

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

```

```

C:\Users\Sabat\Introduction_to_Linux\Assignment2_Work\Projects
├── client_work
│   ├── mobile
│   │   ├── android
│   │   └── ios
│   └── web
│       ├── backend
│       ├── database
│       └── frontend
├── personal
│   ├── archive
│   ├── experiments
│   └── resources
└── shared
    ├── templates

```

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.

```

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\personal\experiments> pwd
Path
----
C:\Users\sabat\Introduction_to_linux\assignment2_work\projec...

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\personal\experiments> cd ../../shared/templates
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\shared\templates> pwd
Path
----
C:\Users\sabat\Introduction_to_linux\assignment2_work\projec...

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\shared\templates> cd ../../client_work/web/fronte
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\client_work\web\frontend> pwd
Path
----
C:\Users\sabat\Introduction_to_linux\assignment2_work\projec...

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\client_work\web\frontend> cd ../../
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\projects\client_work> cd ../../

```

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

```
d----- 9/30/2025 6:21 PM          9
-a----- 9/30/2025 6:24 PM          0 abackup_1.bak
-a----- 9/30/2025 6:24 PM          0 abackup_1.log
-a----- 9/30/2025 6:24 PM          0 abackup_1.old
-a----- 9/30/2025 6:24 PM          0 abackup_1.tmp
-a----- 9/30/2025 6:24 PM          0 abackup_1.txt
-a----- 9/30/2025 6:24 PM          0 abackup_2.bak
-a----- 9/30/2025 6:24 PM          0 abackup_2.log
-a----- 9/30/2025 6:24 PM          0 abackup_2.old
-a----- 9/30/2025 6:24 PM          0 abackup_2.tmp
-a----- 9/30/2025 6:24 PM          0 abackup_2.txt
-a----- 9/30/2025 6:24 PM          0 abackup_3.bak
-a----- 9/30/2025 6:24 PM          0 abackup_3.log
-a----- 9/30/2025 6:24 PM          0 abackup_3.old
-a----- 9/30/2025 6:24 PM          0 abackup_3.tmp
-a----- 9/30/2025 6:24 PM          0 abackup_3.txt
-a----- 9/30/2025 6:24 PM          0 abackup_4.bak
-a----- 9/30/2025 6:24 PM          0 abackup_4.log
-a----- 9/30/2025 6:24 PM          0 abackup_4.old
-a----- 9/30/2025 6:24 PM          0 abackup_4.tmp
-a----- 9/30/2025 6:24 PM          0 abackup_4.txt
-a----- 9/30/2025 6:24 PM          0 abackup_5.bak
-a----- 9/30/2025 6:24 PM          0 abackup_5.log
-a----- 9/30/2025 6:24 PM          0 abackup_5.old
-a----- 9/30/2025 6:24 PM          0 abackup_5.tmp
-a----- 9/30/2025 6:24 PM          0 abackup_5.txt
-a----- 9/30/2025 6:21 PM          0 about.html
-a----- 9/30/2025 6:24 PM          0 bbackup_1.old
-a----- 9/30/2025 6:24 PM          0 bbackup_1.tmp
-a----- 9/30/2025 6:25 PM          0 cbackup_1.old
-a----- 9/30/2025 6:25 PM          0 cbackup_1.tmp
-a----- 9/30/2025 6:24 PM          0 config.js
-a----- 9/30/2025 6:24 PM          0 config.min.js
-a----- 9/30/2025 6:21 PM          0 contact.html
-a----- 9/30/2025 6:25 PM          0 dbackup_1.old
-a----- 9/30/2025 6:25 PM          0 dbackup_1.tmp
-a----- 9/30/2025 6:24 PM          0 desktop.css
-a----- 9/30/2025 6:21 PM          0 index.html
-a----- 9/30/2025 6:24 PM          0 main.css
-a----- 9/30/2025 6:24 PM          0 mobile.css
-a----- 9/30/2025 6:23 PM          0 page_001.html
-a----- 9/30/2025 6:23 PM          0 page_002.html
-a----- 9/30/2025 6:23 PM          0 page_003.html
-a----- 9/30/2025 6:23 PM          0 page_004.html
-a----- 9/30/2025 6:23 PM          0 page_005.html
-a----- 9/30/2025 6:23 PM          0 page_006.html
-a----- 9/30/2025 6:23 PM          0 page_007.html
-a----- 9/30/2025 6:23 PM          0 page_008.html
-a----- 9/30/2025 6:23 PM          0 page_009.html
```

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

[bcdfhgijklmnpqrstvwxyz]* - Files starting with consonants

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

