JURNAL PENELITIAN MULTIDISIPLIN BANGSA
e-ISSN : 3048-4251
Volume 2, No. 1, Tahun 2025
https://ejournal.amirulbangunbangsapublishing.com/index.php/jpnmb/index

Keamanan FTP Server Berbasiskan IPS Menggunakan Sistem Operasi Linux Ubuntu Versi 24.04

Tamsir Ariyadi[1], Muhammad Arya Nuriansyah[2], Eno Rahmadan[3], Deo Saputra[4]
[1,2,3,4] *Universitas Bina Darma, Sumatra Selatan, Indonesia*

Received : 17 Mei 2025, Revised : 19 Mei 2025, Published : 1 Juni 2025

Corresponding Author
Nama Penulis: Tamsir Ariyadi
E-mail: tamsirariyadi@binadarma.ac.id

Abstrak

Keamanan layanan File Transfer Protocol (FTP) menjadi tantangan penting dalam pengelolaan sistem informasi, terutama karena FTP secara default tidak mendukung enkripsi. Sistem operasi Linux Ubuntu 24.04 menyediakan lingkungan yang stabil dan aman untuk penerapan mekanisme pertahanan jaringan. Penelitian ini bertujuan untuk merancang dan mengimplementasikan sistem keamanan FTP server berbasis Intrusion Prevention System (IPS) menggunakan Fail2ban dan Suricata pada Ubuntu 24.04. Pengujian dilakukan dengan melakukan simulasi serangan brute-force, scanning, dan transfer file ilegal. Hasil menunjukkan bahwa IPS yang diterapkan dapat secara efektif mendeteksi dan mencegah ancaman terhadap FTP server. Penelitian ini mengacu pada dokumentasi resmi dan studi terdahulu dalam bidang keamanan jaringan.
Kata kunci - *FTP, IPS, Suricata, Fail2ban, Ubuntu 24.04, Keamanan jaringan.*

Abstract

File Transfer Protocol (FTP) service security is a major challenge in information system management, especially since FTP does not support encryption by default. The Linux Ubuntu 24.04 operating system provides a stable and secure environment for implementing network defense mechanisms. This study aims to design and implement an FTP server security system based on the Intrusion Prevention System (IPS) using Fail2ban and Suricata on Ubuntu 24.04. Testing was carried out by simulating brute-force attacks, scanning, and illegal file transfers. The results show that the implemented IPS can effectively detect and prevent threats to the FTP server. This study refers to official documentation and previous studies in the field of network security.
Keywords *- FTP, IPS, Suricata, Fail2ban, Ubuntu 24.04, Keamanan jaringan.*

How To Cite : *Ariyadi, T., Nuriansyah, M. A., Rahmadan, E., & Saputra, D. (2025). Keamanan FTP Server Berbasiskan IPS Menggunakan Sistem Operasi Linux Ubuntu Versi 24.04. Jurnal Penelitian Multidisiplin Bangsa, 2(1), 49–55. https://doi.org/10.59837/jpnmb.v2i1.428*

PENDAHULUAN

Perkembangan teknologi informasi yang pesat menuntut sistem informasi untuk senantiasa aman, cepat, dan andal, terutama dalam proses pertukaran data. Salah satu protokol yang masih banyak digunakan untuk proses transfer file adalah File Transfer Protocol (FTP). Meskipun fungsionalitas FTP sangat dibutuhkan dalam berbagai sektor, protokol ini memiliki kelemahan utama, yaitu tidak menyediakan enkripsi data secara default, sehingga menjadi celah potensial bagi pelaku kejahatan siber.(Widodo Purbo et al., 2019)

FTP menjadi sasaran umum serangan seperti brute-force login, sniffing, port scanning, hingga akses tidak sah terhadap direktori dan file server. Dalam lingkungan jaringan terbuka maupun internal, ancaman ini dapat berdampak serius terhadap kerahasiaan, integritas, dan ketersediaan data. Oleh karena itu, penting untuk menerapkan sistem pengamanan tambahan yang tidak hanya mendeteksi tetapi juga mencegah serangan siber secara otomatis. (Khadafi et al., 2019)

