Vol 3 No. 2 April 2026 P-ISSN : 3047-9029 E-ISSN : 3047-9010, Hal 58 – 62

JURNAL RISET SISTEM INFORMASI
Halaman Jurnal: https://journal.smartpublisher.id/index.php/jissi
Halaman UTAMA Jurnal : https://journal.smartpublisher.id

DOI:https://doi.org/10.69714/38pr8578

# ANALISIS KEAMANAN FILE SERVER BERBASIS LINUX TERHADAP AKSES TIDAK SAH

**Rakhmadi Rahman [a], Nurfaida [b*], Muhammad Hasyim Rusmin [c]**
[a] Program Studi Sistem Informasi, rakhmadi.rahman@ith.ac.id, Institut Teknologi Bacharuddin Jusuf Habibie, Kota Parepare, Sulawesi Selatan, Indonesia
[b] Program Studi Sistem Informasi, nrpaidapaidaa@gmail.com, Institut Teknologi Bacharuddin Jusuf Habibie, Kota Parepare, Sulawesi Selatan, Indonesia
[c] Program Studi Sistem Informasi, hasyim0172646@gmail.com, Institut Teknologi Bacharuddin Jusuf Habibie, Kota Parepare, Sulawesi Selatan, Indonesia
[*] Penulis Korespondensi : Nurfaida

***ABSTRACT***

*In organizational environments, file servers function as centralized platforms for data storage and sharing, making system security a critical requirement. Inadequate security configurations may increase the risk of unauthorized access and data breaches. This study analyzes the security of a Linux-based file server through experimental testing of layered security mechanisms. The experiment was conducted on an Ubuntu Server configured with Samba and Network File System services. The applied security mechanisms include user and group management, Discretionary Access Control, Mandatory Access Control using AppArmor, and network access restrictions through a firewall. Security evaluation was performed using authorized and unauthorized access scenarios, including network scanning and authentication attempts. The results demonstrate that implementing layered security mechanisms significantly enhances protection against unauthorized access compared to basic permission settings alone. This research contributes practical guidance for strengthening Linux file server security in organizational environments.*

**Keywords**: *Unauthorized access, AppArmor, File server security, Linux, Access control.*

**Abstrak**

Dalam lingkungan organisasi, sistem file server digunakan sebagai media utama penyimpanan dan pertukaran data, sehingga perlindungan terhadap sistem tersebut menjadi kebutuhan yang tidak dapat diabaikan. Pengaturan keamanan yang kurang tepat dapat membuka peluang terjadinya akses tidak sah terhadap data. Penelitian ini bertujuan untuk menganalisis tingkat keamanan file server berbasis Linux melalui pengujian penerapan beberapa lapisan mekanisme pengamanan. Metode yang digunakan adalah eksperimen pada Ubuntu Server yang dikonfigurasikan sebagai file server dengan layanan Samba dan Network File System (NFS). Mekanisme keamanan yang diterapkan meliputi manajemen pengguna dan grup, Discretionary Access Control (DAC), Mandatory Access Control (MAC) berbasis AppArmor, serta pembatasan akses jaringan menggunakan firewall. Pengujian dilakukan melalui skenario akses legal dan ilegal, termasuk simulasi pemindaian jaringan dan percobaan autentikasi menggunakan Nmap dan Hydra. Hasil pengujian menunjukkan bahwa penerapan sistem keamanan secara berlapis mampu meningkatkan perlindungan terhadap akses tidak sah secara signifikan dibandingkan dengan penggunaan pengaturan permission dasar saja. Penelitian ini diharapkan dapat menjadi referensi dalam penerapan keamanan file server Linux pada lingkungan organisasi.

**Kata Kunci**: Akses tidak sah, AppArmor, Keamanan file server, Linux, Pengendalian akses.

## 1. PENDAHULUAN

Penggunaan *file server* sebagai sarana penyimpanan terpusat telah menjadi kebutuhan utama di berbagai organisasi, baik pada institusi pendidikan maupun sektor industri. Dalam penerapannya, *file server* dituntut

*Naskah Masuk 5 Januari 2026; Revisi 7 Januari 2026; Diterima 12 Januari 2026; Tersedia 13 Januari 2026*

mampu menjamin ketersediaan layanan, keutuhan data, serta perlindungan terhadap informasi yang bersifat sensitif. Seiring bertambahnya jumlah pengguna serta layanan jaringan, potensi munculnya ancaman keamanan, terutama akses data oleh pihak yang tidak berwenang, juga semakin meningkat [5]. Beberapa penelitian menunjukkan bahwa lemahnya pengaturan layanan berbagi file dan kontrol akses dapat menyebabkan kebocoran data serta penyalahgunaan hak akses pada sistem *file server* [1].

