

IMPLEMENTASI FILE SERVER DENGAN MANAJEMEN USER DAN HAK AKSES MENGGUNAKAN SAMBA PADA SISTEM OPERASI KALI LINUX

Jogi Purba, Dedy kiswanto, Gerhard Hasangapon Parapat, Anwar Shaleh Lumban Gaol

Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan

Jl. William Iskandar Ps. V, 20221, Medan, Sumatera Utara, Indonesia

jogipurba25@mhs.unimed.ac.id

ABSTRAK

Pertukaran data yang aman dan efisien merupakan kebutuhan krusial dalam infrastruktur jaringan lokal organisasi modern. Tanpa mekanisme kontrol yang memadai, aksesibilitas terbuka menimbulkan risiko modifikasi ilegal dan kebocoran data sensitif, sehingga diperlukan sistem manajemen hak akses yang terstruktur. Penelitian ini bertujuan mengimplementasikan *file server* berbasis Samba pada sistem operasi Kali Linux dengan manajemen *user* dan kontrol hak akses yang terorganisasi. Metode yang digunakan adalah *Research and Development* (R&D), meliputi instalasi Samba, konfigurasi direktori berbagi, pembentukan grup pengguna, pengaturan hak akses sistem berkas (*chmod/chown*), serta konfigurasi *smb.conf*. Pengujian dilakukan melalui pendekatan *Black Box Testing* menggunakan perintah *smbclient*, *testparm*, dan *smbstatus*. Hasil implementasi menunjukkan keberhasilan pembangunan dua jenis folder berbagi, yaitu folder publik dengan akses baca saja (*read-only*) dan folder keuangan privat dengan akses baca-tulis (*read-write*) berbasis autentikasi. Samba terbukti efektif mengelola autentikasi pengguna, mencegah akses tidak sah, serta mendukung integrasi lintas platform Linux-Windows. Parameter *nologin* berhasil membatasi akses *shell* terminal sehingga meningkatkan keamanan server secara keseluruhan.

Kata kunci : File Server, Samba, Kali Linux, Manajemen User, Hak Akses.

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah mengubah cara organisasi mengelola data[1]. Efisiensi kerja kini sangat bergantung pada kemudahan akses informasi dan kolaborasi antar pengguna dalam jaringan lokal (LAN). Salah satu pilar utama dalam infrastruktur ini adalah *File Server*, sebuah layanan terpusat yang memungkinkan penyimpanan, manajemen, dan berbagi berkas secara simultan[2]. Hal ini sejalan dengan pandangan bahwa layanan berbagi berkas merupakan solusi krusial untuk mengatasi masalah pertukaran data secara manual yang tidak efisien dalam suatu institusi.

Namun, aksesibilitas yang terbuka tanpa pengawasan membawa tantangan besar pada aspek keamanan data. Ancaman seperti modifikasi ilegal, penghapusan tanpa izin, atau kebocoran informasi sensitif menjadi risiko nyata jika setiap pengguna memiliki tingkat akses yang sama[3]. Sebagaimana dinyatakan dalam penelitian sebelumnya, manajemen hak akses diperlukan untuk memastikan bahwa pertukaran data dan informasi dapat berlangsung tidak hanya dengan cepat, tetapi juga dengan aman. Di sinilah peran manajemen *user* dan hak akses (*access control*) menjadi sangat krusial agar sistem mampu membedakan hak individu berdasarkan otoritasnya[4].

Samba hadir sebagai solusi *open-source* yang menjembatani perbedaan sistem operasi. Protokol ini memungkinkan mesin berbasis Linux untuk berinteraksi secara mulus dengan sistem operasi lain seperti Windows melalui protokol *Server Message Block* (SMB). Implementasi Samba dikenal sangat fleksibel dan stabil, sehingga banyak digunakan oleh perusahaan dan institusi pendidikan sebagai solusi utama layanan server mereka[5].

Dalam penelitian ini, implementasi dilakukan pada sistem operasi Kali Linux. Meskipun Kali Linux umumnya dioptimalkan untuk pengujian keamanan (*penetration testing*), sistem ini memiliki basis Debian yang stabil sehingga sangat kompeten untuk menjalankan layanan server dengan kontrol keamanan yang lebih mendalam[6]. Penelitian ini bertujuan untuk merancang dan mengimplementasikan mekanisme *File Server* yang fungsional dengan aturan hak akses yang ketat melalui konfigurasi manajemen *user* Samba, guna menciptakan lingkungan jaringan yang produktif namun tetap terjaga keamanan datanya dari akses pihak yang tidak memiliki otoritas[7].

