Minor–2 Project Report

Project Title: Vulnerable Web Application Lab using Metasploitable and Mutillidae II

Student Name: Govind Sahu

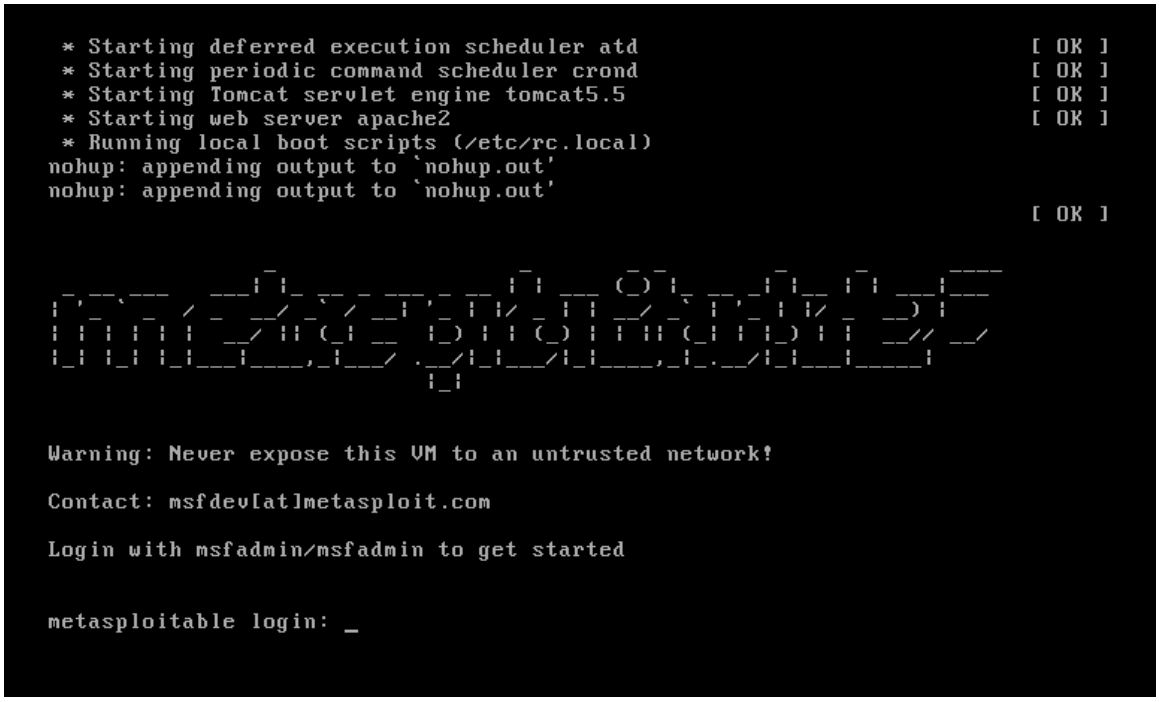
Platform Used: VMware Workstation Pro

1. Introduction

This project is designed to create a controlled vulnerable lab environment for understanding basic web application security concepts. Metasploitable is used as a vulnerable operating system and Mutillidae II is used as a deliberately insecure web application.