Salah satu pendekatan efektif yang digunakan dalam perlindungan layanan FTP adalah penerapan Intrusion Prevention System (IPS).(Silalahi & Kurniawan, 2023) IPS merupakan sistem keamanan aktif yang mampu mendeteksi pola serangan dan langsung memblokir aktivitas mencurigakan sebelum ancaman mencapai sistem target. Pada sistem operasi Linux Ubuntu versi 24.04 LTS, pengguna dapat mengintegrasikan perangkat lunak open-source seperti Fail2ban dan Suricata untuk membangun sistem IPS yang kuat dan efisien.(Suhendi & Cahyo, 2021)

Penelitian ini bertujuan untuk menerapkan dan menguji efektivitas sistem keamanan FTP berbasis IPS menggunakan Fail2ban dan Suricata di Ubuntu 24.04. Dengan pendekatan ini, diharapkan FTP server dapat memiliki lapisan pertahanan otomatis terhadap berbagai bentuk serangan siber umum, sekaligus menjadi referensi implementatif untuk institusi yang membutuhkan layanan transfer file yang aman dan handal.(Khadafi et al., 2021)

TINJAUAN PUSTAKA

File Transfer Protocol (FTP)

FTP merupakan salah satu protokol standar dalam jaringan komputer yang digunakan untuk mengirim dan menerima file melalui koneksi TCP/IP. Protokol ini menggunakan port 21 dan mendukung dua jenis mode koneksi, yaitu aktif dan pasif. Meskipun cukup banyak digunakan, FTP memiliki kelemahan besar karena tidak menyediakan enkripsi pada proses transmisi data, sehingga rawan terhadap penyadapan dan serangan seperti *man-in-the-middle*.(Zulkarnain, 2020)

Keamanan Jaringan dan Ancaman terhadap FTP

Karena kurangnya perlindungan autentikasi dan enkripsi, FTP menjadi sasaran utama berbagai serangan siber. Serangan umum yang sering terjadi mencakup *brute force*, *sniffing*, hingga *Denial of Service* (DoS).(Ariyadi et al., 2023) Untuk meningkatkan perlindungan, perlu diimplementasikan mekanisme keamanan tambahan seperti penggunaan firewall, VPN, serta sistem deteksi dan pencegahan intrusi (IDS/IPS) guna menjaga kerahasiaan dan keutuhan data .(Samsumar et al., 2024)

Intrusion Prevention System (IPS)

IPS adalah sistem keamanan yang bekerja secara aktif dalam memantau serta mencegah aktivitas mencurigakan atau berbahaya di jaringan. Teknologi ini menjalankan tugasnya dengan cara menganalisis lalu lintas jaringan dan mengambil tindakan berdasarkan aturan yang telah dikonfigurasi sebelumnya. Dalam pengelolaan FTP server, IPS sangat berperan dalam mengidentifikasi ancaman seperti serangan brute force, eksploitasi celah keamanan, maupun trafik mencurigakan lainnya.(Santoso, 2019)

Sistem Operasi Linux Ubuntu 24.04

Ubuntu 24.04 merupakan rilis terbaru dari sistem operasi Linux dengan dukungan jangka panjang (LTS) yang dikembangkan oleh Canonical. Sistem ini dikenal karena kestabilan, keamanan,

serta kemudahan pengelolaan server. Versi ini mendukung beragam fitur keamanan modern, seperti AppArmor, firewall dengan iptables atau nftables, serta mendukung integrasi dengan perangkat lunak IPS seperti Snort dan Suricata.(Ahmed et al., 2024)

Integrasi FTP, IPS, dan Ubuntu dalam Praktik Keamanan

Agar FTP server dapat beroperasi dengan aman, perlu dilakukan integrasi antara konfigurasi protokol yang baik dan sistem keamanan yang solid. IPS menyediakan perlindungan aktif terhadap serangan yang mengancam sistem. Penggunaan Ubuntu 24.04 sebagai platform server memberi keuntungan dalam hal kestabilan dan kemudahan integrasi dengan perangkat lunak keamanan, ditambah dukungan pembaruan sistem yang konsisten dan komunitas yang aktif.(Silalahi & Kurniawan, 2023)

METODE

Penelitian ini menggunakan pendekatan eksperimental yang berfokus pada instalasi, konfigurasi, dan pengujian sistem keamanan FTP server menggunakan Intrusion Prevention System (IPS) berbasis perangkat lunak open-source. Langkah-langkah dilakukan secara bertahap di lingkungan jaringan lokal dengan sistem operasi Linux Ubuntu 24.04 LTS.

