# MODUL JOBSHEET PRAKTIKUM MANDIRI

## ADMINISTRASI SISTEM JARINGAN FASE F (KELAS XI)

*Project-Based Learning (PjBL): Manajemen Pengguna Linux Server, Kontrol Hak Akses (Sudoers), Hardening Akun (Password Aging & PAM), Isolasi Shell, dan Automasi Provisioning Massal pada Virtual Machine*

## A. IDENTITAS PRAKTIKUM

| Parameter Identitas | Keterangan & Spesifikasi |
|---|---|
| Satuan Pendidikan | SMK Negeri 22 Jakarta |
| Bidang Keahlian | Teknologi Informasi |
| Program Keahlian | Teknik Komputer dan Jaringan (TKJ) |
| Mata Pelajaran | Administrasi Sistem Jaringan (ASJ) |
| Fase / Kelas | F / Kelas XI TKJ |
| Semester / Tahun Pelajaran | Ganjil (Semester 1) / 2026/2027 |
| Model Pembelajaran | Project-Based Learning (PjBL) |
| Metode Pembelajaran | Praktikum Mandiri Laboratorium, Eksplorasi Teknis, Problem Solving, Diskusi |
| Alokasi Waktu | 30 Jam Pelajaran (5 Pertemuan @ 6 x 45 Menit / 30 Jam Praktik) |
| Kode Tujuan Pembelajaran | TP 5.1.1 (Manajemen Pengguna, Hak Akses, dan Keamanan Dasar Akun Linux Server) |
| Nama Penyusun | Fernandez Eko NS |

## B. CAPAIAN PEMBELAJARAN (CP) & ALUR TUJUAN PEMBELAJARAN (ATP)

**1. Capaian Pembelajaran (CP) Fase F (Elemen ASJ):**
Pada akhir Fase F, peserta didik mampu menginstalasi sistem operasi jaringan; menjelaskan konsep; menginstalasi services; serta mengonfigurasi dan menguji remote server, DHCP server, DNS server, FTP server, file server, web server, mail server, database server, Control Panel Hosting, Shared Hosting Server, Dedicated Hosting Server, Virtual Private Server, VPN server, serta sistem kontrol dan monitoring.

**2. Alur Tujuan Pembelajaran (ATP) - Posisi Ke-1 Kelas XI (Juli - Agustus):**
• TP 5.1.1: Menerapkan manajemen pengguna sistem operasi jaringan (user & group management), mengontrol privilese administratif (sudo delegation), mengonfigurasi kebijakan umur kata sandi, serta melakukan automasi pembuatan akun sesuai standar SOP kerja.
• Alur Proyek PjBL:
1. Merefleksikan & Merencanakan (TP 1): Analisis arsitektur identitas Linux, pemetaan User ID (UID) & Group ID (GID), dan pemahaman fungsi berkas inti /etc/passwd, /etc/shadow, /etc/group, serta /etc/gshadow.
2. Mengaplikasikan Kontrol Akun & Grup (TP 2): Eksekusi pembuatan, modifikasi, dan penghapusan akun serta grup departemen sekolah menggunakan utilitas CLI (useradd, groupadd, usermod, gpasswd, userdel).
3. Mengaplikasikan Delegasi Privilese (TP 3): Konfigurasi hak akses administratif menggunakan kebijakan Sudoers (visudo), penerapan prinsip Least Privilege, dan pembuatan alias perintah sistem.
4. Manajemen Keamanan & Hardening Akun (TP 4): Menerapkan kebijakan umur kata sandi (password aging) menggunakan chage, penguncian akun bermasalah (account locking), dan isolasi akses terminal dengan /usr/sbin/nologin.
5. Automasi Provisioning Massal (TP 5): Pengembangan skrip pemrograman Bash mandiri untuk pembuatan akun pengguna massal (bulk user provisioning) menggunakan chpasswd dan looping bersyarat.
6. Evaluasi, Hardening, & Dokumentasi (TP 6): Pengujian isolasi direktori antar-grup (chmod, chown), pembuatan titik cadangan (VM Snapshot), analisis pemecahan masalah (troubleshooting), dan penyusunan laporan teknis.

## C. TUJUAN PEMBELAJARAN (TP) OPERASIONAL

1. TP 5.1.1.1: Peserta didik mampu menjelaskan struktur berkas sistem manajemen pengguna (/etc/passwd, /etc/shadow, /etc/group), serta membedakan klasifikasi akun (Root, System User, dan Regular User).

2. TP 5.1.1.2: Peserta didik mampu mengoperasikan perintah CLI (useradd, usermod, groupadd, gpasswd, userdel) untuk mengelola siklus hidup akun pengguna dan mengelompokkannya ke dalam grup departemen kerja.

3. TP 5.1.1.3: Peserta didik mampu mengonfigurasi delegasi wewenang administratif menggunakan utilitas visudo, termasuk pemberian hak sudo terbatas untuk eksekusi layanan jaringan spesifik tanpa kata sandi (NOPASSWD).

4. TP 5.1.1.4: Peserta didik mampu menerapkan kebijakan pengamanan akun (account hardening) melalui pengaturan batas waktu kedaluwarsa sandi (chage), penguncian akun non-aktif (passwd -l), serta pembatasan login shell.

5. TP 5.1.1.5: Peserta didik mampu membangun skrip automasi pemeliharaan dan pembuatan akun massal (bulk user provisioning) berbasis Bash, serta mendokumentasikan prosedur manajemen pengguna ke dalam laporan teknis.

## D. KOMPETENSI INDUSTRI

Modul praktikum ini dirancang untuk membekali peserta didik dengan standar kompetensi teknis Junior Network & System Administrator di dunia kerja industri IT:

**1. Hard Skills (Kompetensi Teknis):**
• Penguasaan administrasi identitas dan otentikasi pada Linux Server berstandar POSIX (Portable Operating System Interface).
• Pemahaman algoritma enkripsi kata sandi (hashing SHA-512/yescrypt) pada direktori shadow.
• Implementasi Role-Based Access Control (RBAC) sederhana melalui manajemen Primary Group dan Supplementary Group.
• Konfigurasi berkas /etc/sudoers secara aman menggunakan utilitas visudo untuk mencegah kerusakan sintaks parser sistem.
• Administrasi kebijakan kepemilikan dan hak akses berkas/direktori (File Permissions) menggunakan chown, chgrp, dan chmod (metode oktal & simbolik).
• Penulisan skrip automasi Shell Bash untuk provisioning dan deprovisioning akun secara massal di pusat data.

**2. Soft Skills (Kompetensi Kerja Industri):**
• Kepatuhan Keamanan (Security Awareness): Menerapkan prinsip Least Privilege (hanya memberikan hak akses seminimal mungkin sesuai kebutuhan tugas pokok karyawan/teknisi).
• Ketelitian Prosedural (SOP): Selalu memverifikasi dampak perubahan Group ID terhadap akses direktori kerja sebelum menghapus atau memodifikasi akun pengguna.
• Manajemen Dokumentasi Teknis: Mencatat alokasi User ID (UID), struktur grup organisasi, dan kebijakan password aging ke dalam logbook administrasi sistem.

