VulnHub Lab Report

1. Title Page

Lab Name: OverTheWire – Bandit
Platform: Online via SSH (Termux)
Author: Praful Awasarmol

Date: 15/5/2025
Difficulty Level: Easy

2. Executive Summary

Objective:
To practice basic Linux commands by connecting to an online server via SSH and capturing passwords to progress from Bandit Level 0 to Level 2.

Final Outcome:
- Level 0 Password Captured: Yes
- Level 1 Password Captured: Yes
- Level 2 Password Captured: Yes

Time Taken: Around 20–30 minutes

3. Tools Used

- Termux (Android Terminal App)
- OpenSSH (via Termux)
- Basic Linux commands: ls, cat, cd, ls -a

4. Methodology

4.1 Level 0 to Level 1

Login:
ssh bandit0@bandit.labs.overthewire.org -p 2220
Password: bandit0

Command Used:

ls
cat readme

Output:
The password for Level 1 is displayed on the terminal.

4.2 Level 1 to Level 2

Login:
ssh bandit1@bandit.labs.overthewire.org -p 2220
Password: (from Level 0)

Command Used:
ls -a
cat .hidden

Output:
The password for Level 2 is displayed.

4.3 Level 2 to Level 3

Login:
ssh bandit2@bandit.labs.overthewire.org -p 2220
Password: (from Level 1)

Command Used:
ls
cat spaces\ in\ this\ filename

Output:
The password for Level 3 is displayed.

5. Vulnerabilities Identified

Not applicable — this lab is for learning Linux and command-line basics.

6. Mitigation Strategies

Not applicable — this is an educational simulation.

7. Challenges Faced

- Initial delay while learning how to use ssh on mobile via Termux.
- Escaping spaces in filenames required special syntax using backslashes (\).

8. Learning Outcomes

- Understood how to connect to remote Linux servers using SSH.
- Learned basic Linux file and directory operations.
- Gained confidence in navigating Linux through terminal commands on mobile.