Linux menjadi salah satu sistem operasi yang umum dimanfaatkan sebagai platform *file server,* terutama karena karakteristiknya yang stabil dan fleksibel dalam berbagai lingkungan implementasi. Layanan berbagai file seperti Samba dan Network File System (NFS) memudahkan proses pertukaran data antar pengguna. Akan tetapi, kesalahan dalam pengaturan hak akses, pengendalian pengguna, maupun layanan jaringan dapat menimbulkan kerentanan keamanan apabila tidak diimbangi dengan mekanisme pengamanan yang memadai [5]. Oleh sebab itu, diperlukan penerapan mekanisme keamanan yang tepat dan berlapis untuk meminimalkan risiko akses tidak sah.

Penelitian ini difokuskan pada analisis keamanan *file server* berbasis Linux dengan melakukan pengujian terhadap mekanisme *permission*, pengendalian akses, serta pembatasan jaringan sebagai upaya perlindungan data.

## 2. TINJAUAN PUSTAKA

Keamanan pada sistem *file server* Linux didukung oleh beberapa komponen utama, antara lain manajemen pengguna dan grup, pengaturan permission file, serta model pengendalian akses. Pada model Discretionary Access Control (DAC), pengaturan hak akses ditentukan oleh pemilik sumber daya, sementara Mandatory Access Control (MAC) memberlakukan kebijakan keamanan yang ditetapkan dan dikendalikan oleh sistem secara terpusat.

Implementasi MAC pada Linux dapat dilakukan menggunakan AppArmor atau SELinux, yang berfungsi membatasi ruang lingkup akses aplikasi terhadap sistem. Beberapa penelitian sebelumnya menyatakan bahwa penerapan MAC dapat meningkatkan tingkat perlindungan sistem, terutama ketika dikombinasikan dengan mekanisme keamanan lain seperti firewall [2]. Selain itu, penggunaan tools pengujian keamanan seperti Nmap dan Hydra umum digunakan untuk mengevaluasi tingkat kerentanan layanan jaringan.

## 3. METODOLOGI PENELITIAN

Pendekatan penelitian yang digunakan adalah metode eksperimen, yang bertujuan untuk menguji dan mengevaluasi tingkat keamanan *file server* berbasis Linux melalui skenario pengujian terkontrol.

### 3.1 Lingkungan Pengujian

Pengujian dilakukan pada lingkungan simulasi laboratorium dengan spesifikasi sebagai berikut:

a. Sistem Operasi: Ubuntu Server 22.04 LTS
b. Layanan File Server: Samba dan Network File System (NFS)
c. Mekanisme Keamanan: Discretionary Access Control, AppArmor (MAC), dan Firewall UFW
d. Tools Pengujian: Nmap dan Hydra
e. Jenis Jaringan: Local Area Network (LAN)

### 3.2 Skenario Pengujian

Pengujian keamanan dilakukan melalui dua skenario utama, yaitu:

a. Akses Sah, di mana pengguna resmi mengakses direktori sesuai dengan hak akses yang telah ditetapkan.
b. Akses Tidak Sah, di mana pengguna tanpa izin mencoba mengakses file dan layanan yang dibatasi.

Setiap skenario diuji pada tiga kondisi konfigurasi keamanan, yaitu:

a. Konfigurasi dasar menggunakan DAC
b. Kombinasi DAC dan firewall
c. Kombinasi DAC, firewall, dan MAC (AppArmor)

Pengujian dilakukan pada lingkungan simulasi laboratorium menggunakan mesin virtual dengan skenario akses sah dan tidak sah, serta pencatatan hasil dilakukan berdasarkan observasi langsung terhadap respon sistem.

## 4. HASIL DAN PEMBAHASAN

### 4.1 Contoh Konfigurasi dan Pengujian Sistem

Pada bagian ini dijelaskan tahapan konfigurasi serta proses pengujian keamanan file server yang dilakukan pada lingkungan penelitian. Penjelasan difokuskan pada langkah-langkah teknis yang diterapkan untuk memastikan mekanisme pengendalian akses berjalan sesuai dengan perancangan, sehingga proses analisis dapat dipahami secara sistematis dan terstruktur.

