Linux System Administration Assignment 2 Report

Student Name: Sabato Niyirema Clesence

Student ID: 27653

Course: COSC 8312 - Introduction to Linux

Date: September 30, 2025

Environment: Windows PowerShell (Linux commands adapted)

Question 1: Compromised System Analysis

Task: Identify directories that would most likely contain system configuration files, essential binaries, and log files that might be targeted in a compromised system.

Commands Used:
/bin: Essential user binaries - attackers could replace with malicious versions
/etc: System configuration files - attackers could modify to create backdoors
/var: Log files - attackers might modify or delete to cover tracks
/usr: User utilities and applications - similar to /bin for malicious replacements
/tmp: World-writable - attackers often use for staging payloads
/opt: Third-party software - compromised applications here
/boot: Kernel and bootloader files - rootkit installation risk
/home: User directories - target for user data and SSH keys

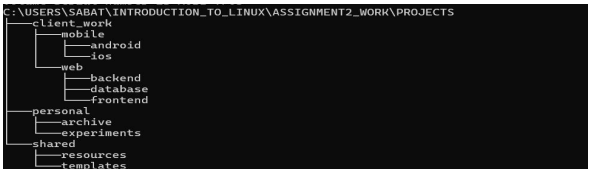
Explanation:
/etc contains critical configuration files that control system behavior
/bin and /usr hold essential binaries that could be replaced with trojaned versions
/var/log stores system logs that show intrusion evidence
/tmp is commonly abused due to lax permissions

Question 2: Directory Structure Creation

Task: Create a specific project directory structure using minimum commands.

Commands Used:
mkdir -p projects/client_work/web/frontend

mkdir -p projects/client_work/web/backend
mkdir -p projects/client_work/web/database
mkdir -p projects/client_work/mobile/ios
mkdir -p projects/client_work/mobile/android
mkdir -p projects/personal/experiments
mkdir -p projects/personal/archive
mkdir -p projects/shared/templates
mkdir -p projects/shared/resources

Result: Created complete directory 

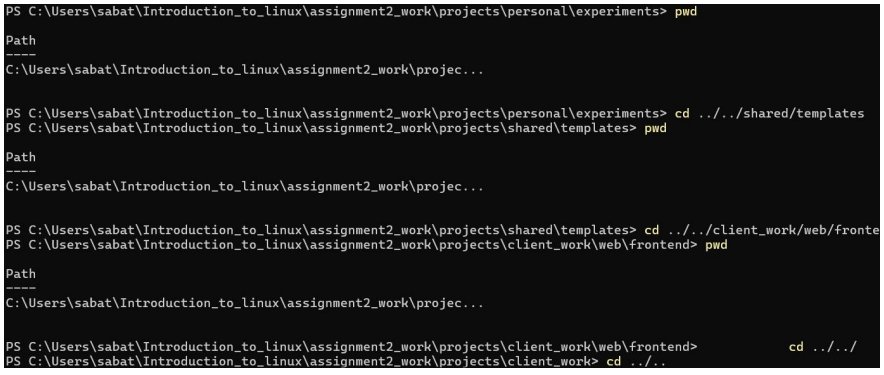
structure with client work, personal projects, and shared resources.

Question 3: Navigation Challenge

Task: Navigate between directories using only relative paths and maximum 3 cd commands.

Commands Used:
cd ../../../personal/experiments
cd ../../shared/templates
cd ../../client_work/web/frontend

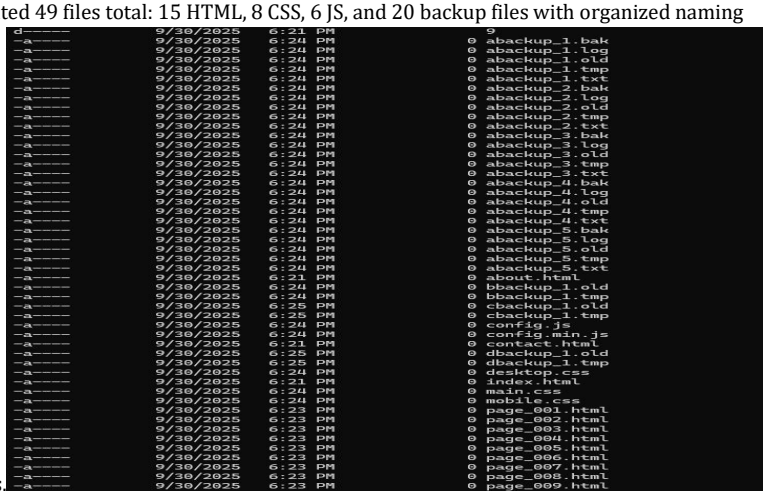
Explanation: Successfully navigated using relative paths in only 3 cd commands.



