Rungta College of Engineering and Technology

Department of B.Tech CSE (Cybersecurity)

Minor-2 Project Report

Metasploitable 2 & Mutillidae II Lab

Submitted By:

Kumar Sambhava

ERP No: 6605516

3rd Semester (2025–26)

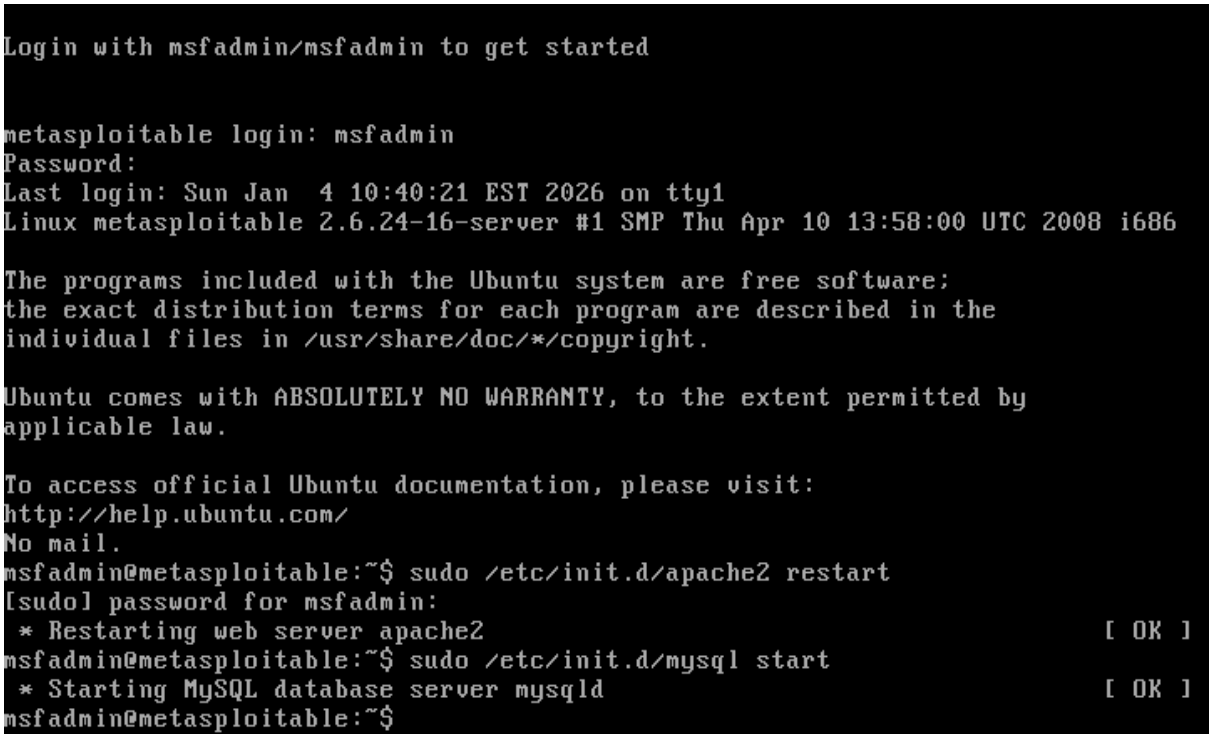
Subject: Minor-2 Project

1.Introduction

This project demonstrates the setup and configuration of an intentionally vulnerable virtual lab using Metasploitable 2 and the Mutillidae II web application. The objective is to understand vulnerable environments, perform basic Linux administrative tasks, and troubleshoot common configuration errors.

2. Environment Setup

Metasploitable 2 is an Ubuntu-based virtual machine designed for security testing and learning. The VM was imported into a virtualization platform and accessed using default credentials (username: msfadmin, password: msfadmin)



3. User Management

A new Linux user account was created using my own name to demonstrate system administration skills. The adduser command was used, followed by verification through the /etc/passwd file.

