ANALISIS PERBEDAAN METODE PENCEGAHAN RANSOMWARE PADA PFSENSE DENGAN SNORT IDS/IPS DAN ANTIVIRUS AVAST

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

ROCHMAT PRAMUDYA

21.11.4226

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

ANALISIS PERBEDAAN METODE PENCEGAHAN RANSOMWARE PADA PFSENSE DENGAN SNORT IDS/IPS DAN ANTIVIRUS AVAST

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Informatika

disusun oleh

ROCHMAT PRAMUDYA

21.11.4226

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2025

HALAMAN PERSETUJUAN

SKRIPSI

ANALISIS PERBEDAAN METODE PENCEGAHAN RANSOMWARE PADA PFSENSE DENGAN SNORT IDS/IPS DAN ANTIVIRUS AVAST

yang disusun dan diajukan oleh

Rochmat Pramudya

21.11.4226

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal

Dosen Pembimbing,

(Sudarmawan, S.T., M.T.)
NIK. 190302035

HALAMAN PENGESAHAN

SKRIPSI

ANALISIS PERBEDAAN METODE PENCEGAHAN RANSOMWARE PADA PFSENSE DENGAN SNORT IDS/IPS DAN ANTIVIRUS AVAST

yang disusun dan diajukan oleh

Rochmat Pramudya

21.11.4226

Telah dipertahankan di depan Dewan Penguji
pada tanggal Kamis, 22 Mei 2025

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Rizqi Sukma Kharisma, M.Kom. **NIK. 190302215**	
Yudi Sutanto, S.Kom., M.Kom. **NIK. 190302039**	
Arifiyanto Hadinegoro, S.Kom. M.T **NIK. 190302289**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal Kamis, 22 Mei 2025

DEKAN FAKULTAS ILMU KOMPUTER

Prof. Dr. Kusrini, M.Kom
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Rochmat Pramudya
NIM : 21.11.4226

Menyatakan bahwa Skripsi dengan judul berikut:

ANALISIS PERBEDAAN METODE PENCEGAHAN RANSOMWARE PADA PFSENSE DENGAN SNORT IDS/IPS DAN ANTIVIRUS AVAST

Dosen Pembimbing : Sudarmawan, S.T., M.T.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari 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 tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian 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.

Yogyakarta, Kamis, 22 Mei 2025

Yang Menyatakan,

Rochmat Pramudya

HALAMAN PERSEMBAHAN

Dengan rasa syukur yang paling dalam, skripsi ini saya persembahkan kepada:

1. Tuhan Yang Maha Esa Allah SWT
2. Kedua orang tua tercinta, Bapak Wagirin dan Ibu Kartiyemi yang telah memberikan doa terbaik dan telah memberikan support terbaik kepada saya.
3. Bapak Sudarmawan selaku dosen pembimbing saya, yang selalu membimbing dan memberikan saran dalam penulisan skripsi ini.
4. Segenap Civitas akademik, Bapak/Ibu dosen Program Studi Teknik informatika Universitas Amikom Yogyakarta.
5. Teman-teman sepermainan game online, yang selalu membuat saya selalu berpikir fresh dan tidak mudah depresi, walaupun selalu kalah.
6. Teman-teman dari kelas 21-IF06
7. Seluruh Mahasiswa Informatika 2021 Universitas Amikom Yogyakarta
8. Almamater Tercinta Universitas Amikom Yogyakarta

KATA PENGANTAR

Puji syukur kehadirat Allah SWT atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi dengan judul *"ANALISIS PERBEDAAN METODE PENCEGAHAN RANSOMWARE PADA PFSENSE DENGAN SNORT IDS/IPS DAN ANTIVIRUS AVAST"*. Skripsi ini disusun sebagai salah satu syarat untuk menyelesaikan program studi S1 Informatika di Universitas Amikom Yogyakarta.

Penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada berbagai pihak yang telah memberikan dukungan, bimbingan, dan motivasi selama proses penyusunan skripsi ini. Secara khusus, ucapan terima kasih penulis sampaikan kepada:

1. Pak Sudarmawan, ST, MT. selaku Dosen Pembimbing, atas bimbingan, saran, dan arahan yang diberikan dalam proses penyusunan skripsi ini.
2. Bu Eli Pujastuti, M.Kom. selaku Ketua Program Studi Informatika Universitas Amikom Yogyakarta, atas dukungan dan fasilitas yang diberikan.
3. Tim Dosen Penguji, atas masukan dan kritik yang membangun untuk penyempurnaan skripsi ini.
4. Kedua orang tua tercinta, yang selalu memberikan semangat tanpa henti, doa yang tulus, dan cinta yang tak terhingga, sehingga penulis dapat melewati setiap tantangan dalam penyusunan skripsi ini.
5. Orang-orang sekitar, yang tanpa lelah menanyakan, “Skripsi kapan selesai?” atau “Mau lulus kapan?”—yang meski terkadang terasa seperti beban, pada akhirnya menjadi pemicu untuk menyelesaikan skripsi ini.

Yogyakarta, Kamis, 22 Mei 2025

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

C2	Command & Control
PC	Personal Computer
LAN	Local Area Network
TCP	Transmission Control Protocol
exe	Executable

DAFTAR ISTILAH

open-source	Perangkat lunak yang kode sumbernya tersedia secara bebas
siber	Segala hal yang berkaitan dengan dunia digital, komputer, dan jaringan internet.
heuristic detection	Mendeteksi ancaman baru atau tidak dikenal (seperti virus atau malware)mendeteksi ancaman baru atau tidak dikenal (seperti virus atau malware)
signature	Pola atau ciri khas spesifik yang digunakan untuk mengidentifikasi malware
Executable	File yang dapat dijalankan langsung oleh sistem operasi untuk memulai sebuah program atau instruksi tertentu.
Meterpreter	Framework Metasploit untuk mengendalikan sistem target secara jarak jauh setelah berhasil dieksploitasi.

INTISARI

Ancaman ransomware menjadi salah satu bentuk serangan siber yang paling merugikan dan berkembang pesat. Penelitian ini bertujuan untuk menganalisis efektivitas serta membandingkan metode pencegahan ransomware menggunakan pfSense dengan Snort IDS/IPS dan Antivirus Avast. Penelitian dilakukan melalui simulasi serangan crypto ransomware yang melibatkan koneksi reverse shell dan distribusi file malware, dengan pengujian terhadap dua skenario sistem keamanan.

Hasil pengujian menunjukkan bahwa pfSense dengan Snort IDS/IPS mampu mendeteksi aktivitas jaringan mencurigakan secara real-time dan memblokir koneksi reverse shell sebelum malware aktif, menandakan efektivitas tinggi dalam pencegahan berbasis jaringan. Sementara itu, Antivirus Avast berhasil mendeteksi dan mengarantina file berbahaya setelah proses unduhan hampir selesai, yang menunjukkan pendekatan deteksi yang bersifat reaktif di sisi endpoint.

Kesimpulannya, pfSense dengan Snort lebih unggul dalam mencegah serangan sejak dini melalui jaringan, sedangkan Avast lebih efektif dalam menangani file berbahaya yang sudah masuk ke sistem. Untuk meningkatkan keamanan secara menyeluruh, kombinasi penggunaan keduanya direkomendasikan guna membentuk sistem pertahanan berlapis terhadap berbagai jenis serangan ransomware.

Kata kunci: pfSense, Snort IDS/IPS, Antivirus Avast, Keamanan Jaringan, Crypto Ransomware.

ABSTRACT

Ransomware has emerged as one of the most damaging and rapidly evolving forms of cyberattacks. This research aims to analyze and compare the effectiveness of ransomware prevention methods using pfSense with Snort IDS/IPS and Avast antivirus. The study involves simulated crypto ransomware attacks, including reverse shell connections and malware distribution, tested across two different security scenarios.

The results show that pfSense with Snort IDS/IPS successfully detects suspicious network activity in real time and blocks reverse shell connections before the malware becomes active, demonstrating high effectiveness in network-based prevention. On the other hand, Avast antivirus detects and quarantines a malicious file after the download is nearly complete, indicating a reactive detection approach at the endpoint level.

In conclusion, pfSense with Snort proves to be more effective in early detection and prevention of network-based attacks, while Avast is more capable of handling threats that reach the endpoint. For optimal protection, the combined use of both systems is recommended to establish a comprehensive layered defense against various types of ransomware attacks..

Keyword: *pfSense, Snort IDS/IPS, Avast Antivirus, Network Security, Crypto Ransomware.*