```
-a----- 9/30/2025 6:24 PM          0 bbackup_1.old
-a----- 9/30/2025 6:24 PM          0 bbackup_1.tmp
-a----- 9/30/2025 6:25 PM          0 cbackup_1.old
-a----- 9/30/2025 6:24 PM          0 cbackup_1.tmp
-a----- 9/30/2025 6:24 PM          0 config.js
-a----- 9/30/2025 6:24 PM          0 config.min.js
-a----- 9/30/2025 6:21 PM          0 contact.html
-a----- 9/30/2025 6:25 PM          0 dbackup_1.old
-a----- 9/30/2025 6:25 PM          0 dbackup_1.tmp
-a----- 9/30/2025 6:24 PM          0 desktop.css
-a----- 9/30/2025 6:24 PM          0 main.css
-a----- 9/30/2025 6:24 PM          0 mobile.css
-a----- 9/30/2025 6:24 PM          0 print.css
-a----- 9/30/2025 6:24 PM          0 reset.css
-a----- 9/30/2025 6:24 PM          0 script.js
-a----- 9/30/2025 6:24 PM          0 script.min.js
-a----- 9/30/2025 6:24 PM          0 tablet.css
-a----- 9/30/2025 6:24 PM          0 theme_dark.css
-a----- 9/30/2025 6:24 PM          0 theme_light.css

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> # Fil
es like example.js, file.html, etc.
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Get-C
hilditem *. [a-z][a-z]

Directory:
C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project

Mode                LastWriteTime         Length Name
----                -
-a----- 9/30/2025 6:24 PM          0 config.js
-a----- 9/30/2025 6:24 PM          0 config.min.js
-a----- 9/30/2025 6:24 PM          0 script.js
-a----- 9/30/2025 6:24 PM          0 script.min.js
-a----- 9/30/2025 6:24 PM          0 util.js
-a----- 9/30/2025 6:24 PM          0 util.min.js
```

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.

```
d----- 9/30/2025 6:35 PM 21
d----- 9/30/2025 6:35 PM 22
d----- 9/30/2025 6:35 PM 23
d----- 9/30/2025 6:35 PM 24
d----- 9/30/2025 6:35 PM 25
d----- 9/30/2025 6:35 PM 26
d----- 9/30/2025 6:35 PM 27
d----- 9/30/2025 6:35 PM 28
d----- 9/30/2025 6:35 PM 29
d----- 9/30/2025 6:21 PM 3
d----- 9/30/2025 6:35 PM 30
d----- 9/30/2025 6:35 PM 31
d----- 9/30/2025 6:21 PM 4
d----- 9/30/2025 6:21 PM 5
d----- 9/30/2025 6:21 PM 6
d----- 9/30/2025 6:21 PM 7
d----- 9/30/2025 6:21 PM 8
d----- 9/30/2025 6:21 PM 9
d----- 9/30/2025 6:28 PM archive
d----- 9/30/2025 6:29 PM desktop
-a----- 9/30/2025 6:24 PM 0 abackup_1.bak
-a----- 9/30/2025 6:24 PM 0 abackup_1.log
-a----- 9/30/2025 6:24 PM 0 abackup_1.old
-a----- 9/30/2025 6:24 PM 0 abackup_1.tmp
-a----- 9/30/2025 6:24 PM 0 abackup_1.txt
-a----- 9/30/2025 6:24 PM 0 abackup_2.bak
-a----- 9/30/2025 6:24 PM 0 abackup_2.log
-a----- 9/30/2025 6:24 PM 0 abackup_2.old
-a----- 9/30/2025 6:24 PM 0 abackup_2.tmp
-a----- 9/30/2025 6:24 PM 0 abackup_2.txt
-a----- 9/30/2025 6:24 PM 0 abackup_3.bak
-a----- 9/30/2025 6:24 PM 0 abackup_3.log
-a----- 9/30/2025 6:24 PM 0 abackup_3.old
-a----- 9/30/2025 6:24 PM 0 abackup_3.tmp
-a----- 9/30/2025 6:24 PM 0 abackup_3.txt
-a----- 9/30/2025 6:24 PM 0 abackup_4.bak
-a----- 9/30/2025 6:24 PM 0 abackup_4.log
-a----- 9/30/2025 6:24 PM 0 abackup_4.old
-a----- 9/30/2025 6:24 PM 0 abackup_4.tmp
-a----- 9/30/2025 6:24 PM 0 abackup_4.txt
```

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.

```
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> # File 1 - Just normal text
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "serve=localhost" | Out-File file1.txt
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "port=8080" | Out-File file1.txt -Append
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "debug=true" | Out-File file1.txt -Append
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> # File 2 - Same content, different method (still creates Windows line endings)
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "serve=localhost" | Out-File file2.txt -Append
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "port=8080" | Out-File file2.txt -Append
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "debug=true" | Out-File file2.txt -Append
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Write-Host "=== File sizes ==="
=== File sizes ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Write-Host "File1: $(Get-Item file1.txt).Length ) bytes"
File1: 80 bytes
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Write-Host "File2: $(Get-Item file2.txt).Length ) bytes"
File2: 80 bytes
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Write-Host "=== Compare content ==="
=== Compare content ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Compare-Object (Get-Content file1.txt) (Get-Content file2.txt)
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Write-Host "=== Files look the same but sizes are different! ==="
=== Files look the same but sizes are different! ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> "QUESTIONS"
```

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.

