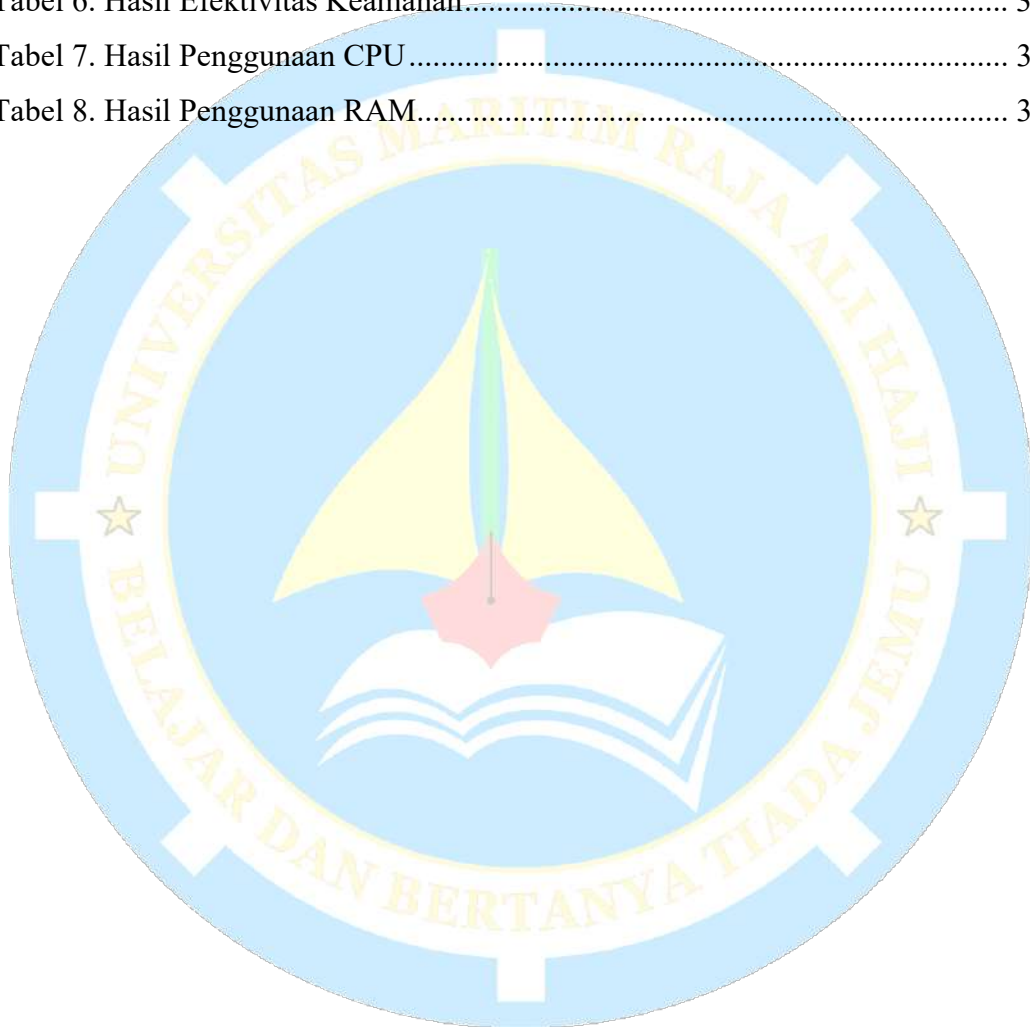
BAB III METODE PENELITIAN.....	16
A. Waktu dan Tempat Penelitian	16
B. Bahan dan Alat.....	16
C. Prosedur Pelaksanaan Penelitian.....	17
1. Lingkungan Pengujian	17
2. Skenario Serangan <i>Fileless malware</i>	18
3. Tahap Rekognisi dan Identifikasi Kerentanan.....	18
4. Pengujian Skenario	19
5. Pemantauan dan Pengumpulan Data.....	19
6. Diagram Alur Penelitian	20
D. Perancangan Sistem	21
1. Arsitektur Lingkungan Sistem	21
2. Desain Kondisi Pengujian.....	22
3. ★ Mekanisme Keamanan.....	22
4. Alur Serangan Pada Sistem.....	22
5. Pemantauan dan Pencatatan Data	23
6. Diagram Arsitektur Sistem	23
E. Analisis Data	24
1. Analisis Performa Sistem (CPU dan RAM)	25
2. Analisis Perbandingan Pola Serangan	26
3. Penyajian Data	26
BAB IV HASIL DAN PEMBAHASAN	27
A. HASIL	27
1. Hasil Efektivitas Keamanan.....	27
2. Hasil Efisiensi Sistem	31
3. Hasil Efisiensi Sistem Serangan Bersamaan.....	43