Commands Used:

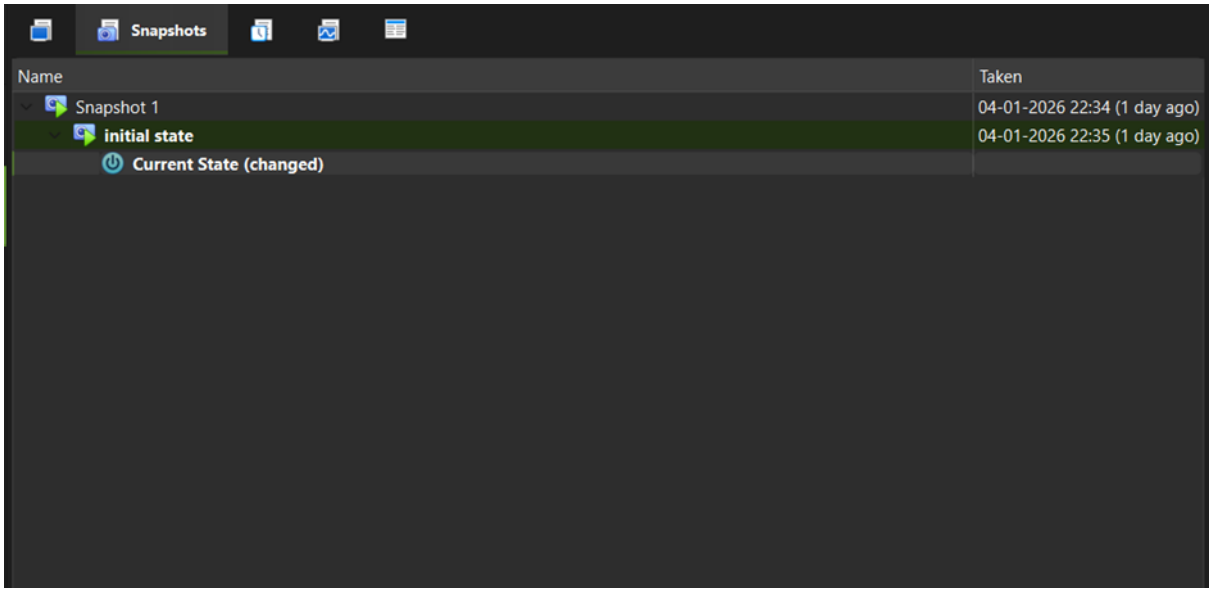
sudo adduser sambhava

cat /etc/passwd | grep sambhava

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo adduser sambhava
[sudo] password for msfadmin:
Adding user `sambhava' ...
Adding new group `sambhava' (1003) ...
Adding new user `sambhava' (1003) with group `sambhava' ...
Creating home directory `/home/sambhava' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for sambhava
Enter the new value, or press ENTER for the default
        Full Name []: Sambhava
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [y/N] y
msfadmin@metasploitable:~$ cat /etc/passwd | grep sambhava