```
Directory:
C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project

Mode                LastWriteTime         Length Name
----                -
-a-----          9/30/2025   6:42 PM             0 config_api_dev.conf
-a-----          9/30/2025   6:42 PM             0 config_api_prod.conf
-a-----          9/30/2025   6:42 PM             0 config_api_staging.conf
-a-----          9/30/2025   6:42 PM             0 config_db_dev.conf
-a-----          9/30/2025   6:42 PM             0 config_db_prod.conf
-a-----          9/30/2025   6:42 PM             0 config_db_staging.conf
-a-----          9/30/2025   6:42 PM             0 config_web_dev.conf
-a-----          9/30/2025   6:42 PM             0 config_web_prod.conf
-a-----          9/30/2025   6:42 PM             0 config_web_staging.conf
-a-----          9/30/2025   7:00 PM            28 my_config.conf

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project>
```

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.

```
=== 5. Show first 10 lines ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Get-Content app.log | Select-Object -First 10
INFO: User 1 logged in successfully
DEBUG: Processing request 1
ERROR: Failed to connect to database on attempt 1
WARNING: High memory usage detected
INFO: User 2 logged in successfully
DEBUG: Processing request 2
ERROR: Failed to connect to database on attempt 2
WARNING: High memory usage detected
INFO: User 3 logged in successfully
DEBUG: Processing request 3
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Write-Host "=== 6. Show last 10 lines ==="
=== 6. Show last 10 lines ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project> Get-Content app.log | Select-Object -Last 10
ERROR: Failed to connect to database on attempt 98
WARNING: High memory usage detected
INFO: User 99 logged in successfully
DEBUG: Processing request 99
ERROR: Failed to connect to database on attempt 99
WARNING: High memory usage detected
INFO: User 100 logged in successfully
DEBUG: Processing request 100
ERROR: Failed to connect to database on attempt 100
WARNING: High memory usage detected
```

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.

```
Mode                LastWriteTime         Length Name
----                -
-a-----          9/30/2025   7:17 PM             28 app.conf
-a-----          9/30/2025   7:17 PM            28 app.conf.backup
-a-----          9/30/2025   7:17 PM             26 backup.bak
-a-----          9/30/2025   7:17 PM             18 readme.txt
-a-----          9/30/2025   7:17 PM             34 settings.conf
-a-----          9/30/2025   7:17 PM            34 settings.conf.backup
-a-----          9/30/2025   7:17 PM             34 temp.tmp

PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10> Write-Host "=== 5. Remove .tmp and .bak files (simulate cleanup) ==="
=== 5. Remove .tmp and .bak files (simulate cleanup) ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10> Get-ChildItem *.tmp, *.bak | Remove-Item -WhatIf
What if: Performing the operation "Remove File" on target "C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10\temp.tmp".
What if: Performing the operation "Remove File" on target "C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10\backup.bak".
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10> Write-Host "=== Note: -WhatIf shows what WOULD be deleted ==="
=== Note: -WhatIf shows what WOULD be deleted ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10> Write-Host "=== Remove -WhatIf to actually delete ==="
=== Remove -WhatIf to actually delete ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\question10>
```

Question 11: Compression Analysis

Task: Compare compression efficiency.

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

```
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> # Create ZIP file
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> Compress-Archive -Path text_data.txt, binary_data.bin -DestinationPat
h text_files.zip
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> Write-Host "ZIP archive created: text_files.zip"
ZIP archive created: text_files.zip
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> # Note: In Windows, we mainly use ZIP compression
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> # For targzip, tarbzip2, tartxz we would need WSL or Linux
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> Write-Host "=== File Size Comparison ==="
=== File Size Comparison ===
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> $originalSize = (Get-ChildItem text_data.txt, binary_data.bin | Measu
re-Object -Property Length -Sum).Sum
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> $compressedSize = (Get-Item text_files.zip).Length
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11>
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> Write-Host "Original size: $originalSize bytes"
Original size: 110786 bytes
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> Write-Host "Compressed size: $compressedSize bytes"
Compressed size: 703 bytes
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11> Write-Host "Compression ratio: $([math]::Round($originalSize / $compr
essedSize, 2)):1"
Compression ratio: 157.59:1
PS C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
on11>
```

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
h "full_weekly_$(Get-Date -Format 'yyyy-MM')*.zip"
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13>
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> # Monthly Archive
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Write-Host "Creating monthly archive..."
reating monthly archive...
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n11\question13> Compress-Archive -Path production_server\* -DestinationPat
h "monthly_$(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             full_weekly_20250930-193
000.zip
a-----          9/30/2025   7:30 PM             incr_20250930-193000.zip
a-----          9/30/2025   7:30 PM             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.

```

PRINCIPLE OF LEAST PRIVILEGE:

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

WEB SERVER FILES:
- Windows: IIS_IUSR 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:"
Archive analysis commands:
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17> Write-Host "`n 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 "`n Expand-Archive: Extract archives"
Expand-Archive: Extract archives
S C:\Users\sabat\Introduction_to_linux\assignment2_work\web_project\questi
n17> Write-Host "`n [IO.Compression.ZipFile]::OpenRead(): Examine without e
xtracting"
[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**,