B. Pembahasan.....	45
1. Analisis Efektivitas Keamanan.....	45
2. Analisis Efisiensi Sistem	46
BAB V SIMPULAN DAN SARAN	50
A. Simpulan	50
B. Saran.....	50
DAFTAR PUSTAKA	52
LAMPIRAN.....	55



DAFTAR TABEL

Tabel 1. Penelitian Yang Pernah Dilakukan	6
Tabel 2. Bahan yang digunakan	16
Tabel 3. Alat yang digunakan	16
Tabel 4. Skenario Serangan.....	18
Tabel 5. Kondisi Tanpa <i>Linux Security Module (Baseline)</i>	28
Tabel 6. Hasil Efektivitas Keamanan.....	30
Tabel 7. Hasil Penggunaan CPU	31
Tabel 8. Hasil Penggunaan RAM.....	32



DAFTAR GAMBAR

Gambar 1. Contoh Serangan <i>Fileless Malware</i> (Sumber :[21])	12
Gambar 2. Arsitektur Umum <i>Linux Security Module</i> (LSM)	13
Gambar 3. Diagram Mekanisme Kerja SELinux	14
Gambar 4. Diagram Alur Penelitian.....	20
Gambar 5. Arsitektur Sistem.....	23
Gambar 6. Log SELinux	29
Gambar 7. Log Landlock	29
Gambar 8. Grafik Performa CPU & RAM skenario <i>shutdown</i>	34
Gambar 9. Grafik Performa CPU & RAM skenario <i>Reverse Shell</i>	35
Gambar 10. Grafik Performa CPU & RAM skenario <i>Credential Exfiltration</i>	36
Gambar 11. Grafik Performa CPU & RAM skenario <i>Defacement</i>	37
Gambar 12. Grafik Performa CPU & RAM skenario <i>Defense Evasion</i>	38
Gambar 13. Grafik Performa CPU & RAM skenario <i>Log Clearing</i>	39
Gambar 14. Grafik Performa CPU & RAM skenario <i>Kernel Reconnaissance</i>	40
Gambar 15. Grafik Performa CPU & RAM skenario <i>Bind Shell</i>	41
Gambar 16. Grafik Performa CPU & RAM skenario <i>Environment Variable Theft</i>	42
Gambar 17. Grafik Performa CPU & RAM skenario <i>Configuration Injection</i>	43
Gambar 18. Grafik Perbandingan Performa CPU & RAM Serangan Bersamaan	44

DAFTAR LAMPIRAN

Lampiran 1. Hasil Tahapan Rekognisi.....	55
Lampiran 2. <i>Shutdown</i>	55
Lampiran 3. <i>Reverse Shell</i>	56
Lampiran 4. <i>Credential Exfiltration</i>	56
Lampiran 5. <i>Defacement</i>	57
Lampiran 6. <i>Defense Evasion</i>	57
Lampiran 7. <i>Log Clearing</i>	57
Lampiran 8. <i>Kernel Reconnaissance</i>	58
Lampiran 9. <i>Bind Shell</i>	58
Lampiran 10. <i>Environment Variable Theft</i>	58
Lampiran 11. <i>Configuration Injection</i>	58