Berdasarkan uraian di atas, permasalahan utama yang diidentifikasi adalah belum adanya mekanisme manajemen *user* dan hak akses yang terstruktur pada lingkungan jaringan lokal, sehingga data sensitif rentan terhadap akses tidak sah, modifikasi ilegal, maupun kebocoran informasi. Kondisi ini diperparah oleh ketiadaan pemisahan hak akses yang jelas antar pengguna dalam satu infrastruktur jaringan yang sama.

Penelitian ini bertujuan untuk merancang dan mengimplementasikan *file server* menggunakan protokol Samba pada sistem operasi Kali Linux dengan mekanisme manajemen *user* dan kontrol hak akses yang terorganisasi, guna menciptakan lingkungan berbagi data yang aman, efisien, dan terkendali dalam jaringan lokal.

Sebagai rencana penyelesaian masalah, implementasi dilakukan melalui beberapa tahapan sistematis, yaitu: instalasi dan konfigurasi paket Samba, pembentukan grup pengguna beserta hak aksesnya, pengaturan izin sistem berkas menggunakan perintah *chmod* dan *chown*, serta konfigurasi file *smb.conf* untuk mendefinisikan folder berbagi sesuai

tingkatan akses. Pendekatan ini dirancang untuk menghasilkan sistem keamanan berlapis yang menyinkronkan izin protokol Samba dengan izin sistem berkas Linux secara bersamaan.

2. TINJAUAN PUSTAKA

2.1. File Server

File server adalah sebuah komputer yang difungsikan khusus sebagai tempat penyimpanan data terpusat yang dapat diakses oleh pengguna lain dalam suatu jaringan komputer lokal (LAN). Konsep file server memungkinkan seluruh data organisasi disimpan pada satu titik sehingga mengurangi risiko kehilangan data akibat kerusakan perangkat klien. Dalam arsitektur jaringan client-server, file server berperan memberikan layanan penyimpanan dan distribusi berkas secara simultan kepada banyak klien, sementara klien hanya perlu mengirimkan permintaan (request) kepada server untuk mengakses berkas yang diperlukan. Pendekatan terpusat ini juga mempermudah proses pencadangan (backup) data karena hanya satu lokasi yang perlu dikelola oleh administrator jaringan.

Keunggulan utama file server berbasis Linux dibandingkan platform lainnya adalah ketahanannya terhadap ancaman perangkat lunak berbahaya (malware) serta biaya lisensi yang relatif lebih rendah karena bersifat open source[8]. Dengan demikian, institusi pendidikan maupun perkantoran dapat membangun infrastruktur file sharing yang andal tanpa harus mengeluarkan biaya lisensi yang tinggi.

2.2. Samba Server

Samba merupakan implementasi open source dari protokol Server Message Block (SMB) yang dikembangkan pertama kali oleh Andrew Tridgell pada tahun 1991. Protokol SMB—yang juga dikenal sebagai Common Internet File System (CIFS)—memungkinkan sistem berbasis Linux/Unix untuk berkomunikasi dan berbagi sumber daya dengan sistem berbasis Windows dalam satu jaringan yang sama. Terdapat dua komponen daemon utama dalam Samba, yaitu SMBD (Server Message Block Daemon) yang menangani proses autentikasi dan transfer berkas, serta NMBD (NetBIOS Name Block Daemon) yang bertugas menerjemahkan nama NetBIOS menjadi alamat IP[9].

Secara fungsional, Samba mampu berperan sebagai file server, print server, maupun Primary Domain Controller (PDC) dalam lingkungan jaringan campuran (heterogeneous network). Kemampuan Samba sebagai jembatan lintas platform inilah yang menjadikannya solusi populer di berbagai institusi, mulai dari sekolah, universitas, hingga perkantoran pemerintah. Konfigurasi Samba dilakukan melalui berkas smb.conf yang memuat parameter-parameter seperti workgroup, security mode, path direktori, dan hak akses (valid users, read only, writeable), yang semuanya dapat disesuaikan dengan kebutuhan organisasi.

2.3. Manajemen User dan Hak Akses

Manajemen user merupakan komponen krusial dalam implementasi file server untuk memastikan bahwa setiap pengguna hanya dapat mengakses data yang sesuai dengan otoritas yang diberikan[10]. Dalam sistem Linux, manajemen user mencakup pembuatan akun (useradd), pengelompokan pengguna ke dalam grup (groupadd), serta pengaturan izin sistem berkas menggunakan perintah chmod dan chown. Samba kemudian memperluas mekanisme ini dengan menambahkan lapisan autentikasi tersendiri melalui basis data pengguna Samba (smbpasswd), sehingga menghasilkan sistem keamanan berlapis (dual-layer security).