sambhava:x:1003:1003:Sambhava,,,:/home/sambhava:/bin/bash
msfadmin@metasploitable:~$ _
```

4. Virtual Machine Snapshot

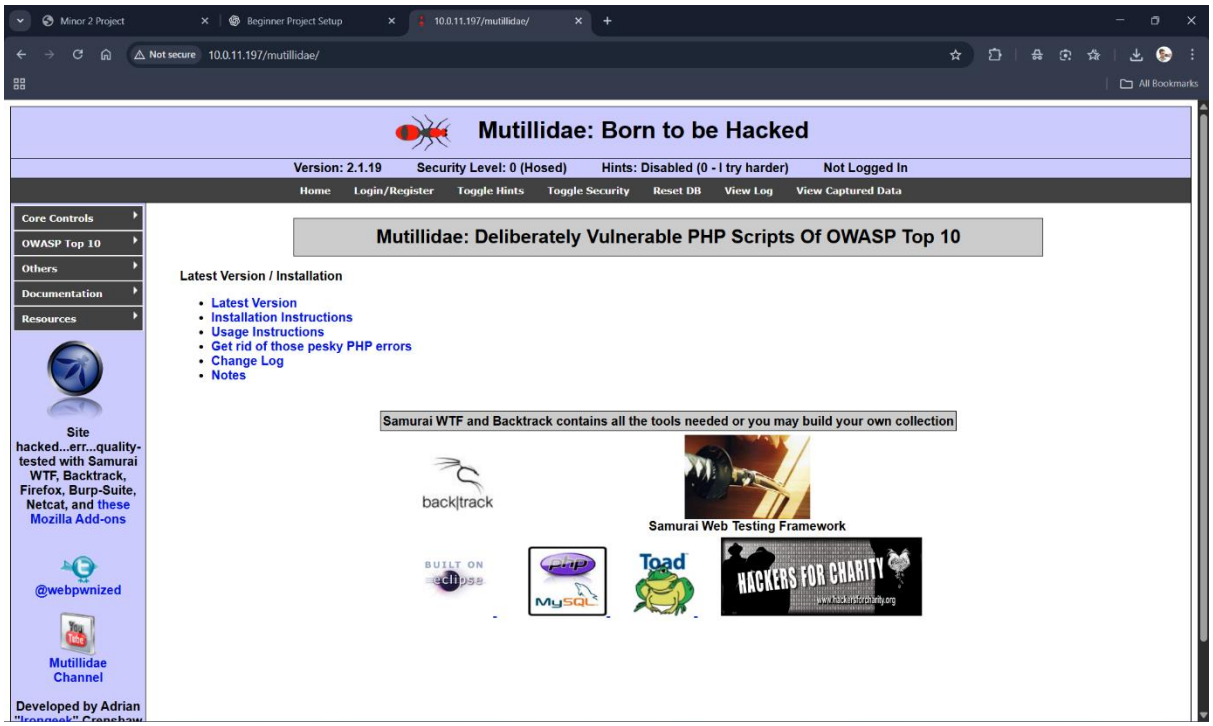
A snapshot was taken after user creation to preserve a safe system state. Snapshots allow easy rollback during testing and troubleshooting.



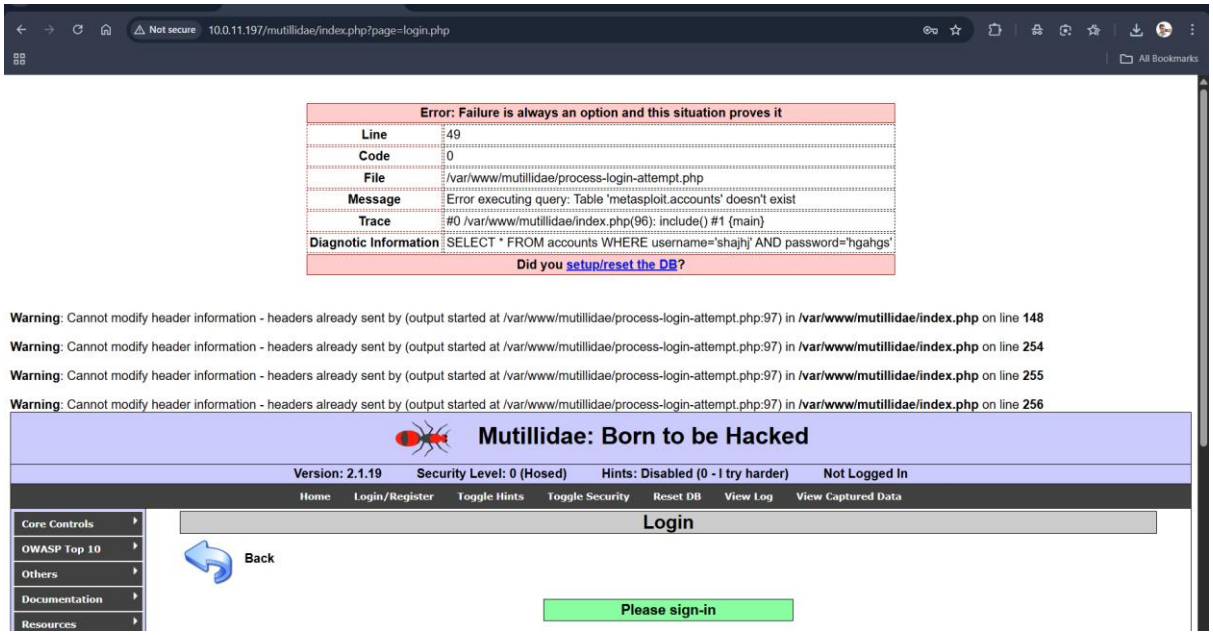
5. Mutillidae II Database Fix

Initially, Mutillidae II displayed database-related errors due to missing tables. The issue was resolved by using the Setup/Reset Database option within the application, which initialized the MySQL database successfully.