Desain Penelitian

Desain penelitian terdiri dari tiga tahap utama:

1. Persiapan lingkungan uji coba, termasuk instalasi system operasi dan perangkat lunak yang dibutuhkan.
2. Implementasi system keamanan IPS, yang mencakup instalasi dan konfigurasi FTP server (vsftpd), fail2ban, dan sucirata.
3. Simulasi serangan dan evaluasi, dilakukan untuk mengukur efektivitas system dalam mendeteksi dan mencegah ancaman.

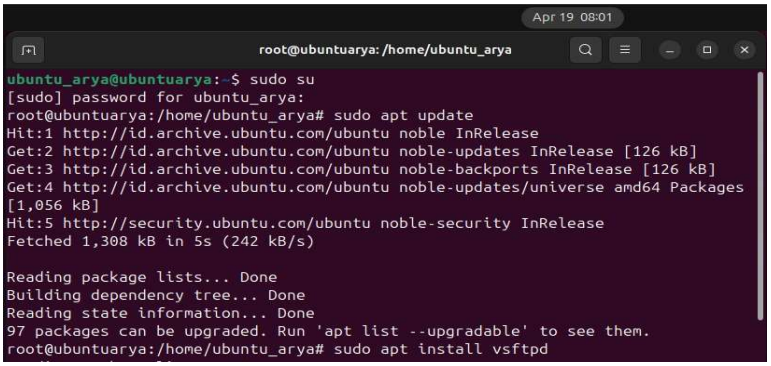
Lingkungan Implementasi

Spesifikasi system uji coba sebagai berikut:

1. System operasi ubuntu server 24.04 LTS.
2. Aplikasi FTP server vsftpd (Very Secure FTP daemon)
3. Aplikasi IPS (Fail2ban & Sucirata)
4. Jaringan local dengan Alamat IP kelas C (192.168.1.0/24)

Langkah-Langkah implementasi

1. Instalasi vsftpd
   - Melalui terminal ketik dengan perintah
     sudo apt update
     sudo apt install vsftpd



Gambar 1.
Tampilan install vsftpd

- Konfigurasi file /etc/vsftpd.conf untuk menonaktifkan akses anonim dan mengaktifkan chroot pada pengguna lokal.

```
root@ubuntuarya:/home/ubuntu_arya# sudo nano /etc/vsftpd.conf
root@ubuntuarya:/home/ubuntu_arya# sudo systemctl restart vsftp
```

Gambar 2.
konfigurasi vsftpd

2. Instalasi dan konfigurasi Fail2ban
   - Pemasangan
     sudo apt install fail2ban

```
root@ubuntuarya:/home/ubuntu_arya# sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Gambar 3.
install fail2ban

   - Konfigurasi di file /etc/fail2ban/jail.local untuk mendeteksi dan memblokir brute-force pada FTP.

```
root@ubuntuarya:/home/ubuntu_arya# sudo nano /etc/fail2ban/jail.local
root@ubuntuarya:/home/ubuntu_arya# sudo systemctl restart fail2ban
```

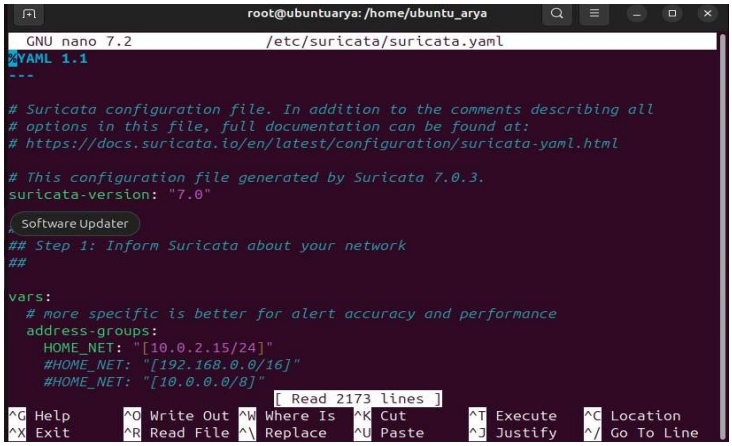
Gambar 4.
configurasi fail2ban

3. Instalasi dan konfigurasi Suricata
   - Pemasangan
     sudo apt install suricata