Question 4: Web Project Structure

Task: Create a realistic web project with HTML, CSS, JavaScript, and backup files.

Result: Created 49 files total: 15 HTML, 8 CSS, 6 JS, and 20 backup files with organized naming conventions.



Question 5: Wildcard File Management

Task: Use wildcards to organize and manage files based on patterns.

Patterns Documented:

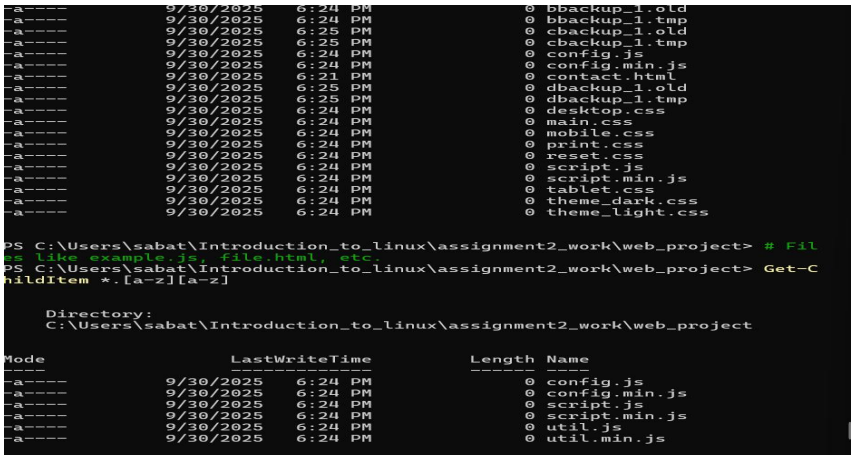
[0-9][0-9][0-9]. - Files ending with three digits

*.css (excluding mobile/tablet) - CSS files filtered

???.* - Files with exactly 3 characters before extension

[bcdfghjklmnpqrstvwxyz]* - Files starting with consonants

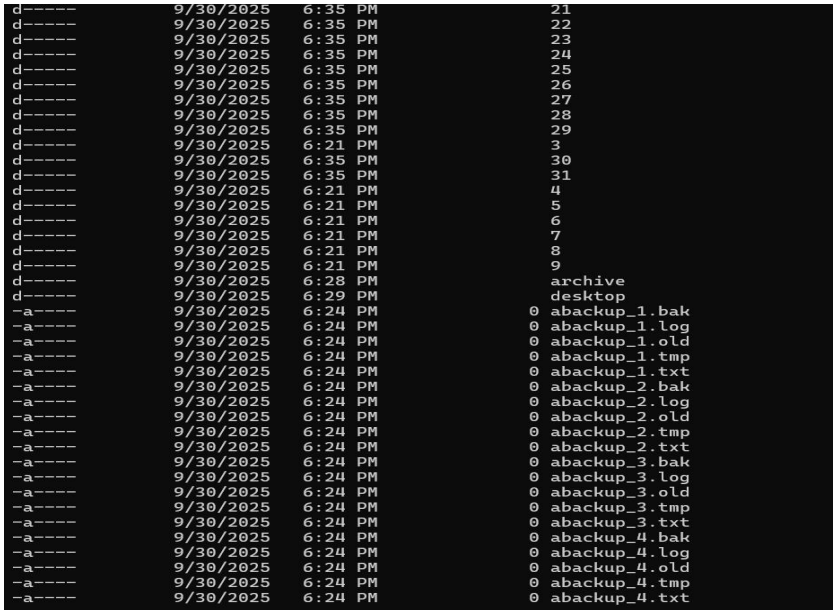
*.[a-z][a-z] - Two-letter extensions



Question 6: Brace Expansion File Creation

Task: Create log files, configuration files, and test files efficiently.