## E. SKENARIO PROJECT-BASED LEARNING (PjBL)

**Konteks Industri/Proyek:**
SMK Negeri 22 Jakarta bersiap menyambut tahun ajaran baru 2026/2027. Tim IT Sekolah bertugas mengimplementasikan server pusat data pada unit Teaching Factory. Sebelum berbagai layanan jaringan seperti Web Server, DNS Server, dan File Sharing dipasang dan diaktifkan, Kepala Unit IT mensyaratkan bahwa server wajib memiliki arsitektur manajemen pengguna yang terstruktur dan aman. Tidak boleh ada pengguna umum atau teknisi magang yang menggunakan akun root secara langsung untuk aktivitas harian.

**INSTRUKSI KERJA PROYEK (WORK ORDER):**
Anda ditugaskan sebagai Tim Teknisi Sistem & Keamanan Jaringan. Tugas Anda adalah melakukan manajemen komprehensif terhadap seluruh akun pengguna dan grup di dalam Virtual Machine Debian Server Anda. Anda diminta untuk:
1. Melakukan audit dan analisis terhadap berkas identitas sistem (/etc/passwd dan /etc/shadow).
2. Membangun struktur grup kerja organisasi sekolah (grp-admin, grp-guru, grp-siswa) dan membuat akun representatif untuk masing-masing divisi dengan parameter direktori home yang terisolasi.
3. Mengonfigurasi delegasi hak sudo terbatas menggunakan visudo agar akun teknisi tertentu dapat mengelola layanan jaringan tanpa harus mengetahui kata sandi root.
4. Menerapkan kebijakan Password Aging (wajib ganti kata sandi setiap 30 hari) dan menguji penguncian akun siswa yang telah lulus/non-aktif.
5. Membangun sebuah skrip automasi mandiri bernama tkj-bulk-user.sh yang mampu membuat 20 akun siswa baru secara otomatis dalam hitungan detik beserta kata sandi acaknya. Proyek diakhiri dengan uji validasi isolasi hak akses dan pembuatan titik cadangan Snapshot VM baru.

## F. PERTANYAAN PEMANTIK

1. Mengapa dalam sistem operasi Linux, setiap layanan daemon (seperti Apache Web Server, Nginx, atau BIND DNS) selalu dijalankan oleh System User khusus yang memiliki shell /usr/sbin/nologin atau /bin/false, bukan dijalankan langsung oleh akun superuser root?

2. Apa risiko fatal yang dapat terjadi pada integritas server jika seorang System Administrator memberikan hak akses administratif penuh kepada pengguna biasa melalui modifikasi berkas /etc/sudoers tanpa pembatasan spesifik (unrestricted sudo privileges)?

3. Bagaimana perbedaan fundamental antara menyimpan informasi pengguna pada berkas /etc/passwd dengan menyimpan kredensial kata sandi pada berkas /etc/shadow dalam konteks keamanan otentikasi Linux? Mengapa berkas /etc/passwd dapat dibaca oleh semua pengguna (world-readable), sedangkan /etc/shadow tidak?

4. Ketika sebuah sekolah atau perusahaan menerima ratusan siswa atau karyawan baru setiap tahunnya, mengapa teknik pembuatan akun secara manual menggunakan perintah useradd satu per satu dianggap sangat tidak efisien dan berisiko tinggi terhadap human error?

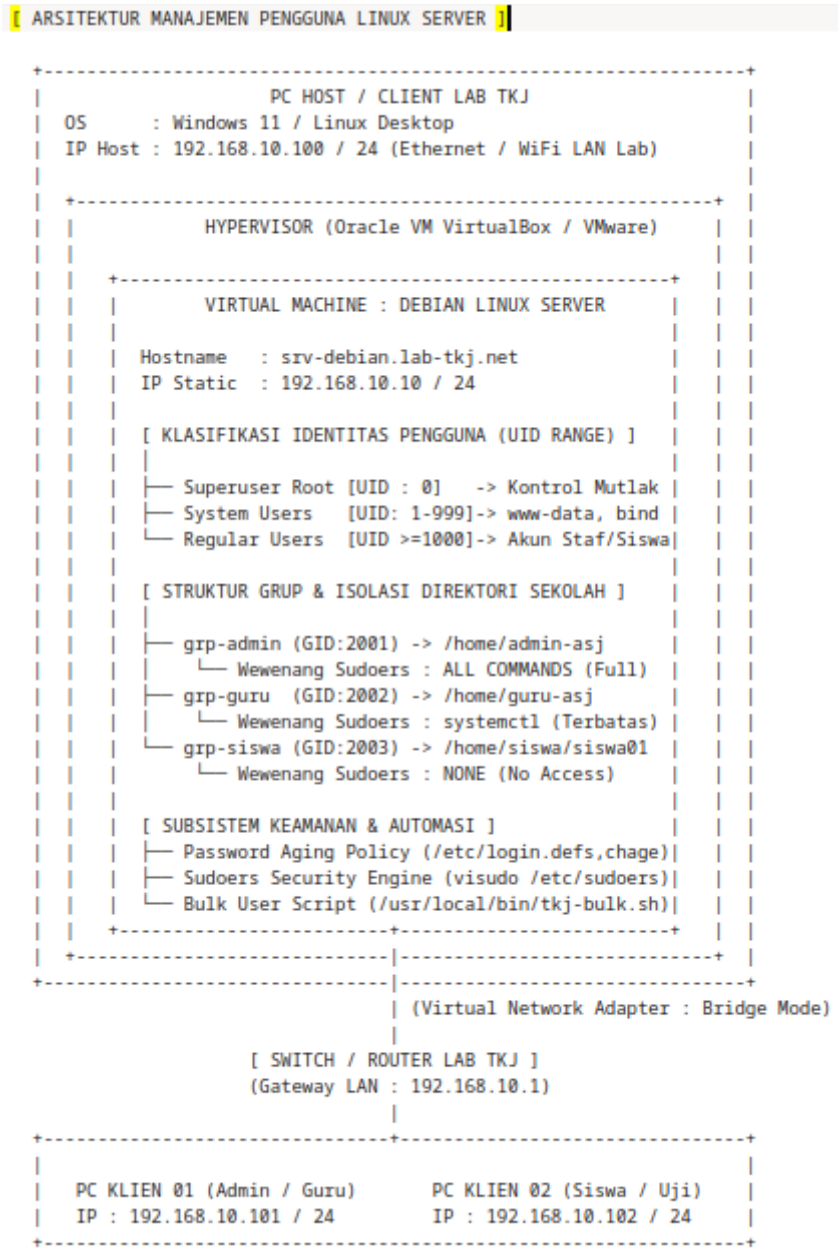
## G. ALAT DAN BAHAN

| Kategori Perangkat | Spesifikasi / Nama Perangkat | Keterangan & Fungsi Teknis |
|---|---|---|
| Perangkat Keras / PC Lab | PC / Laptop Lab TKJ (Intel Core i3 / AMD Ryzen 3 atau lebih tinggi) | CPU Min. 4 Cores/Threads, RAM Min. 8 GB, Storage Min. 100 GB Free Space. Fitur Virtualisasi (VT-x / AMD-V) aktif di BIOS. |
| Perangkat Lunak Virtualisasi | Oracle VM VirtualBox 7.x / VMware Workstation Pro / Proxmox VE | Hypervisor untuk mengelola mesin virtual Linux Debian Server dari proyek praktikum instalasi dasar. |
| Mesin Virtual Target (VM) | VM SMKN22-Debian-Server-XI (Hasil Snapshot Bab Sebelumnya) | Mesin virtual Debian 12/13 Server dengan IP Statis (192.168.10.10/24), partisi manual (Root, Swap, Home), dan akun Sudo aktif. |
| Sistem Operasi Klien (Host) | Windows 10/11 atau Linux Desktop | Berfungsi sebagai terminal klien untuk melakukan akses remote SSH dengan berbagai identitas akun pengguna. |
| Konektivitas Jaringan | Jaringan LAN Laboratorium dengan Akses Internet / Router Lokal | Digunakan untuk mengunduh utilitas pendukung (sudo, whois, libpam-cracklib) melalui repositori APT lokal/internet. |
| Paket Utility & Security Lab | passwd, sudo, chage, whois | Utiliti manajemen identitas, |

| | | |
|---|---|---|
| | (untuk mkpasswd), openssl, libpam-tmpdir, nano, vim | otentikasi PAM (Pluggable Authentication Modules), dan generator enkripsi kata sandi. |

