

**ANALISIS SERANGAN *FILELESS MALWARE* PADA SISTEM
OPERASI LINUX BERBASIS SELINUX DAN APPARMOR
(Studi Kasus Aplikasi Web Berbasis PHP)**

TUGAS AKHIR



Azel Fahrezi

NIM. 2101020034

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2025**

**ANALISIS SERANGAN *FILELESS MALWARE* PADA SISTEM
OPERASI LINUX BERBASIS SELINUX DAN APPARMOR
(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



Azel Fahrezi

NIM. 2101020034

**PROGRAM STUDI TEKNIK INFORMATIKA
JURUSAN TEKNIK ELEKTRO DAN INFORMATIKA
FAKULTAS TEKNIK DAN TEKNOLOGI KEMARITIMAN
UNIVERSITAS MARITIM RAJA ALI HAJI
TANJUNGPINANG
2025**

PERNYATAAN MENGENAI TUGAS AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa tugas akhir berjudul “Analisis Serangan *Fileless Malware* pada Sistem Operasi Linux Berbasis SELinux dan AppArmor (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, Oktober 2025



Azel Fahrezi
NIM 2101020034



© Hak Cipta Milik Universitas Maritim Raja Ali Haji, Tahun 2021

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 Sistem Operasi Linux Berbasis SELinux dan AppArmor (Studi Kasus Aplikasi Web Berbasis PHP)

Nama : Azel Fahrezi

NIM : 2101020034

Program Studi : Teknik Informatika

Tanggal Persetujuan : 24 Oktober 2025

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 Sistem Operasi Linux Berbasis SELinux dan AppArmor (Studi Kasus Aplikasi Web Berbasis PHP)

Nama : Azel Fahrezi

NIM : 2101020034

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	: Muhamad Radzi Rathomi, S.Kom., M.Cs.	(.....)
Anggota I	: Marisha Pertiwi, S.Tr.Kom., M.Kom.	(.....)
Anggota II	: Rifaldi Herikson, S.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 Teknik Elektro dan Informatika

Hollanda Arief Kusuma, S.IK., M.Si.
NIP. 198904012019031016

Tanggal Ujian: 20 November 2025

Tanggal Lulus:

PRAKATA

Puji dan syukur dipanjatkan kepada Allah *subhanahu wa ta'ala* atas segala karunia-Nya sehingga laporan tugas akhir ini berhasil diselesaikan. Tema yang dipilih dalam tugas akhir yang akan dilaksanakan pada bulan November 2025 ini, dengan judul **“Analisis Serangan *Fileless Malware* pada Sistem Operasi Linux Berbasis SELinux dan AppArmor (Studi Kasus Aplikasi Web Berbasis PHP)”**.

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. Ungkapan terima kasih juga disampaikan kepada ayah, ibu, serta seluruh keluarga, atas segala doa dan kasih sayangnya.

Semoga laporan tugas akhir ini bermanfaat.

Tanjungpinang, Oktober 2025



Azel Fahrezi

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.....	xvi
BAB I PENDAHULUAN.....	1
A. Latar Belakang.....	1
B. Perumusan Masalah.....	2
C. Batasan Penelitian.....	3
D. Tujuan Penelitian.....	4
E. Manfaat Penelitian.....	4
BAB II KAJIAN LITERATUR.....	6
A. Tinjauan Pustaka.....	6
B. Landasan Teori.....	16
1. Prinsip Keamanan Sistem Operasi Linux.....	16
2. <i>Fileless Malware</i>	17
3. Modul Keamanan Linux.....	18
4. Metode Analisis <i>Malware</i>	18
5. Ancaman pada Aplikasi Web PHP.....	19