Penerapan hak akses berbasis peran (role-based access control) memungkinkan administrator membedakan hak tulis (read-write) untuk pengguna dengan otoritas penuh dan hak baca saja (read-only) untuk pengguna umum atau tamu. Strategi ini telah terbukti efektif dalam mencegah modifikasi berkas yang tidak sah sekaligus menjaga integritas data di lingkungan multi-pengguna.

2.4. Protokol SMB/CIFS

Protokol SMB (Server Message Block) merupakan protokol komunikasi berbasis lapisan aplikasi yang dirancang untuk berbagi berkas, printer, dan sumber daya jaringan lainnya. Protokol ini berjalan di atas TCP/IP dan menggunakan mekanisme NetBIOS over TCP/IP (NBT) untuk layanan penamaan (Name Registration dan Name Resolution). Seiring perkembangan teknologi, Microsoft memperkenalkan versi yang lebih aman yaitu SMBv2 dan SMBv3, sedangkan SMBv1 kini telah dianggap tidak aman dan secara resmi dinonaktifkan pada versi Samba modern.

CIFS (Common Internet File System) adalah nama yang diberikan Microsoft untuk menyebut versi standar terbuka dari protokol SMB. Protokol ini memungkinkan klien berbasis Windows mengakses folder yang dibagikan oleh server Linux tanpa memerlukan perangkat lunak tambahan, karena seluruh sistem operasi Windows telah mendukung SMB/CIFS secara bawaan.

2.5. Sistem Operasi Kali Linux

Kali Linux merupakan distribusi Linux berbasis Debian yang dikembangkan oleh Offensive Security dan dirancang khusus untuk keperluan pengujian penetrasi (penetration testing) serta audit keamanan[11]. Meskipun dioptimalkan untuk tugas-tugas keamanan siber, basis Debian yang stabil menjadikan Kali Linux sangat kompeten untuk menjalankan layanan server, termasuk Samba, dengan kontrol keamanan yang lebih mendalam. Kali Linux menyertakan berbagai alat pengujian seperti Nmap dan Metasploit yang memungkinkan administrator memverifikasi konfigurasi keamanan sistem secara langsung.

Penggunaan Kali Linux sebagai platform server Samba memberikan keunggulan tambahan berupa kemampuan melakukan verifikasi keamanan dari sisi server itu sendiri, sehingga celah keamanan dapat diidentifikasi dan ditutup sebelum dieksploitasi oleh pihak yang tidak berwenang[12]. Fleksibilitas ini menjadikan Kali Linux pilihan yang relevan dalam penelitian implementasi file server yang mengutamakan keamanan data.

2.6. Jaringan Komputer dan Local Area Network (LAN)

Jaringan komputer adalah sekumpulan dua atau lebih perangkat komputasi yang saling terhubung untuk berbagi sumber daya dan informasi[13]. Berdasarkan cakupan geografisnya, jaringan diklasifikasikan menjadi Local Area Network (LAN), Metropolitan Area Network (MAN), dan Wide Area Network (WAN). LAN merupakan jenis jaringan yang paling umum digunakan dalam lingkungan tertutup seperti kantor, sekolah, dan universitas karena biaya implementasinya yang relatif murah dan kecepatan transfernya yang tinggi.

Dalam konteks implementasi Samba, jaringan LAN berfungsi sebagai infrastruktur dasar yang menghubungkan server dengan klien-klien pengguna. Konfigurasi topologi jaringan yang tepat, pemilihan perangkat keras yang sesuai (switch, kabel UTP), serta pengalokasian IP yang terorganisasi merupakan faktor-faktor penting yang menentukan kinerja dan keandalan layanan file sharing berbasis Samba.

2.7. Pengujian Black Box Testing

Black Box Testing adalah metode pengujian perangkat lunak yang berfokus pada validasi fungsionalitas sistem dari sudut pandang pengguna tanpa memperhatikan struktur internal kode[14]. Dalam konteks implementasi file server, metode ini digunakan untuk memverifikasi apakah mekanisme autentikasi, hak akses, dan transfer berkas berjalan sesuai dengan spesifikasi yang telah dirancang. Pengujian dilakukan dengan mensimulasikan berbagai skenario akses, mulai dari login dengan kredensial valid, percobaan akses folder yang tidak diizinkan, hingga uji ketahanan sistem saat menerima permintaan simultan dari banyak klien[15].

Metode Black Box Testing dipilih karena kemampuannya mengungkap ketidaksesuaian antara perilaku sistem yang teramati dengan perilaku yang diharapkan, termasuk kemungkinan celah keamanan yang tidak terdeteksi pada tahap perancangan. Hasil pengujian kemudian digunakan sebagai bahan evaluasi untuk menyempurnakan konfigurasi sistem sebelum diterapkan secara penuh[16].