## H. TOPOLOGI DAN ARSITEKTUR LAYANAN

Praktikum ini menggunakan arsitektur Single-Host Virtualization dengan Multi-Tier User Access Control. Di dalam sistem operasi tamu (Guest OS), klasifikasi akun dibagi berdasarkan rentang User ID (UID) dan dipetakan ke dalam grup kerja spesifik dengan kebijakan isolasi direktori lokal.



## I. RANCANGAN KONFIGURASI KLASTER / LAYANAN

| Parameter Konfigurasi | Nilai / Spesifikasi Implementasi |
|---|---|
| Nama Mesin Virtual (VM Name) | SMKN22-Debian-Server-XI |
| Alokasi Sumber Daya VM | Memory: 2048 MB (2 GB) \| Processor: 2 vCPU Cores \| Storage: 20 GB |
| Alamat IP Statis & Gateway | IP: 192.168.10.10/24 \| Gateway: 192.168.10.1 \| Hostname: srv-debian |
| Struktur Grup Organisasi (GID) | 1. grp-admin (GID: 2001) - Divisi Administrator Server Sekolah<br>2. grp-guru (GID: 2002) - Divisi Pengajar & Instruktur ASJ<br>3. grp-siswa (GID: 2003) - Divisi Peserta Didik Praktikum |
| Daftar Akun Pengguna Target | • admin-asj (UID: 2001, Grup Utama: grp-admin, Shell: /bin/bash)<br>• guru-asj (UID: 2002, Grup Utama: grp-guru, Shell: /bin/bash)<br>• siswa01 (UID: 2003, Grup Utama: grp-siswa, Shell: /bin/bash)<br>• web-daemon (UID: 990, Grup: www-data, Shell: /usr/sbin/nologin) |
| Kebijakan Delegasi Sudoers | • admin-asj: Akses penuh (ALL=(ALL:ALL) ALL)<br>• guru-asj: Akses terbatas (NOPASSWD: /usr/bin/systemctl, /usr/bin/journalctl)<br>• siswa01: Dilarang menggunakan sudo secara total |
| Kebijakan Umur Kata Sandi (Aging) | • Maximum Password Age: 30 Hari (Wajib ganti sandi setiap bulan)<br>• Minimum Password Age: 2 Hari (Mencegah ganti sandi berulang instan)<br>• Warning Days: 7 Hari (Peringatan kedaluwarsa sebelum masa habis) |
| Identitas Skrip Bulk Provisioning | Nama File: /usr/local/bin/tkj-bulk-user.sh |

| | |
|---|---|
| | Target Automasi: Pembuatan akun siswa-lab01 s.d. siswa-lab20 secara serentak |
| Akun Operator Master Lab | Akun Admin: sysadmin (Grup Sudo aktif) \| Kata Sandi: AdminTKJ#2026! |
| Nama Snapshot Cadangan Baru | Snapshot-02-User-Management-Mastered |

## J. SINTAKS PROJECT-BASED LEARNING (PjBL)

Pelaksanaan praktikum modul ini dijadwalkan selama 30 Jam Pelajaran (5 Pertemuan @ 6 JP) sesuai Program Semester Ganjil (No. 1), yang mencakup bulan Juli dan Agustus dengan alur sintaks:

**1. Penentuan Pertanyaan Mendasar (Start with the Essential Question - Pertemuan 1 / 6 JP):** Guru memberikan studi kasus tentang kebocoran data di sebuah perguruan tinggi akibat mantan karyawan yang akunnya tidak dikunci dan lemahnya pembatasan hak akses sudo. Peserta didik menganalisis pentingnya manajemen identitas, enkripsi /etc/shadow, dan prinsip Least Privilege.

**2. Mendesain Perencanaan Proyek (Design a Plan for the Project - Pertemuan 1 / 6 JP):** Peserta didik memeriksa kondisi mesin virtual dasar, merancang struktur pengelompokan akun pengguna sekolah (grp-admin, grp-guru, grp-siswa), memetakan alokasi UID/GID agar teratur mulai dari 2000, serta merancang skema kebijakan umur kata sandi.

**3. Menyusun Jadwal & Alur Kerja (Create a Schedule - Pertemuan 2 / 6 JP):** Peserta didik dan guru menyepakati jadwal implementasi proyek selama minggu efektif pembelajaran:
• Pertemuan 2 (6 JP): Eksekusi manajemen akun dan grup dasar (groupadd, useradd, usermod), pengujian otentikasi login shell, dan pengamanan akun layanan jaringan (nologin).

**4. Pelaksanaan & Monitor Proyek (Monitor the Students and the Progress - Pertemuan 3 & 4 / 12 JP):** • Pertemuan 3 (6 JP): Konfigurasi delegasi privilese menggunakan visudo, pengujian akses NOPASSWD untuk layanan server, penerapan password aging dengan chage, dan pengujian simulasi akun terkunci.
• Pertemuan 4 (6 JP): Pembuatan dan penyempurnaan skrip pemrograman Bash (tkj-bulk-user.sh) untuk pembuatan akun massal siswa, lalu melakukan pengujian isolasi hak pakai direktori (chmod 770 dan chown).

**5. Pengujian & Validasi Hasil (Assess the Outcome - Pertemuan 5 / 3 JP):** Peserta didik melakukan Acceptance Test: uji coba login remote SSH menggunakan berbagai akun

yang telah dibuat, memverifikasi pembatasan perintah sudo pada akun guru, dan memastikan akun siswa tidak dapat membaca direktori admin.

**6. Evaluasi & Refleksi (Evaluate the Experience - Pertemuan 5 / 3 JP):** Peserta didik membuat titik cadangan sistem baru (Snapshot-02), menganalisis kendala teknis dan pesan error yang ditemukan, melengkapi lembar evaluasi kerja, dan menyerahkan dokumentasi proyek kepada guru pengampu.