#### 4.1.1 Pembuatan Pengguna dan Grup

```
sudo groupadd admin
sudo groupadd staff
sudo groupadd guest
```

**Listing 4.1.1.** Perintah pembuatan grup pada Linux

Perintah di atas digunakan untuk membuat grup dan pengguna berdasarkan peran. Pembagian peran ini bertujuan untuk menerapkan prinsip *least privilege*, sehingga setiap pengguna hanya memiliki hak akses sesuai kebutuhannya.

#### 4.1.2 Pembuatan Direktori dan Pengaturan Hak Akses

```
sudo mkdir /srv/shared_admin
sudo mkdir /srv/shared_staff

sudo chown :admin /srv/shared_admin
sudo chmod 770 /srv/shared_admin

sudo chown :staff /srv/shared_staff
sudo chmod 750 /srv/shared_staff
```

**Listing 4.1.2.** Pengaturan hak direktori berbasis grup

Konfigurasi ini bertujuan untuk membatasi akses direktori berdasarkan grup. Direktori *shared_admin* hanya dapat diakses penuh oleh grup admin, sedangkan *shared_staff* memiliki pembatasan akses tulis bagi pengguna di luar grup staff.

#### 4.1.3 Pengujian Akses Pengguna

```
su staff1
cd /srv/shared_admin
```

**Listing 4.1.3.** Pengujian akses pengguna

Hasil dari perintah tersebut menunjukkan pesan *permission denied,* yang menandakan bahwa sistem berhasil menolak akses pengguna yang tidak memiliki hak.

#### 4.1.4 Aktivasi dan Pengujian Firewall

```
sudo ufw allow ssh
sudo ufw allow samba
sudo ufw enable
sudo ufw status
```

**Listing 4.1.4.** Konfigurasi firewall menggunakan UFW pada sistem Linux

Firewall digunakan untuk membatasi akses layanan jaringan. Setelah firewall diaktifkan, hanya layanan tertentu yang diperbolehkan untuk diakses dari jaringan.

4.1.5 Pemindaian Jaringan Menggunakan Nmap

```
nmap -sS <IP_SERVER>
```

**Listing 4.1.5.** Perintah pemindaian jaringan menggunakan Nmap

Pemindaian ini dilakukan untuk mengidentifikasi port yang terbuka pada server. Hasil pemindaian menunjukkan bahwa jumlah port terbuka berkurang setelah firewall diaktifkan.

4.1.6 Aktivasi Mandatory Access Control (AppArmor)

```
sudo systemctl enable apparmor
sudo systemctl start apparmor
sudo aa-status
```

**Listing 4.1.6.** Aktivasi dan pemeriksaan status AppArmor

AppArmor digunakan sebagai lapisan keamanan tambahan untuk membatasi ruang lingkup akses aplikasi terhadap sistem.

4.1.7 Simulasi Percobaan Autentikasi

```
hydra -l admin1 -P password.txt
ssh://<IP_SERVER>
```

**Listing 4.1.7.** Simulasi percobaan autentikasi menggunakan Hydra

Simulasi ini dilakukan untuk mengevaluasi ketahanan sistem terhadap percobaan autentikasi berulang. Hasil observasi menunjukkan bahwa pembatasan layanan dan kebijakan keamanan tambahan mampu menurunkan peluang keberhasilan serangan.

### 4.2 Pengujian Akses Sah

Pengujian akses sah dilakukan untuk memastikan bahwa pengguna dapat mengakses sumber daya sesuai dengan perannya.

**Tabel 4.2.** Hasil Pengujian Akses Sah

| Jenis Pengguna | Direktori | Hak Baca | Hak Tulis | Keterangan |
|---|---|---|---|---|
| Admin | shared_admin | Ya | Ya | Berhasil |
| Staff | shared_staff | Ya | Ya | Berhasil |
| Staff | shared_admin | Ya | Tidak | Ditolak |
| Guest | shared_staff | Ya | Tidak | Ditolak |

Hasil pengujian menunjukkan bahwa penerapan permission berbasis peran mampu membedakan hak akses antar pengguna secara efektif.

### 4.3 Pengujian Akses Tidak Sah

Pengujian ini dilakukan dengan mencoba mengakses direktori tanpa hak akses yang sesuai.