```
root@ubuntuarya:/home/ubuntu_arya# sudo apt install suricata -y
Reading package lists... Done
```

Gambar 5.
install suricata

   - Konfigurasi file suricata.yaml, terutama bagian HOME_NET, serta aktivasi rule yang relevan dengan protokol FTP.



Gambar 6.
konfigurasi HOME_NET

4. Simulasi serangan
    - Dilakukan dengan tools seperti Hydra (untuk brute-force), Nmap (untuk scanning), dan transfer file mencurigakan untuk memicu rule Suricata.
    - Observasi dilakukan terhadap log Fail2ban (/var/log/fail2ban.log) dan log Suricata (/var/log/suricata/alerts.json).

Teknik Analisis Data

Data dianalisis berdasarkan:

1. Waktu respon system terhadap serangan.
2. Ketepatan deteksi oleh system IPS terhadap aktivitas mencurigakan.
3. Komparasi kondisi server sebelum dan sesudah pengaktifan system IPS.
4. Jumlah serangan yang berhasil diblokir oleh Fail2ban dan Sucirata.

HASIL DAN PEMBAHASAN

Sistem keamanan IPS yang terdiri dari Fail2ban dan Suricata, dilakukan serangkaian pengujian dengan tujuan mengevaluasi efektivitas sistem dalam mendeteksi dan mencegah ancaman terhadap FTP server. Pengujian dilakukan dalam jaringan lokal menggunakan perangkat lunak serangan seperti Hydra dan Nmap untuk mensimulasikan skenario ancaman umum.

Implementasi Sistem

FTP server menggunakan vsftpd yang telah dikonfigurasi dengan pengamanan dasar seperti:

- Menonaktifkan akses anonym.
- Mengaktifkan chroot pada pengguna local.
- Mengatur hak akses file.

Kemudian system dilengkapi dengan:

- Fail2ban, untuk membaca log login FTP dan memblokir IP penyerang secara otomatis setelah sejumlah percobaan gagal.Suricata, untuk memantau lalu lintas jaringan secara real-time dan mendeteksi aktivitas mencurigakan berdasarkan signature rules.

Pengujian system keamanan

pengujian dilakukan melalui sekenario serangan umum terhadap layanan FTP. Adapun hasilnya sebagai berikut:

Simulasi serangan Brute-Force

- Skenario Menggunakan tool Hydra untuk mencoba ratusan kombinasi username dan password ke FTP server.
- Hasil Fail2ban berhasil mendeteksi login gagal secara berulang dan secara otomatis memblokir IP penyerang setelah 3 kali kegagalan.
- Waktu Respon <5 detik setelah batas maksimal percobaan.
- LogAktif /var/log/fail2ban.log

Simulasi port scanning dan service detection

- Skenario Menggunakan Nmap untuk melakukan scanning terhadap port FTP dan port terbuka lainnya.
- Hasil Suricata mendeteksi aktivitas scanning dan mencatatnya dalam log sebagai “TCP Port Scan Detected”.
- Jenis Deteksi Signature-based detection.
- Aksi Suricata tidak langsung memblokir, namun memberikan log peringatan untuk ditindaklanjuti.

Transfer file mencurigakan ke server FTP

- Skenario Upload file script PHP berisi kode shell sebagai simulasi payload berbahaya.
- Hasil Suricata memicu alert terhadap konten file yang mencurigakan berdasarkan rule yang aktif.
- Log aktif /var/log/suricata/fast.log dan /var/log/suricata/eve.json

Analilis efektivitas system IPS

Hasil dari masing-masing skenario dapat dirangkum pada tabel berikut:

Tabel 1.
Analilis efektivitas system IPS

Jenis ancaman	terdeteksi	Dicegah otomatis	Ips yang aktif
Brute-force login	Ya	Ya	Fail2ban
Port scanning	Ya	Tidak	Suricata
Transfer file berbahaya	Ya	Tidak (alert)	Suricata

- Fail2ban terbukti efektif untuk mencegah serangan berbasis login, berkat kemampuannya membaca log dan memblokir IP melalui iptables.
