README

Assignment2

Name: INEZA Agape

ID: 27464

Email: agape.ineza010@gmail.com

# What I Did

I completed a comprehensive Linux lab covering 17 tasks (plus a bonus) related to:  
- Investigating a compromised system.  
- Navigating and managing directories.  
- Creating large sets of files with automation (wildcards, brace expansion).  
- Handling archives and compression.  
  
  
Each task included:  
- Exact Linux commands (ls, mkdir, tar, find, etc.).  
- Example outputs to simulate real execution.  
- Explanations of why each command was used.  
- Screenshot placeholders to show proof of execution.

# Why I Did It

The purpose of this project was to:  
- Practice realistic Linux system administration tasks.  
- Gain experience with security investigation and forensic analysis.  
- Learn how attackers might hide in the file system and how to detect them.  
- Automate repetitive tasks to become more efficient.

# What I Learned

- File system structure: /etc for configs, /bin for binaries, /var for logs, etc.  
- Efficient file creation: brace expansion ({01..31}) and loops to avoid manual work.  
- Wildcards & patterns: matching by extension, filename length, or starting character.  
- Sudo security: the risks of overly permissive sudo rules.  
- Forensic analysis: identifying suspicious files, symlinks, special bits (sticky, setuid, setgid), and system artifacts.

# Challenges and Recommendations

## Challenges

- Remembering exact tar options (-cf, -tvf, -xf, -uf).  
- Forgetting to use mkdir -p when creating nested directories.  
- Running into errors when including the archive itself inside tar.  
- Handling missing commands (tree, zip) in minimal Linux environments.  
- Dealing with line ending issues between Windows and Linux.

## Recommendations

- Always verify paths with pwd and ls before running destructive commands (rm, mv).  
- Use -p with mkdir to avoid 'No such file or directory' errors.  
- Exclude the archive file itself when using tar with \*.  
- Install basic tools (tree, zip, unzip) for smoother workflow.  
- When investigating, always work on copies of critical files to preserve evidence.  
- Follow the principle of least privilege in user and group assignments.