**Tabel 4.3.** Hasil Pengujian Akses Tidak Sah

| Skenario | Konfigurasi Keamanan | Aktivitas | Hasil |
|---|---|---|---|
| Guest mengakses direktori Admin | DAC | Membaca file | Gagal |
| Guest mengakses direktori Admin | DAC + Firewall | Membaca file | Gagal |
| Guest mengakses direktori Admin | DAC + Firewall + MAC | Membaca file | Gagal |

### 4.4 Evaluasi Keamanan Jaringan dan Autentikasi

Pemindaian jaringan menggunakan Nmap menunjukkan bahwa penerapan firewall mampu membatasi port layanan yang terbuka. Simulasi percobaan autentikasi menggunakan Hydra menunjukkan penurunan peluang keberhasilan serangan setelah penerapan pembatasan akses dan kebijakan keamanan tambahan.

**Tabel 4.4.** Tingkat Risiko Akses Tidak Sah pada Berbagai Mekanisme Keamanan File Server

| Mekanisme Keamanan | Risiko Akses Tidak Sah |
|---|---|
| DAC | Sedang |
| DAC + Firewall | Rendah |
| DAC + Firewall + MAC | Sangat Rendah |

Hasil tersebut mengindikasikan bahwa penerapan mekanisme keamanan secara berlapis memberikan perlindungan yang lebih optimal. Klasifikasi tingkat risiko ditentukan berdasarkan jumlah layanan terbuka, keberhasilan autentikasi, dan pembatasan akses yang teramati selama pengujian.

## 5. KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa penerapan kombinasi beberapa mekanisme pengamanan mampu meningkatkan tingkat perlindungan pada sistem file server berbasis Linux secara signifikan. Hanya menggunakan Discretionary Access Control (DAC) masih belum cukup memberikan perlindungan yang memadai terhadap akses yang tidak sah. Dengan menggabungkan firewall serta Mandatory Access Control (MAC) berbasis AppArmor, sistem keamanan menjadi lebih kuat, terutama dalam situasi terjadi kesalahan pengaturan atau serangan dari luar.

Penelitian selanjutnya disarankan untuk mengembangkan sistem keamanan file server berbasis Linux dengan menambahkan mekanisme pengamanan lanjutan, seperti enkripsi data pada layanan berbagi file dan penerapan sistem deteksi serta pencegahan intrusi. Selain itu, pengujian dapat diperluas pada lingkungan jaringan yang lebih kompleks dengan jumlah pengguna dan variasi skenario serangan yang lebih beragam guna memperoleh hasil analisis yang lebih komprehensif.

**Ucapan Terima Kasih**

Penulis mengucapkan terima kasih kepada seluruh pihak yang telah memberikan dukungan, bimbingan akademik, serta masukan yang konstruktif selama pelaksanaan penelitian ini, sehingga penelitian dapat diselesaikan dengan baik.

## DAFTAR PUSTAKA

[1] T. Ariyadi, “Analisis keamanan layanan Network File System (NFS) pada sistem operasi Linux,” *Jurnal Sistem Informasi dan Keamanan Jaringan*, vol. 5, no. 1, pp. 45–54, 2023.

[2] Tamsir and T. Ariyadi, “Implementasi Mandatory Access Control menggunakan SELinux untuk meningkatkan keamanan sistem Linux,” *Jurnal Keamanan Informasi dan Sistem*, vol. 6, no. 2, pp. 89–98, 2024 .

[3] D. B. P. Pamungkas, Isnawaty, and L. M. F. Aksara, “Implementation of Samba server using OpenVPN based on single board computer (SBC) for private cloud storage,” *Journal of Applied Informatics and Computing (JAIC),* vol. 8, no. 2, pp. 316–325, 2024.

[4] K. Brimhall, A. Bates, Y. Tian, and M. Sherr, “A comparative analysis of Linux mandatory access control policy enforcement mechanisms,” in *Proceedings of the ACM European Workshop on Systems Security (EuroSec)*, ACM, 2023. doi:10.1145/3576915.3623072.

[5] V. Dakic, K. Jakobovic, and L. Zgrablic, “Linux security in physical, virtual, and cloud environments,” in *Proceedings of the 33rd DAAAM International Symposium on Intelligent Manufacturing and Automation*, B. Katalinic, Ed. Vienna, Austria: DAAAM International, 2022, pp. 151–160. doi:10.2507/33rd.daaam.proceedings.021.