## K. LANGKAH KERJA PRAKTIKUM MANDIRI

> **PERINGATAN K3LH & SOP:**
> **Bekerja dengan konfigurasi identitas dan sudoers memiliki risiko tinggi fatalitas sistem. JANGAN PERNAH mengedit berkas /etc/sudoers menggunakan teks editor biasa seperti nano /etc/sudoers atau vim /etc/sudoers secara langsung! Selalu gunakan perintah resmi sudo visudo yang dilengkapi mekanisme pemeriksaan sintaks otomatis sebelum berkas disimpan. Kesalahan satu karakter pada /etc/sudoers dapat menyebabkan seluruh akun admin kehilangan hak sudo secara permanen (lockout)! Selalu buka satu jendela terminal root aktif sebagai pengaman selama konfigurasi berlangsung.**

### Langkah 1: Audit Struktur Berkas Identitas & Kredensial Linux

1. Nyalakan PC Host laboratorium, buka aplikasi Oracle VM VirtualBox Manager, dan pilih mesin virtual SMKN22-Debian-Server-XI.
2. (Opsi SOP) Pastikan VM berada pada kondisi bersih dengan melakukan restore ke Snapshot-01-Base-OS-Installed-Clean. Klik tombol Start.
3. Login ke dalam terminal server menggunakan akun administratif:
   • Username: sysadmin | Kata Sandi: AdminTKJ#2026!
4. Lakukan inspeksi terhadap 5 baris terakhir dari berkas penyimpan identitas pengguna (/etc/passwd):

```
tail -n 5 /etc/passwd
```

Anatomi baris /etc/passwd: sysadmin:x:1000:1000:System Admin,,,:/home/sysadmin:/bin/bash.
(Kolom: Username : Password Placeholder : UID : GID : Comment/GECOS : Home Directory : Login Shell).
5. Periksa hak akses pembacaan pada berkas /etc/passwd dan /etc/shadow:

```
ls -l /etc/passwd /etc/shadow
```

Perhatikan bahwa /etc/passwd memiliki hak akses -rw-r--r-- (semua pengguna bisa membaca), sedangkan /etc/shadow memiliki hak akses -rw-r----- atau -rw------- dengan kepemilikan root/shadow (sangat rahasia).
6. Lihat struktur algoritma enkripsi pada berkas /etc/shadow (wajib menggunakan sudo):

```
sudo tail -n 3 /etc/shadow
```

Jika hash kata sandi diawali dengan tanda $y$ atau $6$, itu menunjukkan sistem menggunakan enkripsi modern yang sangat kuat (yescrypt atau SHA-512).

## Langkah 2: Manajemen Grup dan Akun Pengguna Terstruktur

Kita akan mengklasifikasikan pengguna sekolah berdasarkan departemen kerja mulai dari GID/UID 2000 agar terpisah rapi dari akun sistem standar.
1. Buat 3 grup departemen sekolah dengan spesifikasi Group ID (GID) khusus:

```
sudo groupadd -g 2001 grp-admin
sudo groupadd -g 2002 grp-guru
sudo groupadd -g 2003 grp-siswa
```

2. Verifikasi bahwa ketiga grup tersebut telah berhasil terdaftar pada sistem:

```
tail -n 3 /etc/group
```

3. Membuat Akun Administrator Khusus (admin-asj):
Buat akun dengan UID 2001, grup utama grp-admin, serta sertakan dalam grup tambahan sudo dan adm:

```
sudo useradd -m -u 2001 -g grp-admin -G sudo,adm -s /bin/bash -c "Administrator Server ASJ" admin-asj
```

Parameter: -m (buat direktori home), -u (tentukan UID), -g (grup utama), -G (grup tambahan), -s (shell standar), -c (komentar identitas).
4. Membuat Akun Pengajar (guru-asj):
Buat akun pengajar dengan UID 2002 dan direktori home khusus:

```
sudo useradd -m -u 2002 -g grp-guru -s /bin/bash -c "Guru Mata Pelajaran ASJ" guru-asj
```

5. Membuat Akun Peserta Didik (siswa01):
Buat akun siswa di dalam sub-direktori khusus /home/siswa/siswa01:

```
sudo mkdir -p /home/siswa
sudo useradd -m -d /home/siswa/siswa01 -u 2003 -g grp-siswa -s /bin/bash -c "Siswa Praktikum TKJ" siswa01
```

6. Membuat Akun Layanan Sistem (System Account):
Buat akun khusus untuk menjalankan aplikasi layanan jaringan (web-daemon) tanpa hak akses terminal (shell nologin):

```
sudo useradd -r -u 990 -g www-data -s /usr/sbin/nologin -c "Custom Web Daemon User" web-daemon
```

Parameter -r menandakan pembuatan System User (UID di bawah 1000).
7. Buat kata sandi untuk ketiga akun reguler yang baru saja dibentuk:

```
sudo passwd admin-asj
sudo passwd guru-asj
sudo passwd siswa01
```

(Gunakan kata sandi lab standar: RahasiaTKJ#2026! untuk masing-masing akun agar mudah diuji).
8. Verifikasi pemetaan identitas, UID, GID, dan keanggotaan grup akun tersebut dengan utilitas id:

```
id admin-asj
id guru-asj
id siswa01
id web-daemon
```

## Langkah 3: Konfigurasi Delegasi Privilese dengan Sudoers (visudo)

Kita ingin memberikan wewenang kepada akun guru-asj untuk dapat me-restart layanan server dan melihat log sistem tanpa memberikan hak superuser penuh, dan tanpa perlu memasukkan kata sandi setiap saat untuk efisiensi instruksi lab.

1. Buka editor konfigurasi keamanan Sudoers menggunakan utilitas resmi:

```
sudo visudo
```

(Secara default akan membuka editor nano atau vi pada berkas sementara di memori buffer /etc/sudoers.tmp).

2. Arahkan kursor ke bagian paling bawah berkas konfigurasi, lalu tambahkan aturan delegasi berikut secara presisi:

```
# Delegasi Hak Akses Khusus Laboratorium ASJ SMKN 22 Jakarta

# 1. Akun admin-asj memiliki hak sudo mutlak (sama seperti root)
admin-asj    ALL=(ALL:ALL) ALL

# 2. Akun guru-asj hanya boleh mengelola service dan log Tanpa Password
guru-asj     ALL=(ALL) NOPASSWD: /usr/bin/systemctl, /usr/bin/journalctl

# 3. Grup grp-admin memiliki hak sudo mutlak dengan verifikasi sandi
%grp-admin   ALL=(ALL:ALL) ALL
```

(Simpan berkas konfigurasi: Jika nano, tekan CTRL+O, ENTER, CTRL+X).
Sistem akan memeriksa sintaks secara otomatis. Jika tidak ada pesan kesalahan, aturan langsung aktif!
3. Pengujian Verifikasi Hak Akses Sudo:

- Buka sesi terminal baru atau beralih identitas (switch user) menjadi guru-asj:

```
su - guru-asj
```

- Periksa daftar wewenang sudo apa saja yang dimiliki oleh akun ini:

```
sudo -l
```

Output akan menampilkan daftar perintah NOPASSWD: /usr/bin/systemctl, /usr/bin/journalctl.

- Uji coba me-restart layanan SSH menggunakan hak sudo tanpa kata sandi:

```
sudo systemctl restart ssh
```

Perintah harus langsung berhasil dieksekusi tanpa meminta input kata sandi!

- Uji coba melakukan tindakan di luar wewenang (misalnya menambahkan user baru):

```
sudo useradd peretas01
```

Sistem akan menolak dengan tegas: Sorry, user guru-asj is not allowed to execute '/usr/sbin/useradd peretas01' as root on srv-debian. (Prinsip Least Privilege sukses!)

- Ketik exit untuk kembali ke akun operator sysadmin.