BAB III METODE PENELITIAN.....	20
A. Waktu dan Tempat Penelitian.....	20
B. Bahan dan Alat.....	20
C. Prosedur Pelaksanaan Penelitian.....	21
1. Rancangan Percobaan.....	21
2. Variabel Penelitian.....	22
3. Jenis Data dan Satuan Pengukuran.....	22
4. Diagram Alir Penelitian.....	22
D. Perancangan Sistem.....	23
1. Arsitektur Penelitian.....	23
2. Rancangan Serangan <i>Fileless Malware</i>	24
3. Rancangan Mekanisme Deteksi.....	25
4. Rancangan Pemantauan Performa.....	25
5. Diagram Arsitektur Sistem.....	25
E. Analisis Data.....	25
1. Analisis Efektivitas Deteksi dan Pencegahan.....	26
2. Analisis Dampak Performa Sistem.....	26
3. Teknik Penyajian Data.....	27
BAB IV HASIL DAN PEMBAHASAN.....	28
A. Hasil.....	28
1. Hasil Deteksi dan Pencegahan.....	28
1.1 Hasil Tanpa <i>Linux Security Module</i>	29
1.2 Hasil Deteksi SELinux.....	29
1.3 Hasil Deteksi AppArmor.....	30
2. Hasil Dampak Performa Sistem.....	31
2.1 Visualisasi Performa Skenario <i>System Shutdown</i>	33

2.2 Visualisasi Performa Skenario <i>Reverse Shell</i>	36
2.3 Visualisai Performa Skenario <i>Log Clearing</i>	40
2.4 Performa Skenario <i>Kernel Reconnaissance</i>	43
2.5 Performa Skenario <i>Environment Variable Theft</i>	46
2.6 Performa Skenario <i>Defense Evasion</i>	49
2.7 Performa Skenario <i>Defacement</i>	52
2.8 Performa Skenario <i>Credential Exfiltration</i>	55
2.9 Performa Skenario <i>Configuration Injection</i>	58
2.10 Performa Skenario <i>Bind Shell</i>	61
B. Pembahasan.....	65
1. Analisis Efektivitas Deteksi dan Pencegahan.....	65
2. Analisis Dampak Performa Sistem (Penggunaan CPU dan RAM).....	67
BAB V SIMPULAN DAN SARAN.....	70
A. Simpulan.....	70
B. Saran.....	71
DAFTAR PUSTAKA.....	73
LAMPIRAN.....	76