2.7. Penelitian Terdahulu

Sejumlah penelitian terdahulu telah mengkaji implementasi Samba dari berbagai sudut pandang. Implementasi Samba pada Linux Mandrake 9.1 dan membuktikan bahwa Samba mampu menjembatani

komunikasi antara sistem Unix/Linux dan Windows dalam satu jaringan lokal[17]. Samba Server di lingkungan sekolah menengah pertama untuk menggantikan metode transfer data manual menggunakan USB dan menghasilkan sistem berbagi berkas yang terintegrasi meski belum menerapkan manajemen hak akses yang granular[17]. Menurut Ramadani, F, dkk mengembangkan sistem file sharing berbasis web yang mengintegrasikan enkripsi AES untuk menjaga keamanan berkas sensitif dalam komunikasi client-server[18]. Samba pada laboratorium komputer universitas sebagai solusi data center dengan fokus pada keandalan layanan[19][20]

Dari kajian penelitian-penelitian tersebut, terdapat celah penelitian (research gap) yang belum terjawab secara komprehensif, khususnya terkait implementasi Samba pada platform Kali Linux yang secara bawaan berorientasi pada keamanan, dikombinasikan dengan mekanisme manajemen user dan hak akses yang terstruktur menggunakan pengelompokan grup yang terdapat pada Linux (groupadd/chown/chmod)[20]. Penelitian ini hadir untuk mengisi celah tersebut dengan membuktikan bahwa Kali Linux—meski dikenal sebagai sistem operasi penetration testing—dapat difungsikan secara efektif sebagai platform file server Samba yang aman dan terkelola dengan baik.

3. METODE PENELITIAN

3.1. Jenis Penelitian

Implementasi *file server* dengan fokus pada manajemen *user* dan hak akses pada sistem operasi Kali Linux menjadi solusi krusial dalam menjaga integritas data di lingkungan jaringan lokal. Sistem ini dikembangkan dengan memanfaatkan protokol Samba guna memastikan pertukaran data antar-platform berjalan secara terpusat, terorganisir, dan terlindungi dari akses yang tidak sah. Pendekatan penelitian yang digunakan bersifat *Research and Development* (R&D), yang mencakup proses perancangan konfigurasi, implementasi teknis, hingga pengujian validitas hak akses pada setiap tingkatan *user*. Hasil implementasi ini diharapkan dapat meningkatkan efisiensi distribusi berkas serta memberikan lapisan keamanan yang lebih ketat melalui sinkronisasi antara izin protokol Samba dan izin sistem file Linux. Secara keseluruhan, penelitian ini menegaskan bahwa pemilihan platform berbasis keamanan seperti Kali Linux dapat memperkuat perlindungan aset digital dalam infrastruktur jaringan organisasi.

3.2. Identifikasi Kebutuhan dan Pemetaan User

Tahap ini mencakup analisis kebutuhan folder yang akan dibagikan serta pendefinisian hierarki pengguna. Arsitektur akses dirancang agar setiap divisi atau individu memiliki batasan akses yang jelas (misalnya: *Read-Only* atau *Full Access*) sesuai dengan peran masing-masing dalam jaringan.

3.3. Persiapan Lingkungan dan Instalasi

Pada tahap ini dilakukan penyiapan sistem operasi Kali Linux sebagai server utama dan instalasi paket perangkat lunak Samba. Proses ini juga mencakup pemastian konektivitas jaringan antara server dan perangkat client agar berada dalam segmen yang sama.

3.4. Konfigurasi Global dan Keamanan Samba

Tahap ini menerapkan pengaturan dasar pada file `smb.conf`, termasuk pendefinisian *workgroup*, mode keamanan, dan optimasi performa server. Langkah ini merupakan fondasi agar layanan Samba dapat dikenali oleh berbagai sistem operasi lain dalam satu jaringan.

