TryHackMe Advent of Cyber 2025

Day 1 Challenge Report

Linux Command Line Fundamentals

1. Executive Summary

This report documents the completion of Day 1 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on fundamental Linux command-line operations, file system navigation, and basic security investigation techniques. Successfully completed all main objectives and the optional side quest, recovering multiple flags and learning essential penetration testing skills.

2. Challenge Overview

Objective: Navigate through a Linux system, investigate security logs, and retrieve hidden flags using command-line tools.

Environment: Linux-based virtual machine with multiple user accounts and hidden files.

3. Methodology & Findings

3.1 Initial System Reconnaissance

Basic commands were executed to familiarize with the environment and identify the initial flag location.

- Displayed simple output to verify command execution
- Listed directory contents to identify available files
- Examined README.txt file for instructions
- Verified current working directory location

First Flag Discovered: THM{learning-linux-cli}

3.2 Security Log Analysis

Investigated system authentication logs to identify potential security incidents.

```
Command: ls -la
```

This revealed a hidden guide file (.guide.txt) containing the first flag.

```
Command: grep "Failed password" /var/log/auth.log
```

This command filtered authentication logs for failed login attempts, a common indicator of brute-force attacks or unauthorized access attempts.

3.3 File Discovery & Analysis

Used the find command to locate files matching specific patterns across the file system.

```
Command: find /home/socmas -name *egg*
```

Located a suspicious script: eggstrike.sh

```
Command: cat eggstrike.sh
```

Second Flag Discovered: THM{sir-carrotbane-attacks}

3.4 Privilege Escalation

Escalated privileges to root user to access restricted areas and command history.

```
Command: sudo su
Command: whoami
```

Confirmed root access, then examined command history for clues.

```
Command: cd /home/socmas/2025
Command: history
```

Third Flag Discovered: THM{until-we-meet-again}

4. Optional Side Quest

4.1 Initial Discovery & User Enumeration

Found a note in McSkidy's Document directory containing credentials for another user.

```
File: /home/mcskidy/Document/read-me-please.txt
```

Credentials Found: username: eddi_knapp, password: S0mrthing1Sc0ming

4.2 Password Fragment Hunt

After logging in as eddi_knapp, discovered an encrypted GPG file and began searching for password fragments.

Fragment 1: Hidden File Discovery

```
Command: find /home/eddi_knapp -name *egg*
```

Found hidden file: .easter_egg

PASSFRAG3: c0m1nG

Fragment 2: Git Repository Analysis

Discovered hidden git repository containing password fragments in commit history. Both .secret_git and .secret_git.bak contained the same information.

```
Location: /home/eddi_knapp/.secret_git and .secret_git.bak
Command: git log --stat
Command: git show d12875c8b62e089320880b9b7e41d6765818af3d
```

PASSFRAG2: -1s-

Fragment 3: Recursive Search

```
Command: grep -r PASS /home/eddi_knapp
```

This recursive search successfully located PASSFRAG1, though PASSFRAG2 required a different approach (git repository analysis).

PASSFRAG1: 3ast3r

Complete Password: 3ast3r-1s-c0m1nG

4.3 GPG Decryption & Web Challenge

Used the assembled password to decrypt McSkidy's encrypted note.

```
Command: gpg -d /home/eddi_knapp/Documents/mcskidy_note.txt.gpg
```

The decrypted file contained instructions for accessing a web service and creating a wishlist.

```
Steps performed:
```

1. Open wishlist.txt in /home/socmas/2025 and paste content from decrypted file
2. Accessed web interface at {VM_IP}:8080
3. Copied encrypted message from website
4. Saved encrypted message to /tmp/website_output.txt

```
Command: openssl enc -aes-256-cbc -d -pbkdf2 -iter 200000 -salt -base64 -in
/tmp/website_output.txt -out /tmp/decoded_message.txt -pass
pass:'9IJ6X7R4fQ9TQPM9JX2Q9X2Z'
```

Fourth Flag Discovered: THM{w3lcome_2_A0c_2025} -- But Not Necessary

4.4 Final Secret Directory

The decoded message revealed another secret location containing a compressed archive.

```
Location: /home/eddi_knapp/.secret/dir
```

Important Note: Try to use the 4th Flag but it won't work, it's an ambush.

Solution: Decrypt the file and copy the output to a different folder, then extract it.

```
Command: gpg -d [FILENAME] > /tmp/dir.tar.gz
```

```
Command: cd /tmp && tar -xf dir.tar.gz
```

Extracted a directory containing an image file with a hidden message, completing the side quest.

5. Summary of Flags Captured

Challenge	Flag
Initial Recon	**THM{learning-linux-cli}**
File Discovery	**THM{sir-carrotbane-attacks}**
Privilege Escalation	**THM{until-we-meet-again}**
Side Quest - Web Challenge	**THM{w3lcome_2_A0c_2025}**

6. Key Skills & Techniques Learned

6.1 Linux Command Line

- Basic file system navigation (cd, ls, pwd)
- File content examination (cat, less)
- Hidden file detection with ls -la
- Advanced file searching with find command

- Text searching with grep and recursive search

6.2 Security & Cryptography

- Log file analysis for security incidents
- GPG decryption operations
- OpenSSL AES-256-CBC decryption
- Password fragment assembly
- Archive extraction and manipulation

6.3 Investigation Techniques

- Git repository forensics
- Command history analysis
- Hidden file and directory enumeration
- Multi-step challenge solving methodology
- Web application interaction

7. Conclusion

Day 1 of the TryHackMe Advent of Cyber 2025 provided an excellent introduction to Linux command-line fundamentals and basic penetration testing techniques. The challenge successfully demonstrated the importance of systematic enumeration, attention to detail, and persistence in cybersecurity investigations.

The optional side quest added significant complexity, requiring password fragment assembly, cryptographic operations, and git repository analysis. All objectives were completed successfully, with four flags captured and multiple valuable skills acquired.

Challenge Status: **COMPLETED ✓**