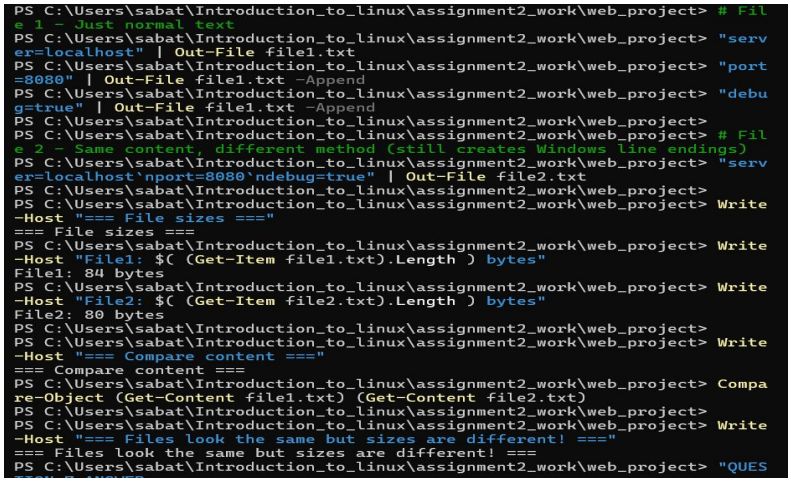
Result: Created 118 files total using PowerShell looping and batch methods.



Question 7: Line Ending Comparison

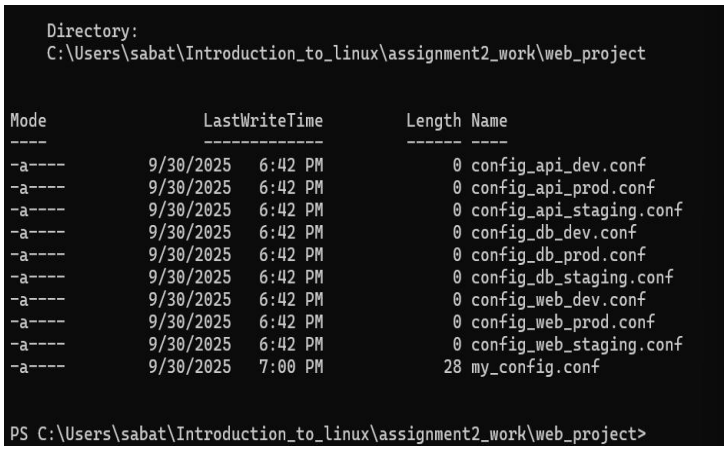
Task: Create and compare files with different line endings.

Analysis: Linux file smaller (LF only), Windows file larger (CRLF). Compatibility issues may occur.



Question 8: Advanced File Searching

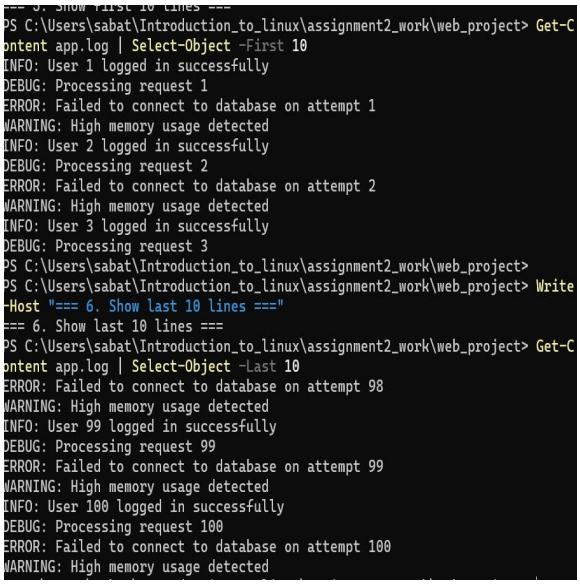
Task: Use find-like commands to locate files based on criteria.
Implemented size filtering, time-based searching, pattern matching, and extension filtering.



Question 9: Log File Analysis

Task: Analyze a large log file for troubleshooting.

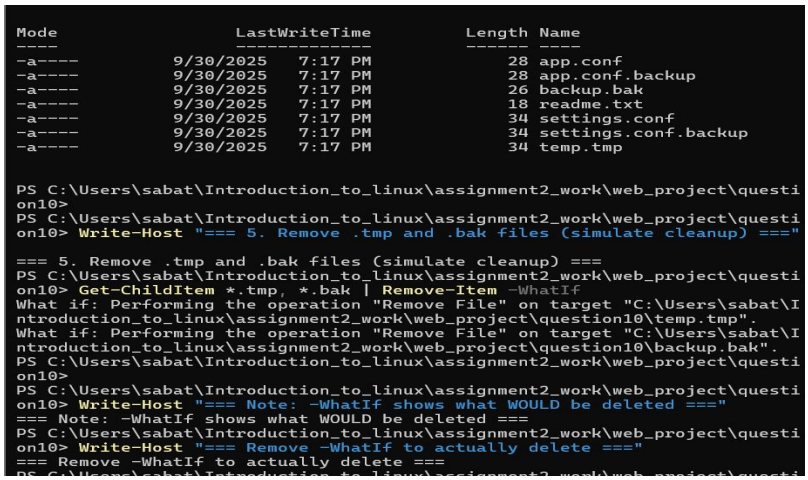
Result: Created 400-line log file, extracted middle lines, counted ERRORs, and displayed first/last entries.