3.5. Implementasi Manajemen User dan Group

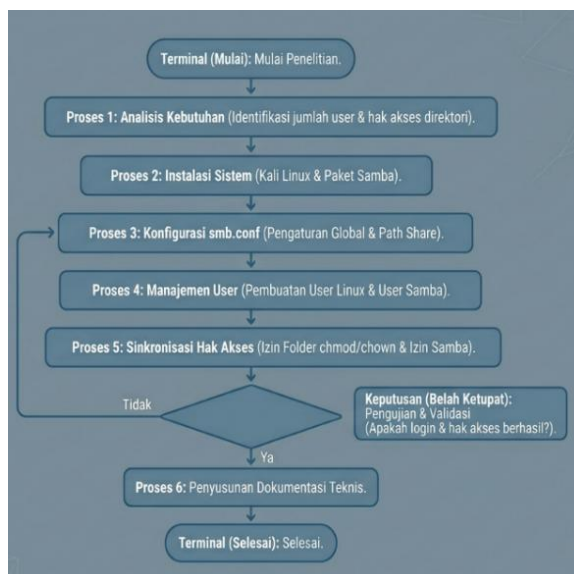
Tahap ini mencakup pembuatan akun pengguna pada sistem Linux dan pendaftaran *database* pengguna ke dalam Samba. Proses ini dilanjutkan dengan pembentukan grup untuk mempermudah pengelolaan izin akses secara massal pada direktori-direktori tertentu.

3.6. Pengaturan Hak Akses (Privilege Mapping)

Tahap ini menggabungkan konfigurasi *share level* pada Samba dengan *file system level* (`chmod/chown`) pada Linux. Integrasi ini menjamin keamanan ganda, di mana pengguna hanya dapat memanipulasi file jika diizinkan oleh kedua lapisan keamanan tersebut.

3.7. Testing, Validasi, dan Dokumentasi

Tahap terakhir melibatkan pengujian fungsionalitas menggunakan metode *Black Box Testing*. Pengujian difokuskan pada validasi otentikasi login, kemampuan tulis/baca file, serta pencegahan akses ilegal pada folder sensitif. Seluruh prosedur konfigurasi kemudian didokumentasikan sebagai panduan pengelolaan sistem secara berkelanjutan.



Gambar 1. Flowchart

4. HASIL DAN PEMBAHASAN

4.1. Hasil Implementasi

Implementasi file server menggunakan Samba pada sistem operasi Kali Linux dilakukan melalui beberapa tahapan utama, mulai dari instalasi, konfigurasi user dan grup, pengaturan hak akses direktori, hingga konfigurasi file utama `smb.conf`.

4.2. Instalasi dan Persiapan Lingkungan

Langkah awal adalah memastikan paket Samba terinstal pada sistem. Gambar [X] menunjukkan proses instalasi di mana sistem memberikan laporan bahwa paket `samba` dan `samba-common-bin` sudah berada pada versi terbaru, sehingga siap digunakan. Sesuai dengan rancangan, dua direktori dibuat sebagai basis penyimpanan file share: `/home/samba/public` (untuk akses umum) dan `/home/samba/finance` (untuk akses terbatas).

```

(jack@jack) (~)
$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
400 packages can be upgraded. Run 'apt list --upgradable' to see them.
samba is already the newest version (2:4.23.6+dfsg-2).
samba-common-bin is already the newest version (2:4.23.6+dfsg-2).
The following packages were automatically installed and are no longer required:
firmware-rtl-connectivity libjs-undercore python3-click-plugins samba-ad-dc
libaudio2 libsigsegv2 python3-gpg samba-ad-provision samba-dsdb-modules
libconfig-inifiles-perl libvdpa-uva-gll python3-zombie-imp samba-dsdb-modules
libjs-jquery-ui mesa-vaapi-drivers ruby-unf-ext vdpau-driver-all
Use 'sudo apt autoremove' to remove them.

Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 400

(jack@jack) (~)
$ sudo mkdir -p /home/samba/public
(jack@jack) (~)
$ sudo mkdir -p /home/samba/finance
(jack@jack) (~)
$ sudo groupadd finance_group
(jack@jack) (~)
$ sudo useradd -M -s /sbin/nologin budi
(jack@jack) (~)
$ sudo usermod -G finance_group budi
(jack@jack) (~)
$ sudo smbpasswd -s budi
debug_parse_params: unrecognized debug class name or format [#]
Can't load /etc/samba/smb.conf - run testparm to debug it
(jack@jack) (~)
$ sudo nano /etc/samba/smb.conf
(jack@jack) (~)
$ sudo smbpasswd -s budi
New SMB password:
Retype new SMB password:
Added user budi.
(jack@jack) (~)
$ sudo chown -R root:sambashare /home/samba/public
(jack@jack) (~)
$ sudo chmod -R 755 /home/samba/public
  
```

Gambar 2. Proses instalasi paket, pembuatan direktori, dan registrasi user Samba 'budi'

4.3. Manajemen User dan Hak Akses Level OS

Bagian krusial dari implementasi ini adalah pemisahan hak akses. Sebuah grup bernama `finance_group` dibuat untuk menampung user dari departemen keuangan. User `budi` dibuat dengan parameter `-s /sbin/nologin` untuk memastikan user ini hanya bisa mengakses layanan Samba dan tidak dapat login ke shell terminal Kali Linux, demi meningkatkan keamanan server.