## Langkah 4: Hardening Akun & Kebijakan Umur Kata Sandi (chage)

Kata sandi yang tidak pernah diganti dalam jangka waktu lama rentan terhadap pembobolan. Kita akan menerapkan aturan masa kedaluwarsa kata sandi (Password Aging) pada akun siswa.

1. Periksa parameter informasi umur kata sandi saat ini pada akun siswa01:

```
sudo chage -l siswa01
```

Secara default, Maximum number of days between password change bernilai 99999 (tidak pernah kedaluwarsa).
2. Ubah kebijakan masa pakai kata sandi untuk akun siswa01 dengan ketentuan: Max 30 hari, Min 2 hari, Peringatan 7 hari sebelum habis, dan akun otomatis terkunci 5 hari setelah masa tenggang habis:

```
sudo chage -M 30 -m 2 -W 7 -I 5 siswa01
sudo chage -l siswa01
```

Perhatikan perubahan tanggal pada kolom Password expires dan Account expires.
3. Memaksa Pengguna Mengganti Kata Sandi Saat Login Pertama Kali:
Untuk menyimulasikan akun baru siswa yang wajib mengganti sandi sementara dari guru saat pertama kali login:

```
sudo chage -d 0 siswa01
```

Aturan ini mengubah tanggal modifikasi sandi terakhir menjadi nol (kedaluwarsa instan).
4. Pengujian Penguncian Akun Non-Aktif (Account Locking):
Jika seorang siswa telah lulus atau mutasi, kita harus mengunci akunnya tanpa menghapus direktori datanya:

```
sudo usermod -L siswa01
sudo grep siswa01 /etc/shadow
```

Perhatikan bahwa setelah di-lock (-L), tanda seru (!) akan ditambahkan di depan string hash kata sandi pada /etc/shadow, yang membuat otentikasi login mustahil dilakukan.
5. Untuk membuka kembali kunci akun tersebut (unlock):

```
sudo usermod -U siswa01
```

## Langkah 5: Pembuatan Skrip Automasi Provisioning Akun Massal

Di dunia kerja nyata, admin tidak membuat akun satu per satu. Anda akan membuat skrip pemrograman Bash yang memanfaatkan utilitas chpasswd untuk melakukan bulk provisioning 20 akun siswa sekaligus.

1. Buat berkas skrip automasi baru di direktori /usr/local/bin/:

```
sudo nano /usr/local/bin/tkj-bulk-user.sh
```

Masukkan kode skrip automasi berikut dengan teliti:

```
#!/bin/bash
# Skrip Automasi Bulk User Provisioning - Lab ASJ SMKN 22 Jakarta
# Pembuat: Fernandez Eko NS

GROUP_NAME="grp-siswa"
PREFIX="siswa-lab"
TOTAL_USERS=20
DEFAULT_PASS="SiswaTKJ#2026"
LOG_FILE="/var/log/tkj-user-provisioning.log"

echo "============================================================" > $LOG_FILE
echo "[*] MEMULAI AUTOMATION PROVISIONING AKUN SISWA SMKN 22" >> $LOG_FILE
echo " -> Tanggal Eksekusi : $(date '+%Y-%m-%d %H:%M:%S')" >> $LOG_FILE
echo " -> Target Group     : $GROUP_NAME" >> $LOG_FILE
echo "============================================================" >> $LOG_FILE

# Memastikan grup siswa sudah ada
if ! getent group $GROUP_NAME > /dev/null 2>&1; then
   groupadd $GROUP_NAME
   echo "[+] Grup $GROUP_NAME berhasil dibuat." >> $LOG_FILE
fi

for i in $(seq -f "%02g" 1 $TOTAL_USERS); do
   USERNAME="${PREFIX}${i}"

   # Periksa apakah user sudah ada
   if id "$USERNAME" >/dev/null 2>&1; then
      echo " [!] Skip: Akun $USERNAME sudah terdaftar di sistem." >> $LOG_FILE
   else
      # Create user dengan home directory dan shell bash
      useradd -m -g $GROUP_NAME -s /bin/bash -c "Peserta Didik Lab TKJ $i" "$USERNAME"

      # Set password secara batch menggunakan chpasswd
      echo "$USERNAME:$DEFAULT_PASS" | chpasswd
```

```
        # Set wajib ganti sandi saat login perdana
        chage -d 0 "$USERNAME"

        echo " [+] Sukses: Akun $USERNAME berhasil dibuat & dikonfigurasi." >> $LOG_FILE
    fi
done

echo "============================================================" >> $LOG_FILE
echo "[*] PROVISIONING SELESAI. TOTAL AKUN DIPROSES: $TOTAL_USERS" >> $LOG_FILE
echo "============================================================" >> $LOG_FILE
```

(Simpan berkas skrip dengan CTRL+O, ENTER, CTRL+X).
2. Berikan hak akses eksekusi (executable permission) pada skrip tersebut:

```
sudo chmod +x /usr/local/bin/tkj-bulk-user.sh
```

3. Eksekusi skrip automasi pembuat akun massal tersebut sebagai root:

```
sudo /usr/local/bin/tkj-bulk-user.sh
```

4. Verifikasi hasil eksekusi skrip melalui pembacaan log dan pemeriksaan berkas /etc/passwd:

```
cat /var/log/tkj-user-provisioning.log
tail -n 5 /etc/passwd
```

Anda akan melihat akun siswa-lab01 hingga siswa-lab20 telah tercipta secara sempurna!

## Langkah 6: Pengujian Hak Akses & Isolasi Direktori (Access Control)

Untuk membuktikan bahwa pengelompokan grup berfungsi melindungi privasi data antar-divisi:
1. Buat direktori kerja rahasia khusus untuk divisi guru di dalam /home/guru-asj/sistem-soal:

```
sudo mkdir -p /home/guru-asj/sistem-soal
sudo chown -R guru-asj:grp-guru /home/guru-asj/sistem-soal
```

2. Set hak akses direktori tersebut menjadi 770 (rwxrwx---), yang berarti hanya pemilik (guru) dan anggota grup (grp-guru) yang boleh membaca dan menulis, sedangkan orang lain (Others/Siswa) diblokir total:

```
sudo chmod 770 /home/guru-asj/sistem-soal
ls -ld /home/guru-asj/sistem-soal
```

3. Uji Validasi Isolasi Akses:
   • Beralih identitas menjadi akun siswa-lab01:

```
su - siswa-lab01
```

   • Coba masuk atau membaca direktori rahasia milik guru:

```
cd /home/guru-asj/sistem-soal
ls -la /home/guru-asj/sistem-soal
```

Sistem akan langsung menolak akses Anda dengan pesan: ls: cannot open directory '/home/guru-asj/sistem-soal': Permission denied. (Isolasi keamanan data laboratorium berhasil sempurna!)
   • Ketik exit untuk kembali ke akun admin.

## Langkah 7: Pembuatan Snapshot Mesin Virtual (Backup Point)

Anda telah menguasai manajemen pengguna, struktur grup, delegasi sudoers, hardening sandi, dan automasi provisioning massal. Amankan kondisi server master ini sebelum melanjutkan modul pembelajaran berikutnya!