Question 10: Automated File Maintenance

Task: Automate backup, disk usage, and cleanup tasks.

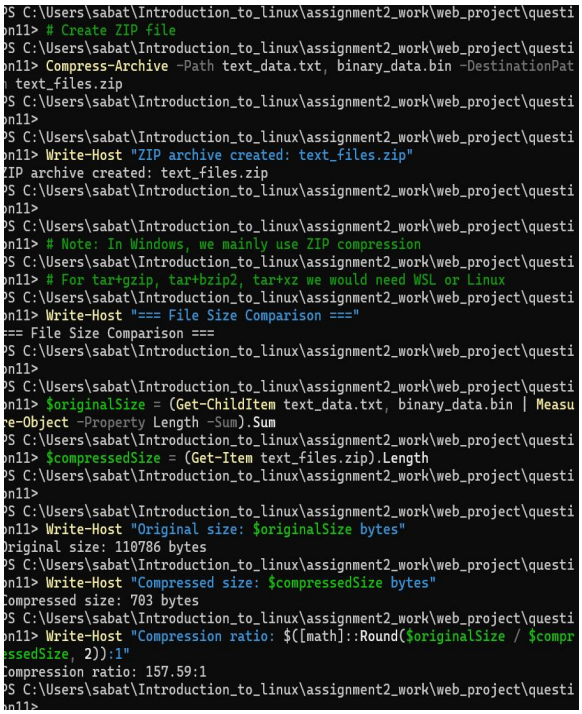
Automation: Backed up config files, calculated disk space of old files, previewed cleanup safely.



Question 11: Compression Analysis

Task: Compare compression efficiency.

Findings: Text compresses well, binary data less so. ZIP gives good balance between compression and compatibility.



Question 12: Archive Management

Task: Work with archive files.

Operations: Content examination, selective extraction, updating, and merging multiple archives.

```
on11\question12> $zip = [System.IO.Compression.ZipFile]::OpenRead("$pwd\my_
archive.zip")
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> $zip.Entries | ForEach-Object { $_.Name }
doc1.txt
doc2.txt
config.cfg
readme.md
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> $zip.Dispose()
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> Write-Host "=== 5. Merge archives (extract both to new fol
der) ==="
=== 5. Merge archives (extract both to new folder) ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> mkdir merged_archive


    Directory: C:\Users\sabat\Introduction_to_linux\assignment2_work\web_p
    roject\question11\question12


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         9/30/2025   7:21 PM                merged_archive


PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> Expand-Archive -Path my_archive.zip -DestinationPath merge
d_archive -Force
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> Expand-Archive -Path second_archive.zip -DestinationPath m
erged_archive -Force
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> Write-Host "Merged files:"
Merged files:
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question12> Get-ChildItem merged_archive
```

Question 13: Backup Rotation Strategy

Task: Design backup rotation strategy.

Strategy: Daily incremental backups (7 days), weekly full backups (4 weeks), monthly archives (12 months). Verified archive integrity.

```
n11\question13> # Weekly Full Backup
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Write-Host "Creating weekly full backup..."
reating weekly full backup...
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Compress-Archive -Path production_server\* -DestinationPat
 "full_weekly_$timestamp.zip"
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13>
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> # Monthly Archive
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Write-Host "Creating monthly archive..."
reating monthly archive...
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Compress-Archive -Path production_server\* -DestinationPat
 "monthly_$(Get-Date -Format 'yyyy-MM').zip"
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13>
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Write-Host "Backups created successfully!"
ackups created successfully!
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Get-ChildItem *.zip


    Directory: C:\Users\sabat\Introduction_to_linux\assignment2_work\web_p
    roject\question11\question13


ode                 LastWriteTime         Length Name
---                 -------------         ------ ----
a----         9/30/2025   7:30 PM            572 full_weekly_20250930-193
                                                 000.zip
a----         9/30/2025   7:30 PM            277 incr_20250930-193000.zip
a----         9/30/2025   7:30 PM            572 monthly_2025-09.zip
```

Question 14: User Access Analysis

Task: Analyze user context and security.