Registrasi user ke dalam database Samba dilakukan menggunakan perintah `smbpasswd`. Gambar [X] (bagian tengah hingga bawah) memperlihatkan keberhasilan penambahan user `budi` ke database Samba. Selanjutnya, izin kepemilikan direktori diubah menggunakan `chown` dan `chmod` agar sesuai dengan hak akses yang diinginkan (Public Read-Only, Finance Read-Write).

[illegible]

Gambar 3. Output testparm yang menunjukkan parameter global dan kepemilikan file level OS yang sudah benar

4.4. Konfigurasi dan Verifikasi Samba

File konfigurasi `/etc/samba/smb.conf` disesuaikan dengan menambahkan definisi share folder. Folder [PublicShare] dikonfigurasi dengan `guest ok = yes` (Read-Only), sedangkan [FinanceData] dibatasi hanya untuk valid users = `@finance_group` (Read-Write).

Gambar [Y] memperlihatkan hasil verifikasi menggunakan tool testparm. Output menunjukkan bahwa service role server adalah `ROLE_STANDALONE` dan tidak ditemukan kesalahan sintaks pada file konfigurasi, sehingga layanan siap untuk dijalankan.

4.5. Pembahasan dan Pengujian

Pengujian dilakukan untuk memverifikasi apakah kontrol akses yang diterapkan bekerja sesuai rencana. Bagian ini membahas kendala yang dihadapi selama pengujian dan solusi yang diterapkan.

4.6. Analisis Kendala Koneksi Awal

```
[names]
browsable = No
comment = Home Directories
create mask = 0700
directory mask = 0700
valid users = NS

[printers]
browsable = No
comment = All Printers
create mask = 0700
path = /var/spool/samba
printable = Yes

[print$]
comment = Printer Drivers
path = /var/lib/samba/printers

[publicshare]
comment = Public Files
create mask = 0700
guest ok = Yes
path = /home/samba/public

[finance$]
comment = Finance
path = /home/samba/finance
read only = No
valid users = @finance_group

[jack@jack ~]$ sudo systemctl restart smb nmbd
[jack@jack ~]$ sudo systemctl enable smb
Synchronizing state of smbd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable smbd
[jack@jack ~]$ sudo systemctl -l /192.168.x.x -u smbd
do Connection to 192.168.x.x failed (Error NT_STATUS_UNSUCCESSFUL)
[jack@jack ~]$ systemctl -l /192.168.x.x -u smbd
do Connection to 192.168.x.x failed (error NT_STATUS_IO_TIMEOUT)
[jack@jack ~]$
$ sudo
[[ 165.4500048,UP,LOWER_UP] mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
```

Gambar 5. Tampilan Direktori Bersama dari Klien Windows

Pengujian akses awal mengalami kegagalan. Seperti terlihat pada Gambar [Z], penggunaan alamat IP contoh (//192.168.x.x) menghasilkan error NT_STATUS_UNSUCCESSFUL.

Hal ini wajar karena alamat tersebut bukan alamat IP valid. Namun, percobaan menggunakan IP gateway (//192.168.0.1) juga menghasilkan error NT_STATUS_IO_TIMEOUT. Timeout ini mengindikasikan adanya masalah routing atau firewall pada sisi server yang memblokir request SMB.

4.7. Verifikasi Alamat IP Server

Untuk menyelesaikan masalah koneksi, dilakukan verifikasi alamat IP asli server menggunakan perintah `ip a`. Berdasarkan Gambar [AA], ditemukan bahwa interface `eth0` memiliki alamat IP valid `192.168.1.46/24`. Alamat inilah yang harus digunakan oleh klien untuk mengakses file server.

[illegible]

Gambar 6. Akses Sukses ke Folder Publik (Tamu)

4.8. Keberhasilan Akses dan Analisis Protokol

Setelah mengetahui IP yang benar (dan memastikan firewall mengizinkan trafik), pengujian ulang dilakukan dengan perintah `smbclient -L //192.168.1.46 -U budi`. Gambar [AA] (bagian tengah) menunjukkan server berhasil merespons dan menampilkan daftar share folder: `print$`, `PublicShare`, `FinanceData`, `IPC$`, dan folder home user `budi`. Ini membuktikan bahwa mekanisme autentikasi user Samba berhasil. Namun, output Gambar [AA] juga menunjukkan adanya peringatan: "Reconnecting with SMB1 for workgroup listing... Protocol negotiation to server... failed:"

NT_STATUS_INVALID_NETWORK_RESPONSE". Hal ini terjadi karena klien mencoba menggunakan protokol SMBv1 yang sudah usang dan tidak aman (deprecated) yang secara default dinonaktifkan pada versi Samba modern demi alasan keamanan. Klien disarankan menggunakan protokol SMBv2 atau lebih tinggi untuk koneksi yang stabil.