1. Matikan server Linux Debian dengan perintah:

```
sudo shutdown -h now
```

2. Pada aplikasi VirtualBox Manager di PC Host, klik pada VM SMKN22-Debian-Server-XI.
3. Klik menu Machine Tools -> pilih Snapshots.
4. Klik tombol Take (Ambil) ikon kamera.
5. Beri nama snapshot baru Anda: Snapshot-02-User-Management-Mastered
   • Description: Modul Manajemen Pengguna selesai. Grup admin, guru, siswa terdaftar. Sudoers visudo NOPASSWD aktif untuk guru. Password aging & account locking teruji. Skrip bulk provisioning tkj-bulk-user.sh aktif.
6. Klik OK.

## L. PERINTAH KONFIGURASI & SPESIFIKASI KODE YAML/SCRIPT

Berikut adalah ringkasan skrip bash (Cheat Sheet / Automated Verifier) yang dapat dijalankan di terminal server untuk melakukan verifikasi cepat terhadap seluruh konfigurasi manajemen pengguna di laboratorium:

```
#!/bin/bash
#
================================================================================
# SCRIPT AUTOMASI VERIFIKASI MANAJEMEN PENGGUNA (LAB ASJ SMKN 22 JAKARTA)
#
================================================================================

echo
"================================================================================"
echo "[1] MEMERIKSA STRUKTUR GRUP DEPARTEMEN SEKOLAH (GID >= 2000)..."
echo "--------------------------------------------------------------------------------"
getent group | grep -E '(grp-admin|grp-guru|grp-siswa)' | awk -F: '{print " -> Nama Grup: " $1 "\t\tGID: " $3
"\tAnggota: " $4}'
echo
"================================================================================"

echo "[2] MEMERIKSA AKUN UTAMA & ALOKASI SHELL SISTEM..."
printf "%-15s %-8s %-12s %-20s %-15s\n" "USERNAME" "UID" "GRUP UTAMA" "DIREKTORI HOME"
"LOGIN SHELL"
echo "--------------------------------------------------------------------------------"
users=("admin-asj" "guru-asj" "siswa01" "web-daemon" "siswa-lab01")
for u in "${users[@]}"; do
  if id "$u" >/dev/null 2>&1; then
    uid=$(id -u $u)
    gid=$(id -gn $u)
    home=$(getent passwd $u | cut -d: -f6)
    shell=$(getent passwd $u | cut -d: -f7)
    printf "%-15s %-8s %-12s %-20s %-15s\n" "$u" "$uid" "$gid" "$home" "$shell"
  else
    printf "%-15s [! AKUN TIDAK TERDAFTAR DI SISTEM !]\n" "$u"
  fi
done
echo
"================================================================================"

echo "[3] MEMERIKSA ATURAN DELEGASI PRIVILESE SUDOERS (/etc/sudoers)..."
echo "--------------------------------------------------------------------------------"
sudo grep -E '(admin-asj|guru-asj|grp-admin)' /etc/sudoers | grep -v '^#' | sed 's/^/ -> /'
echo
"================================================================================"
```

```
echo "[4] MEMERIKSA STATUS KEBIJAKAN PASSWORD AGING (AKUN: siswa01)..."
echo "--------------------------------------------------------------------------------"
if id "siswa01" >/dev/null 2>&1; then
    sudo chage -l siswa01 | grep -E '(Maximum|Minimum|Password expires|Account expires)' | sed 's/^/ -> /'
fi
echo
"================================================================================"

echo "[5] MEMERIKSA HASIL PROVISIONING MASSAL (TOTAL AKUN SISWA-LAB)..."
TOTAL_BULK=$(getent passwd | grep -c '^siswa-lab')
echo " -> Total akun 'siswa-lab' yang terdeteksi pada sistem : $TOTAL_BULK Akun"
if [ -f "/var/log/tkj-user-provisioning.log" ]; then
    echo " -> Log Eksekusi Terakhir:"
    tail -n 3 /var/log/tkj-user-provisioning.log | sed 's/^/    /'
fi
echo
"================================================================================"
```

## M. LEMBAR HASIL PRAKTIKUM

Lengkapi lembar observasi laboratorium berikut berdasarkan hasil pengujian nyata pada mesin virtual Debian Server Anda:

| Tahapan & Parameter Uji | Target Hasil yang Diharapkan | Status & Catatan Hasil Pengujian |
|---|---|---|
| 1. Verifikasi Berkas Identitas | Berkas /etc/passwd dapat dibaca umum (-rw-r--r--), sedangkan /etc/shadow terproteksi root/shadow. | [ ] Ya [ ] Tidak<br>Algoritma Hash Shadow: ..... |
| 2. Pembuatan Grup Sekolah | Tiga grup utama (grp-admin, grp-guru, grp-siswa) terdaftar dengan GID 2001, 2002, 2003. | [ ] Ya [ ] Tidak<br>GID grp-guru: ..... |
| 3. Akun Admin & Pengajar | Akun admin-asj (UID 2001) dan guru-asj (UID 2002) aktif dengan shell /bin/bash. | [ ] Ya [ ] Tidak<br>UID admin-asj: ..... |
| 4. Akun System Daemon | Akun web-daemon (UID | [ ] Ya [ ] Tidak |

| | | |
|---|---|---|
| | 990) terdaftar dengan pembatasan shell /usr/sbin/nologin. | Status Shell Daemon: ..... |
| 5. Sintaks Sudoers (visudo) | Modifikasi /etc/sudoers berhasil disimpan tanpa ada pesan syntax error dari visudo. | [ ] Ya [ ] Tidak<br>Pesan Validasi Visudo: ..... |
| 6. Uji Delegasi NOPASSWD | Akun guru-asj dapat menjalankan sudo systemctl restart ssh tanpa diminta kata sandi. | [ ] Ya [ ] Tidak<br>Respon Perintah Sudo: ..... |
| 7. Uji Pembatasan Sudo | Akun guru-asj ditolak (Sorry, not allowed) saat mencoba mengeksekusi sudo useradd. | [ ] Ya [ ] Tidak<br>Pesan Penolakan: ..... |
| 8. Password Aging (chage) | Akun siswa01 terkonfigurasi masa pakai sandi maks 30 hari dan kedaluwarsa saat login perdana. | [ ] Ya [ ] Tidak<br>Max Password Days: ..... |
| 9. Penguncian Akun (lock) | Akun siswa01 yang dikunci (usermod -L) memiliki tanda seru (!) pada string hash shadow-nya. | [ ] Ya [ ] Tidak<br>Karakter Awal Hash: ..... |
| 10. Skrip Bulk Provisioning | Eksekusi /usr/local/bin/tkj-bulk-user.sh sukses menciptakan 20 akun siswa serentak di /etc/passwd. | [ ] Ya [ ] Tidak<br>Total Akun Tercipta: ..... |
| 11. Isolasi Direktori Guru | Akun siswa ditolak (Permission denied) saat mencoba masuk ke /home/guru-asj/sistem-soal. | [ ] Ya [ ] Tidak<br>Kode Hak Akses (Octal): ..... |