DAFTAR TABEL

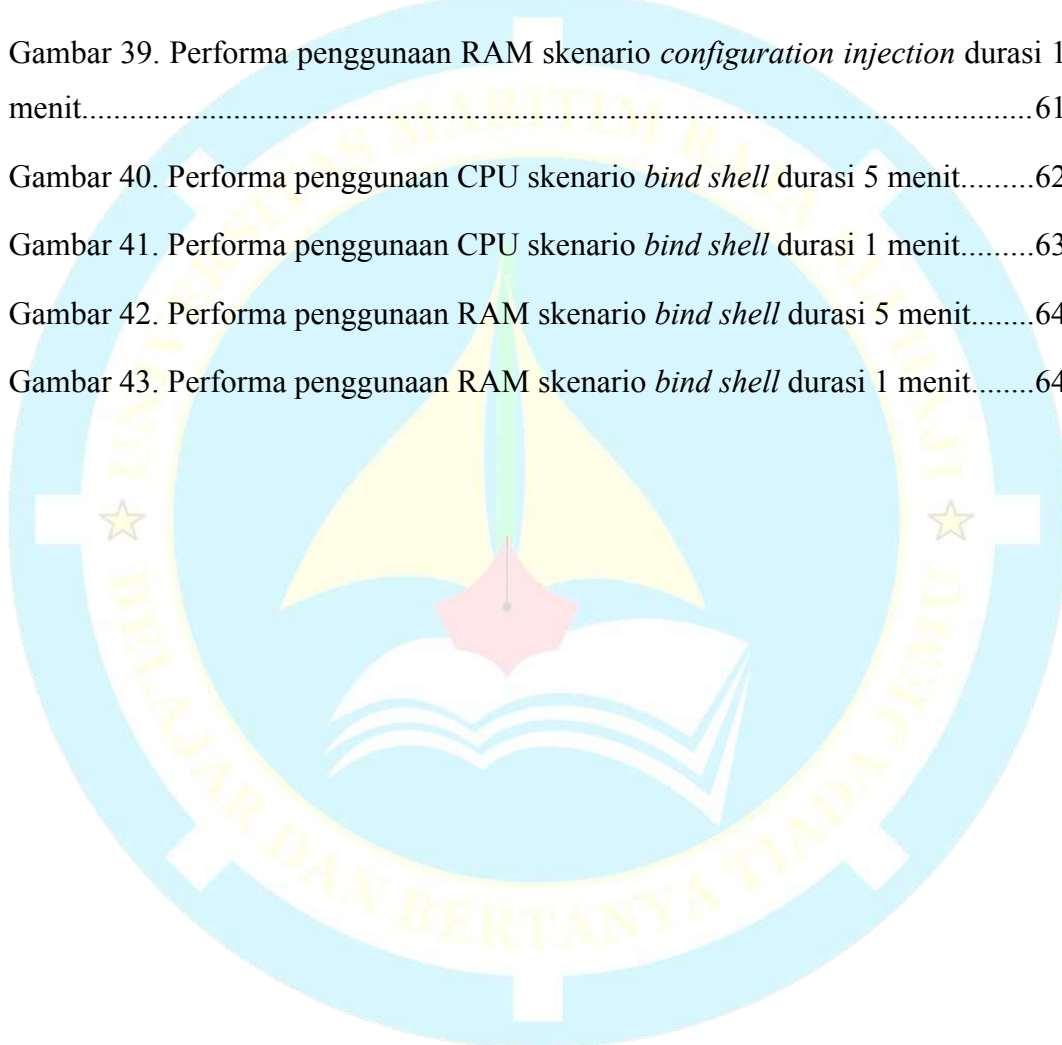
Tabel 1. Tinjauan Pustaka.....	6
Tabel 2. Bahan Data.....	20
Tabel 3. Alat Perangkat Keras.....	20
Tabel 4. Alat Perangkat Lunak.....	21
Tabel 5. Sepuluh skenario dan tujuan-nya.....	28
Tabel 6. Hasil Tanpa Linux Security Module.....	29
Tabel 7. Hasil dengan SELinux.....	29
Tabel 8. Hasil dengan AppArmor.....	30
Tabel 9. Rata-rata Penggunaan CPU (%) Durasi 5 menit.....	31
Tabel 10. Rata-rata Penggunaan CPU (%) Durasi 1 menit.....	31
Tabel 11. Rata-rata Penggunaan Memori Aktif (Memory <i>Used</i> , %) Durasi 5 menit.....	32
Tabel 12. Rata-rata Penggunaan Memori Aktif (Memory <i>Used</i> , %) Durasi 1 menit.....	32

DAFTAR GAMBAR

Gambar 1. Contoh serangan <i>fileless malware</i> (Sumber : [8]).....	17
Gambar 2. Tahapan penelitian.....	23
Gambar 3. Diagram arsitektur.....	25
Gambar 4. Performa penggunaan CPU skenario <i>system shutdown</i> durasi 5 menit.....	34
Gambar 5. Performa penggunaan CPU skenario <i>system shutdown</i> durasi 1 menit.....	34
Gambar 6. Performa penggunaan RAM skenario <i>system shutdown</i> durasi 5 menit	35
Gambar 7. Performa penggunaan RAM skenario <i>system shutdown</i> durasi 1 menit	36
Gambar 8. Performa penggunaan CPU skenario <i>reverse shell</i> durasi 5 menit.....	37
Gambar 9. Performa penggunaan CPU skenario <i>reverse shell</i> durasi 1 menit.....	38
Gambar 10. Performa penggunaan RAM skenario <i>reverse shell</i> durasi 5 menit.....	38
Gambar 11. Performa penggunaan RAM skenario <i>reverse shell</i> durasi 1 menit.....	39
Gambar 12. Performa penggunaan CPU skenario <i>log clearing</i> durasi 5 menit.....	40
Gambar 13. Performa penggunaan CPU skenario <i>log clearing</i> durasi 1 menit.....	41
Gambar 14. Performa penggunaan RAM skenario <i>log clearing</i> durasi 5 menit.....	42
Gambar 15. Performa penggunaan RAM skenario <i>log clearing</i> durasi 1 menit.....	42
Gambar 16. Performa penggunaan CPU skenario <i>kernel reconnaissance</i> durasi 5 menit.....	44
Gambar 17. Performa penggunaan CPU skenario <i>kernel reconnaissance</i> durasi 1 menit.....	44
Gambar 18. Performa penggunaan RAM skenario <i>kernel reconnaissance</i> durasi 5 menit.....	45
Gambar 19. Performa penggunaan RAM skenario <i>kernel reconnaissance</i> durasi 1 menit.....	46