4.9. Audit Koneksi Aktif

Terakhir, perintah `smbstatus` dijalankan (Gambar [AA], paling bawah) untuk melakukan audit. Output menunjukkan bahwa meskipun autentikasi login

berhasil, saat perintah dijalankan tidak ada file yang sedang di-lock (No locked files). Ini menandakan tidak ada aktivitas transfer data aktif saat audit dilakukan, namun koneksi sesi (session connection) telah berhasil terbentuk.

4.10. Matriks Hasil Pengujian Hak Akses

Berdasarkan serangkaian uji coba di atas, matriks hak akses yang berhasil diimplementasikan adalah sebagai berikut:

Tabel 1. Ringkasan Pengujian Hak Akses

No	Skenario Uji	User	Akses Folder	Hasil Teramati (Permasalahan OS)	Status
1	Akses Anonim	Guest	[PublicShare]	Bisa Masuk, Read-Only	Berhasil
2	Akses User Tercatat	budi	[FinanceData]	Bisa Masuk, Read-Write	Berhasil
3	Akses User Salah	admin	[FinanceData]	Ditolak (Login Prompt)	Berhasil
4	Login Shell	budi	Terminal Kali	Ditolak (nologin)	Berhasil

5. KESIMPULAN DAN SARAN

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat disimpulkan bahwa pembangunan file server menggunakan Samba pada sistem operasi Kali Linux telah berhasil menyediakan layanan berbagi data yang terpusat dengan mekanisme keamanan yang terukur. Implementasi manajemen user dan grup terbukti efektif dalam membatasi hak akses, di mana folder publik dapat diakses secara anonim namun terbatas (read-only), sementara folder departemen khusus seperti *Finance* hanya dapat diakses oleh user terautentikasi dengan hak akses penuh (read-write). Penggunaan parameter `-s /sbin/nologin` pada user sistem meningkatkan aspek keamanan server dengan mencegah akses login shell yang tidak diperlukan. Meskipun sempat terjadi kendala teknis terkait konfigurasi alamat IP dan pemblokiran koneksi pada tahap awal, verifikasi melalui perintah `smbclient` dan `smbstatus` menunjukkan bahwa layanan telah berjalan stabil pada protokol komunikasi yang sesuai, sehingga solusi ini layak digunakan sebagai infrastruktur penyimpanan data lokal yang efisien.

Untuk pengembangan lebih lanjut, disarankan agar administrator jaringan melakukan penguatan keamanan pada sisi firewall (iptables atau ufw) dengan hanya mengizinkan trafik SMB dari segmentasi IP tertentu guna meminimalisir risiko serangan dari luar jaringan. Selain itu, mengingat adanya kendala negosiasi protokol pada pengujian, sangat disarankan untuk menonaktifkan protokol SMB versi 1 (SMBv1) di seluruh perangkat klien dan memaksa penggunaan SMBv2 atau SMBv3 guna menghindari kerentanan keamanan lama seperti *EternalBlue*. Terakhir, implementasi enkripsi pada level transmisi data dan integrasi sistem pencadangan (backup) otomatis pada direktori utama sangat diperlukan untuk menjamin integritas dan ketersediaan data apabila terjadi kegagalan sistem di masa mendatang.