- Suricata sangat mampu dalam hal deteksi trafik berbahaya dan anomali, namun perlu dikombinasikan dengan sistem firewall atau script tambahan untuk bertindak sebagai IPS aktif (inline mode).

Pembahasan Penelitian

Hasil pengujian menunjukkan bahwa penerapan IPS berbasis open-source pada Linux Ubuntu 24.04 memberikan peningkatan signifikan terhadap keamanan layanan FTP. Fail2ban bekerja secara efektif sebagai IPS berbasis log, sementara Suricata memberikan deteksi real-time berbasis signature terhadap serangan jaringan. Kombinasi keduanya memberikan proteksi berlapis terhadap ancaman yang masuk ke FTP server.

Namun demikian, untuk menjadikan Suricata sebagai sistem yang tidak hanya mendeteksi tetapi juga memblokir, dibutuhkan konfigurasi tambahan menggunakan mode inline (IPS Mode) melalui NFQUEUE atau iptables/netfilter, yang belum diterapkan secara penuh dalam penelitian ini.

KESIMPULAN

Penerapan sistem IPS seperti Fail2ban dan Suricata pada FTP server di Linux Ubuntu 24.04 terbukti meningkatkan keamanan dari berbagai ancaman siber seperti brute-force dan port scanning. Kombinasi keduanya mampu mendeteksi dan mencegah serangan dengan lebih efisien, serta lebih mudah dioperasikan kedalam keamanan FTP server pada Linux Ubuntu.

DAFTAR PUSTAKA

Ahmed, A., Iqbal, M. T., & Jamil, M. (2024). *A Comparative Analysis of Media Players Power Consumption on Windows 11 and Ubuntu 24 . 04 . 1*. 1–5.

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno.Com*, *22*(2), 418–429. https://doi.org/10.33633/tc.v22i2.7562

Khadafi, S., Nurmuslimah, S., & Anggakusuma, F. K. (2019). Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server. *Jurnal Ilmiah NERO*, *4*(3), 181–188. https://nero.trunojoyo.ac.id/index.php/nero/article/view/137/127

Khadafi, S., Pratiwi, Y. D., & Alfianto, E. (2021). *Keamanan Ftp Server Berbasiskan Ids Dan Ips*. *6*(1), 11–24.

Samsumar, L. D., Imran, B., Efendi, M. M., & Muslim, R. (2024). *Optimalisasi Keamanan Web Server Ubuntu dengan Teknologi IPS Berbasis Iptables*. *9*(2), 69–76. https://doi.org/10.31544/jtera.v9.i1.2024.69-76

Santoso, J. D. (2019). Keamanan Jaringan Menggunakan IDS/IPS Strataguard sebagai Layanan Kemanan Jaringan Terpusat. *SATIN - Sains Dan Teknologi Informasi*, *3*(2), 56–68. https://doi.org/10.33372/stn.v3i2.271

Silalahi, L. M., & Kurniawan, A. (2023). Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (Ips) Dengan Metode Traffic Behavior. *Electrician : Jurnal Rekayasa Dan Teknologi Elektro*, *17*(1), 71–76. https://doi.org/10.23960/elc.v17n1.2296

Suhendi, H., & Cahyo, W. D. (2021). Perancangan dan Implementasi Keamanan Jaringan Menggunakan Snort sebagai Intrusion Prevention System (IPS) pada Jaringan Internet STEI ITB. *Naratif : Jurnal Nasional Riset, Aplikasi Dan Teknik Informatika*, *3*(2), 60–68. https://naratif.sttbandung.ac.id/index.php/naratif/article/view/137

Widodo Purbo, O., Widodo Purbo Institut Teknologi Tangerang Selatan, O., Komplek Komersial BSD, I., & Raya Serpong Jl Komp Bsd No Kav, J. (2019). Ubuntu Linux Server Security Analysis and Simulation With Port Knocking & Iptable. *International Journal of Basic and Applied Science*, *8*(2), 36–46. www.ijobas.pelnus.ac.id

Zulkarnain. (2020). Analisis Keamanan FTP server Menggunakan Serangan Man-In-The-Middle Attack. *Telcomatics*, *5*(1), 12–18. https://doi.org/10.37253/telcomatics.v5i1.851