Gambar 20. Performa penggunaan CPU skenario <i>environment variable theft</i> durasi 5 menit.....	47
Gambar 21. Performa penggunaan CPU skenario <i>environment variable theft</i> durasi 1 menit.....	48
Gambar 22. Performa penggunaan RAM skenario <i>environment variable theft</i> durasi 5 menit.....	48
Gambar 23. Performa penggunaan RAM skenario <i>environment variable theft</i> durasi 1 menit.....	49
Gambar 24. Performa penggunaan CPU skenario <i>defense evasion</i> durasi 5 menit	50
Gambar 25. Performa penggunaan CPU skenario <i>defense evasion</i> durasi 1 menit	51
Gambar 26. Performa penggunaan RAM skenario <i>defense evasion</i> durasi 5 menit	51
Gambar 27. Performa penggunaan RAM skenario <i>defense evasion</i> durasi 1 menit	52
Gambar 28. Performa penggunaan CPU skenario <i>defacement</i> durasi 5 menit.....	53
Gambar 29. Performa penggunaan CPU skenario <i>defacement</i> durasi 1 menit.....	54
Gambar 30. Performa penggunaan RAM skenario <i>defacement</i> durasi 5 menit.....	54
Gambar 31. Performa penggunaan RAM skenario <i>defacement</i> durasi 1 menit.....	55
Gambar 32. Performa penggunaan CPU skenario <i>credential exfiltration</i> durasi 5 menit.....	56
Gambar 33. Performa penggunaan CPU skenario <i>credential exfiltration</i> durasi 1 menit.....	57
Gambar 34. Performa penggunaan RAM skenario <i>credential exfiltration</i> durasi 5 menit.....	57
Gambar 35. Performa penggunaan RAM skenario <i>credential exfiltration</i> durasi 1 menit.....	58

Gambar 36. Performa penggunaan CPU skenario <i>configuration injection</i> durasi 5 menit.....	59
Gambar 37. Performa penggunaan CPU skenario <i>configuration injection</i> durasi 1 menit.....	60
Gambar 38. Performa penggunaan RAM skenario <i>configuration injection</i> durasi 5 menit.....	60
Gambar 39. Performa penggunaan RAM skenario <i>configuration injection</i> durasi 1 menit.....	61
Gambar 40. Performa penggunaan CPU skenario <i>bind shell</i> durasi 5 menit.....	62
Gambar 41. Performa penggunaan CPU skenario <i>bind shell</i> durasi 1 menit.....	63
Gambar 42. Performa penggunaan RAM skenario <i>bind shell</i> durasi 5 menit.....	64
Gambar 43. Performa penggunaan RAM skenario <i>bind shell</i> durasi 1 menit.....	64



DAFTAR LAMPIRAN

Lampiran 1. <i>System Shutdown</i>	76
Lampiran 2. <i>Reverse Shell</i>	76
Lampiran 3. <i>Log Clearing</i>	76
Lampiran 4. <i>Kernel Reconnaissance</i>	77
Lampiran 5. <i>Environment Variable Theft</i>	77
Lampiran 6. <i>Defense Evasion</i>	78
Lampiran 7. <i>Defacement</i>	78
Lampiran 8. <i>Credential Exfiltration</i>	79
Lampiran 9. <i>Configuration Injection</i>	79
Lampiran 10. <i>Bind Shell</i>	79
Lampiran 11. Kode Sumber Target Rentan (vuln.php).....	80