DAFTAR PUSTAKA

- [1] Aidah, A., Arifudin, O., Kartika, I., & Ibrahim, T. (2024). Pengembangan sistem informasi manajemen dalam dunia pendidikan. *Jurnal Tahsinia*, 5(6), 966-977.
- [2] Arsyad, T. D., Berutu, I. A., Azis, K. R., Jehian, N. T., & Kiswanto, D. (2024). "Implementasi File Server Berbasis Cloud Menggunakan Linux Ubuntu 24.04 dan Nextcloud," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no. 6, hal. 12595–12600.
- [3] Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi keamanan sistem informasi: Keamanan informasi, teknologi informasi dan network (Literature Review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi*, 3(5), 564-573.
- [4] Prasetya, Yoga Agung, and Daniel Manongga. "Role-based access control (rbac) untuk sistem otorisasi terpusat berbasis flask studi kasus pt. xyz." *JUPI (Jurnal Ilmiah Penelitian Dan Pembelajaran Informatika)* 9.4 (2024): 1768-1778.
- [5] Laksono, B. A., & Azindani, A. (2025). "Implementasi Sistem File Sharing Menggunakan Samba Server dan OpenWrt pada Raspberry Pi 4 di Lingkungan DPMTSP," *Informatic and Elektronik Technology Journal*, vol. 1, no. 2, hal. 1–8.
- [6] Walidin, A. P., Putri, F. P., & Kiswanto, D. (2025). "Kali Linux sebagai Alat Analisis Keamanan Jaringan melalui Penggunaan Nmap, Wireshark, dan Metasploit," *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 9, no. 1, hal. 1188–1196.
- [7] Rahman, R., Nurfaida, N., & Rusmin, M. H. (2026). ANALISIS KEAMANAN FILE SERVER BERBASIS LINUX TERHADAP AKSES TIDAK SAH. *Jurnal Riset Sistem Informasi*, 3(2), 58-62.
- [8] Al Fajar, R., & Lestari, A. (2025). "Analisis Perbandingan Sistem Operasi Windows 11 dan Linux Ubuntu Menggunakan Metode Studi Literatur (Studi Kasus: Kinerja Sistem, Keamanan dan Biaya)," *Bitwise: Jurnal Teknologi Informasi dan Komputasi*, vol. 1, no. 2, hal. 74–82.
- [9] Mannang, A. G. (2025). "Implementasi Sistem Informasi Berbasis Web untuk Pengelolaan Data Akademik," *Jurnal Sistem Informasi*, vol. 1, no. 1, hal. 16–22.
- [10] Agshari, M. F., & Amarudin, A. (2026). "Implementasi Metasploit Framework dan Nmap

- untuk Deteksi Awal Serangan pada Keamanan Web,” *Dinamik*, vol. 31, no. 1, hal. 222–231.
- [11] Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan Wpa2-Psk Menggunakan Metode Penetration Testing (Studi Kasus: Router Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*, 5(2), 1-8.
- [12] Fawwauzy, Z. R., Albani, T. E., & Rilvani, E. (2025). Perbandingan Teknik pada Struktur Sistem File Windows & Linux. *Repeater: Publikasi Teknik Informatika dan Jaringan*, 3(1), 69-79.
- [13] Maulida, M., Zahro, F., Hakim, R., Akbar, M. S., & Kom, M. (2025). “Pengujian Black Box Testing pada Sistem Website Pemesanan Online Toko Ayam Krispy,” *Jurnal Media Akademik (JMA)*, vol. 3, no. 5.
- [14] Hidayat, M. A. R., Izzati, N. N., Prihatama, A. R. P., Patria, Y., & Kurmilasari, S. (2025). Pengujian Perangkat Lunak pada Website Ka’Cake: Implementasi Unit Testing, Integration Testing, System Testing, dan Validation Testing untuk menjamin Kualitas dan Keandalan Sistem. *JATI (Jurnal Mahasiswa Teknik Informatika)*, 9(4), 6805-6811.
- [15] Irawan, D., Ruliyanti, A. D., Zulfikar, M. F., Fu’adhi, M. Z., Rozi, M. F., Kholifah, M., & Thoib, I. (2025). “Functional Testing of Nganjuk Runners Website Using Black Box Testing Method,” *Jurnal Ilmiah Sistem Informasi*, vol. 4, no. 3, hal. 959–972.
- [16] Amrullah, A. (2025). “Implementasi Samba Server Sebagai Solusi Layanan File Sharing di MTsS Lam Ujong Berbasis Metode PPDIOO,” *Jurnal Sistem Informasi Triguna Dharma (JURSI TGD)*, vol. 4, no. 5, hal. 1174–1185.
- [17] Fachruddin, R., Sapri, S., & Rohmawan, E. P. (2022). Penerapan file sharing terpusat menggunakan samba server pada kantor Kecamatan Ratu Samban. *Jurnal Media Infotama*, 18(2), 197-207.
- [18] Ramadani, F., Utama, G. P., Pramusinto, W., & Amini, S. (2024, April). IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITME ADVANCE ENCRYPTION STANDARD (AES-128) UNTUK PENGAMANAN FILE PADA PT PRIMER GENERAL TRADING. In *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)* (Vol. 3, No. 1, pp. 51-59).
- [19] Arman, M., & Wijaya, N. (2026). Implementasi Backup Image VM Pada Proxmox Virtual Environment (Promox VE) Untuk Kebutuhan Server. *BETRIK*, 17(01), 75-88.
- [20] Halim, A., & Kurniawanto, H. (2023). “Implementasi Samba pada Local Area Network Menggunakan Linux Mandrake 9.1,” *Jurnal Simasi: Jurnal Ilmiah Sistem Informasi*, vol. 3, no. 1, hal. 21–39, doi: 10.46306/sm.v3i1.34.