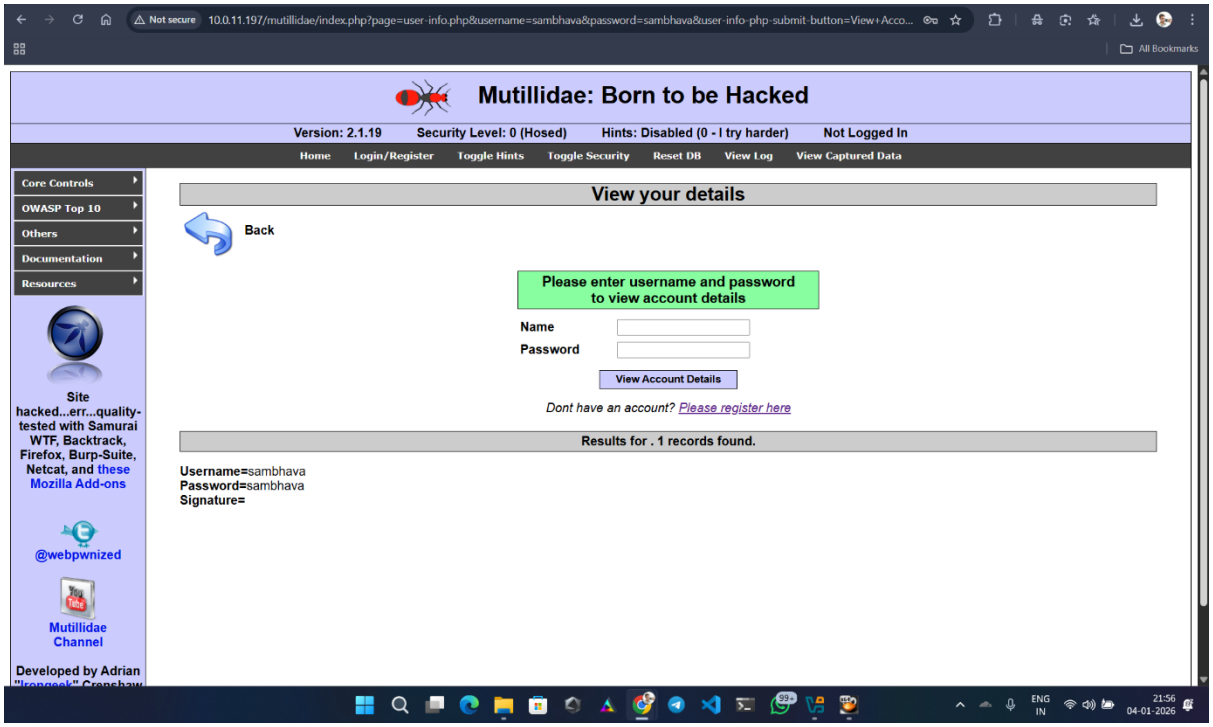
-Mutillidae II working.



-Mutillidae II database error.



-Mutillidae II database fixed.



6.Conclusion

This project successfully demonstrated the setup of a vulnerable lab using Metasploitable2 and the troubleshooting of a real-world configuration issue in Mutillidae II. It enhanced practical understanding of Linux administration, virtualization safety, and web application deployment issues, which are essential skills in cybersecurity.

Appendix: Linux Commands Used

- ifconfig
- sudo adduser sambhava
- cat /etc/passwd | grep sambhava
- service mysql start
- Accessing http://[IP]/mutillidae/