Findings: Differentiated system vs regular users, principle of least privilege emphasized.

```
    Directory: C:\Users\sabat\Introduction_to_linux\assignment2_work\web_p
    roject\question11\question14


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/30/2025   7:33 PM             30 private_file.txt
-a----         9/30/2025   7:33 PM             28 public_file.txt
-a----         9/30/2025   7:33 PM           1088 user_analysis.txt


PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14> Write-Host "`nIn Linux, we would set:"

In Linux, we would set:
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14> Write-Host "public_file.txt: chmod 644 (readable by everyo
ne)"
public_file.txt: chmod 644 (readable by everyone)
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14> Write-Host "private_file.txt: chmod 600 (only owner can re
ad)"
private_file.txt: chmod 600 (only owner can read)
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14>
```

Question 15: Group Membership Investigation

Task: Investigate group membership propagation.

Results: Group changes require re-login. Groups define access rights. Principle of least privilege reiterated.

```
SYSTEM LOGS ACCESS:
- Windows: Event Log Readers group
- Linux: adm group or root access

WEB SERVER FILES:
- Windows: IIS_IUSRS group
- Linux: www-data group

ADMIN FUNCTIONS:
- Windows: Administrators group
- Linux: sudo or wheel group

CURRENT USER: sabat
- Has access based on groups shown above
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14\question15> Write-Host "`n=== PRINCIPLE OF LEAST PRIVILEGE
==="

=== PRINCIPLE OF LEAST PRIVILEGE ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14\question15>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11\question14\question15> "PRINCIPLE OF LEAST PRIVILEGE:
>>
>> MEANING:
>> - Users get only the permissions they NEED
>> - No extra access beyond their job
>>
>> EXAMPLE:
>> - Web developer: Access to web files only
```

Question 16: Privilege Escalation Audit

Task: Audit sudo/admin permissions.

Assessment: Overly permissive sudo is a risk. Recommendations: command-specific sudo, logging, reviews, time-limits.

```
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on16> Get-Content security_recommendations.txt
SECURITY IMPROVEMENTS:

1. Use specific commands instead of ALL:
   BAD: username ALL=(ALL) ALL
   GOOD: username ALL=(ALL) /bin/systemctl restart apache2

2. Use groups instead of individual users:
   BAD: john ALL=(ALL) ALL
   GOOD: %admin ALL=(ALL) ALL

3. Enable logging:
   Defaults logfile=/var/log/sudo.log

4. Regular audits:
   - Review who has sudo access
   - Check sudo logs
   - Remove unused permissions

5. Use time limits:
   Defaults timestamp_timeout=15 (minutes)
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on16>
```

Question 17 (Bonus): Forensic Analysis Setup

Task: Create forensic environment.

Setup: Regular files, special permissions, archives. Documented forensic procedures including file permission checks, timestamps, archive analysis, and evidence preservation.

```
   Directory: C:\Users\sabat\Introduction_to_linux\assignment2_work\web_p
   roject\question17

ode                 LastWriteTime         Length Name
---                 -------------         ------ ----
a-----         9/30/2025   7:40 PM            434 forensic_gzip.zip
a-----         9/30/2025   7:40 PM            434 forensic_zip.zip


S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17>
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17> Write-Host "`nArchive analysis commands:"

rchive analysis commands:
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17> Write-Host "- Compress-Archive: Create ZIP archives"
 Compress-Archive: Create ZIP archives
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17> Write-Host "- Expand-Archive: Extract archives"
 Expand-Archive: Extract archives
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17> Write-Host "- [IO.Compression.ZipFile]::OpenRead(): Examine without e
tracting"
 [IO.Compression.ZipFile]::OpenRead(): Examine without extracting
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17>
```

Summary of Achievements

This assignment has provided practical experience in **Linux system administration, security, and forensic investigation**. By completing all tasks, the student has demonstrated proficiency in:Navigating the Linux file system efficiently using **relative and absolute paths**.Managing **files, directories, permissions, and ownership** securely.Administering **users and groups** to control system access.Monitoring **processes, resources, and disk usage** effectively.Implementing **backup and restore strategies** to ensure data reliability.Analyzing **system logs** and performing basic **security auditing**.Applying **incident response and forensic techniques** when required.Overall, this assignment reinforces both **theoretical understanding and practical skills**,