## N. TROUBLESHOOTING & PEMECAHAN MASALAH (TP 5.1.1.5)

Dalam mengelola akun dan hak akses, teknisi kerap dihadapkan pada kendala otentikasi dan permisi. Tabel berikut merangkum diagnosis dan solusi untuk pesan kesalahan umum di laboratorium:

| Gejala / Pesan Error yang Muncul | Kemungkinan Penyebab Utama | Solusi Diagnostik & Langkah Perbaikan |
|---|---|---|
| Error: useradd: user 'guru-asj' already exists | Username yang ingin Anda buat telah terdaftar di dalam sistem pada sesi praktikum sebelumnya. | 1. Periksa keberadaan akun dengan: id guru-asj<br>2. Jika ingin membuat ulang, hapus akun lama beserta direktori home-nya terlebih dahulu: sudo userdel -r guru-asj<br>3. Jalankan kembali perintah useradd Anda. |
| Error: guru-asj is not in the sudoers file. This incident will be reported. | Akun tersebut mencoba menjalankan perintah sudo, namun namanya belum didaftarkan di dalam aturan /etc/sudoers atau keanggotaan grup sudo. | 1. Login kembali sebagai root atau sysadmin<br>2. Buka konfigurasi: sudo visudo<br>3. Pastikan baris aturan wewenang guru-asj telah ditulis dengan tepat tanpa salah ketik nama akun. |
| Error: visudo: >>> /etc/sudoers: syntax error near line 28 <<< | Anda melakukan kesalahan penulisan sintaks (misal lupa tanda sama dengan = atau salah penempatan tanda titik dua :) saat mengedit berkas sudoers. | 1. JANGAN KELUAR dari editor atau menekan tombol abaikan.<br>2. Ketika prompt visudo muncul, pilih opsi (e)dit sudoers file again.<br>3. Perbaiki baris yang ditunjuk oleh pesan error (baris 28), lalu simpan kembali. |
| Error: su: Authentication failure atau tidak bisa login SSH padahal sandi benar | 1. Akun pengguna sedang dalam status terkunci (locked) oleh administrator | 1. Periksa status penguncian akun di shadow: sudo grep username /etc/shadow |

| | | |
|---|---|---|
| | (usermod -L).<br>2. Masa berlaku sandi telah habis (expired) dan melewati batas masa tenggang chage.<br>3. Shell akun diset ke /usr/sbin/nologin. | (periksa apakah ada tanda ! di awal hash).<br>2. Buka kunci akun dengan: sudo usermod -U username<br>3. Periksa shell akun di /etc/passwd. Jika bernilai nologin, ubah menjadi /bin/bash menggunakan sudo usermod -s /bin/bash username. |
| Error: userdel: user siswa01 is currently used by process 1420 | Anda mencoba menghapus akun pengguna, namun akun tersebut sedang aktif login atau memiliki proses latar belakang yang masih berjalan di server. | 1. Lihat proses apa yang sedang dijalankan oleh pengguna tersebut: ps -u siswa01<br>2. Hentikan paksa seluruh proses milik pengguna tersebut: sudo killall -u siswa01<br>3. Setelah proses bersih, jalankan kembali penghapusan: sudo userdel -r siswa01. |
| Skrip tkj-bulk-user.sh gagal dijalankan dengan pesan Permission denied | Berkas skrip automasi yang Anda buat belum diberi hak akses eksekusi oleh sistem operasi. | 1. Periksa hak akses berkas skrip: ls -l /usr/local/bin/tkj-bulk-user.sh<br>2. Berikan izin eksekusi kepada berkas tersebut: sudo chmod +x /usr/local/bin/tkj-bulk-user.sh<br>3. Jalankan kembali skrip dengan prefix sudo. |

## O. ANALISIS & STUDI KASUS TEKNIS

1. Analisis Prinsip Least Privilege pada Sudoers: Dalam sebuah insiden peretasan server web, penyerang berhasil mengambil alih akun www-data (akun web server). Jika administrator server tersebut sebelumnya secara teledor memasukkan baris www-data ALL=(ALL) ALL ke

dalam /etc/sudoers, jelaskan dampak bencana yang akan terjadi pada sistem pusat data sekolah! Mengapa pemisahan hak akses menggunakan parameter NOPASSWD yang spesifik (seperti pada akun guru-asj) sangat krusial dalam mitigasi serangan siber?

2. Analisis Evolusi Keamanan Berkas Shadow: Pada era awal Linux dan Unix klasik, string hash kata sandi disimpan langsung di dalam berkas /etc/passwd (kolom kedua). Mengapa pendekatan klasik tersebut menjadi cacat keamanan yang sangat berbahaya pada sistem multi-user modern? Jelaskan peran teknik Salting dan algoritma Key Derivation Function (seperti yescrypt atau SHA-512) pada /etc/shadow dalam mencegah serangan peretasan tipe Rainbow Table Attack!

3. Analisis Arsitektur PAM (Pluggable Authentication Modules): Ketika seorang pengguna mencoba login via SSH atau su, perintah tersebut tidak memverifikasi kata sandi secara mandiri, melainkan menyerahkannya kepada subsistem PAM (/etc/pam.d/). Jelaskan keuntungan arsitektur modular PAM bagi seorang System Administrator! Apa yang harus dikonfigurasi pada PAM jika sekolah ingin menerapkan aturan: 'Kata sandi baru minimal harus 12 karakter dan wajib mengandung perpaduan huruf, angka, dan simbol'?

4. Analisis Kebijakan Offboarding & Zombie Accounts: Saat siswa kelas XII lulus dari SMK Negeri 22 Jakarta, ratusan akun praktikum mereka menjadi tidak terpakai (Zombie Accounts). Berdasarkan pertimbangan keamanan data dan manajemen kapasitas penyimpanan (Disk Quota), bandingkan kelebihan dan kekurangan antara tindakan Mengunci Akun (usermod -L) versus Menghapus Akun Beserta Home Directory (userdel -r)! Prosedur SOP mana yang paling ideal diterapkan oleh sekolah?

5. Konsep Sticky Bit & Isolasi Direktori Kolaborasi: Jika guru ASJ ingin membuat sebuah direktori pertukaran tugas di /home/share-tugas di mana seluruh siswa (grp-siswa) dapat membuat dan membaca berkas di dalamnya, namun satu siswa tidak boleh menghapus atau memodifikasi berkas karya siswa lainnya, parameter izin khusus (Special File Permissions) apa yang harus diterapkan pada direktori tersebut? (Petunjuk: Jelaskan konsep dan cara kerja atribut Sticky Bit pada direktori publik).

## P. REFLEKSI PESERTA DIDIK

| Aspek Refleksi Pembelajaran | Catatan Evaluasi Diri Peserta Didik |
|---|---|
| 1. Kompetensi Teknis Baru yang Diperoleh | Tuliskan minimal 3 keahlian teknis baru yang Anda kuasai setelah menyelesaikan proyek manajemen pengguna Linux ini:<br>1. .....<br>2. .....<br>3. ..... |

| | |
|---|---|
| | ..... |
| 2. Kendala & Hambatan Selama Praktikum | Jelaskan kesulitan teknis, pesan error, atau kegagalan otentikasi hak akses yang Anda alami selama praktikum berlangsung:<br>.....<br>.....<br>.....<br>..... |
| 3. Solusi & Langkah Perbaikan yang Diterapkan | Bagaimana cara Anda memecahkan masalah atau error teknis tersebut? (Sebutkan perintah diagnostik atau referensi log yang digunakan):<br>.....<br>.....<br>.....<br>..... |
| 4. Rencana Pengembangan & Eksplorasi Lanjutan | Tuliskan rencana Anda untuk memperdalam keahlian otentikasi (misal: mencoba integrasi login Linux dengan LDAP/Active Directory, atau konfigurasi Quota Disk):<br>.....<br>.....<br>.....<br>..... |

## Q. RUBRIK PENILAIAN PROYEK (KKTP)

Penilaian hasil praktikum mandiri menggunakan rubrik penilaian berbasis proyek (Project-Based Learning Rubric) dengan skala 1–4, yang diturunkan dari Kriteria Ketercapaian Tujuan Pembelajaran (KKTP) Elemen ASJ Fase F (khususnya TP 5.1.1). Peserta didik dinyatakan Tercapai apabila indikator esensial terpenuhi dengan predikat minimal Baik (Skala 3).

| Komponen Penilaian | Bobot | Perlu Bimbingan (1) | Cukup (2) | Baik / Tercapai (3) | Sangat Baik (4) |
|---|---|---|---|---|---|
| 1. Analisis & | 15% | Belum | Memahami | Menjelaskan | Menganalisis |

| | | | | | |
|---|---|---|---|---|---|
| Perencanaan Proyek | | memahami struktur berkas identitas (/etc/passwd); skema alokasi UID/GID tidak disiapkan. | fungsi passwd & shadow, namun masih membutuhkan bimbingan dalam memetakan struktur grup. | struktur identitas Linux, merancang skema grup sekolah (admin, guru, siswa) dengan UID teratur. | keamanan enkripsi shadow dengan kritis, merancang topologi RBAC yang sempurna, dan menyusun skema mitigasi error. |
| 2. Kontrol Akun & Hak Akses Grup | 35% | Gagal mengoperasikan perintah useradd/groupadd; salah menentukan parameter direktori home dan shell. | Mampu membuat akun reguler, namun gagal menerapkan pengelompokan grup dan isolasi shell system (nologin). | Menguasai siklus hidup akun, sukses memetakan grup departemen, dan membatasi shell akun daemon dengan tepat. | Sangat terampil mengontrol akun, mampu mengonfigurasi multi-grup suplemen, serta menerapkan audit hak pakai direktori (chmod). |
| 3. Delegasi Sudoers & Hardening | 25% | Mengedit sudoers tanpa visudo (berisiko error); gagal menerapkan pembatasan perintah dan umur sandi. | Menggunakan visudo setelah dibimbing; berhasil membuat aturan sudo namun masih bersifat | Berhasil mengonfigurasi delegasi NOPASSWD untuk guru; menerapkan password aging (chage) dan | Menyelesaikan konfigurasi visudo tanpa error, menerapkan prinsip Least Privilege sempurna, dan menguji |

| | | | | | |
|---|---|---|---|---|---|
| | | | terlalu luas (kurang aman). | penguncian akun. | penguncian otentikasi. |
| 4. Automasi Provisioning & Scripting | 15% | Tidak mampu membuat skrip Bash automasi; pembuatan akun massal masih dilakukan manual satu per satu. | Mampu menulis dasar skrip bulk user, tetapi error pada looping atau gagal mengonfigurasi sandi via chpasswd. | Skrip tkj-bulk-user.sh berhasil dieksekusi dan menciptakan 20 akun siswa serentak dengan parameter yang rapi. | Skrip automasi sangat robust, dilengkapi validasi pengecekan akun ganda, sistem logging detail, dan struktur kode berstandar industri. |
| 5. Dokumentasi, SOP, & K3LH | 10% | Tidak menyusun laporan kerja; melanggar SOP (mengedit sudoers pakai nano tanpa root pengaman). | Laporan kerja seadanya; masih perlu diingatkan untuk melakukan pengujian otentikasi setelah modifikasi akun. | Laporan teknis lengkap, mencatat logbook UID/GID, mematuhi SOP keselamatan, dan sukses membuat cadangan Snapshot. | Laporan berstandar industri, dokumentasi sangat sistematis dan replikatif, menjaga kerapian lab, serta menjadi tutor sebaya. |

## R. FORMAT DAN SISTEMATIKA LAPORAN PRAKTIKUM

Peserta didik wajib menyusun laporan akhir praktikum mandiri dalam format cetak atau PDF dengan sistematika penulisan standar industri sebagai berikut:

1. HALAMAN SAMPUL / COVER: Judul Proyek (Manajemen Pengguna, Hak Akses Sudoers, dan Automasi Provisioning Linux Server), Identitas Peserta Didik, NISN, Kelas, Nama Sekolah, dan Tahun Pelajaran.

2. BAB I: PENDAHULUAN: Latar Belakang Proyek (Urgensi keamanan otentikasi, pembatasan hak superuser, dan efisiensi manajemen identitas di sekolah), Tujuan Pembelajaran Operasional (TP 5.1.1), Batasan Masalah dan Spesifikasi Implementasi Klasifikasi Akun.

3. BAB II: LANDASAN TEORI: Arsitektur Identitas dan Otentikasi Linux (Anatomi /etc/passwd, /etc/shadow, /etc/group), Konsep Role-Based Access Control (RBAC) dan Prinsip Least Privilege, Aturan Delegasi Privilese Menggunakan Sudoers dan Keunggulan Utiliti visudo, Subsistem Password Aging (chage) dan Pluggable Authentication Modules (PAM).

4. BAB III: METODOLOGI & PERANCANGAN SISTEM: Alat dan Bahan yang Digunakan (Spesifikasi PC Host & Mesin Virtual Debian Server), Gambar Topologi Arsitektur Klasifikasi Pengguna dan Pemetaan Grup (UID 0, 1-999, >=1000), Diagram Alur (Flowchart) Prosedur Audit Akun, Delegasi Sudoers, dan Eksekusi Skrip Provisioning Massal.

5. BAB IV: HASIL DAN PEMBAHASAN: Dokumentasi Langkah Kerja dan Konfigurasi (Disertai bukti tangkapan layar terminal Linux yang relevan), Bukti Eksekusi Delegasi Sudoers (Tangkapan layar hasil sudo -l akun guru dan penolakan sudo akun siswa), Bukti Hardening Akun dan Provisioning Massal (Tangkapan layar chage -l, shadow lock, dan isi log /var/log/tkj-user-provisioning.log), Pembahasan Analisis Troubleshooting dan Temuan Kendala Teknis di Laboratorium, Jawaban Lengkap dari Pertanyaan Analisis & Studi Kasus Teknis (Bagian O).

6. BAB V: PENUTUP: Kesimpulan Hasil Implementasi Proyek Manajemen Pengguna Linux Server, Saran dan Rekomendasi Pengembangan (misalnya integrasi autentikasi terpusat dengan LDAP/Active Directory atau konfigurasi Quota Disk).

7. LAMPIRAN (APPENDIX): Salinan Teks Berkas Konfigurasi Lengkap (Aturan delegasi /etc/sudoers dan kode skrip /usr/local/bin/tkj-bulk-user.sh), Salinan Bukti Tampilan Antarmuka VirtualBox Manager yang menampilkan Snapshot-02, Lembar Hasil Praktikum (Bagian M) yang telah diverifikasi dan ditandatangani oleh Guru Mata Pelajaran.

Mengetahui/Menyetujui,
Kepala SMK Negeri 22 Jakarta

Jaringan

Lia Adawiyah, S.Pd.
NIP. 198004052008012031

Jakarta, 17 Juli 2026
Guru Administrasi Sistem

Fernandez Eko NS
NIP. 198612162022211008