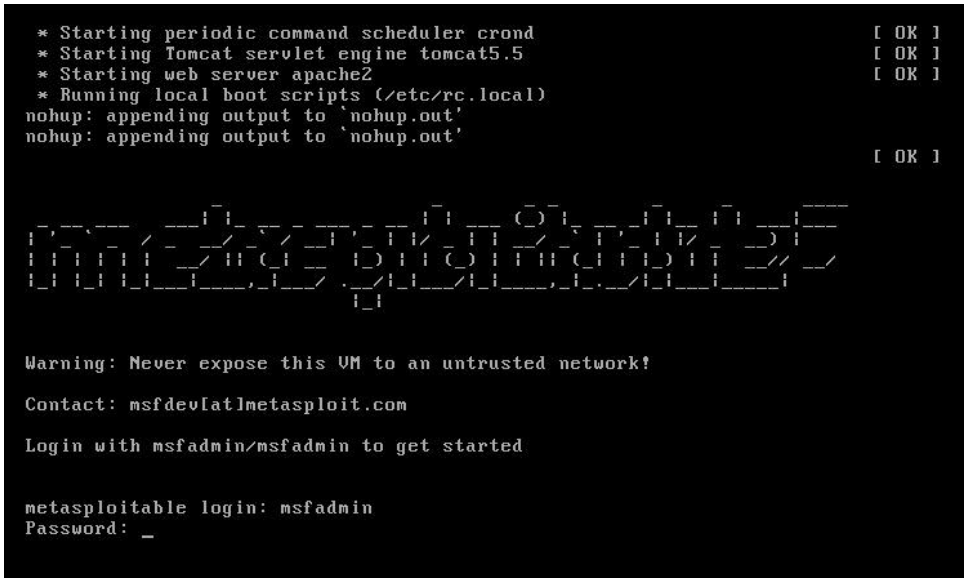
2. Metasploitable Boot and Services

The Metasploitable virtual machine was started successfully. During booting, multiple services such as Apache, Tomcat, and MySQL were initialized. This confirms that the system is fully operational.



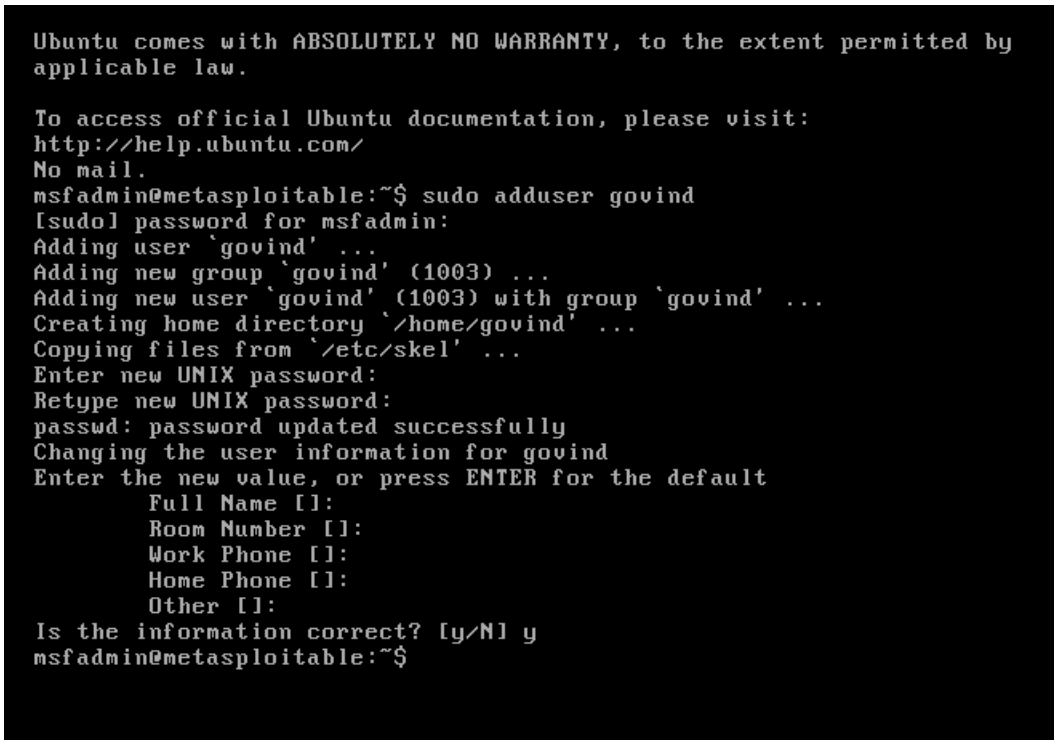
3. System Login

The system was accessed using default credentials (msfadmin / msfadmin). Successful login confirmed terminal access and readiness for further configuration.



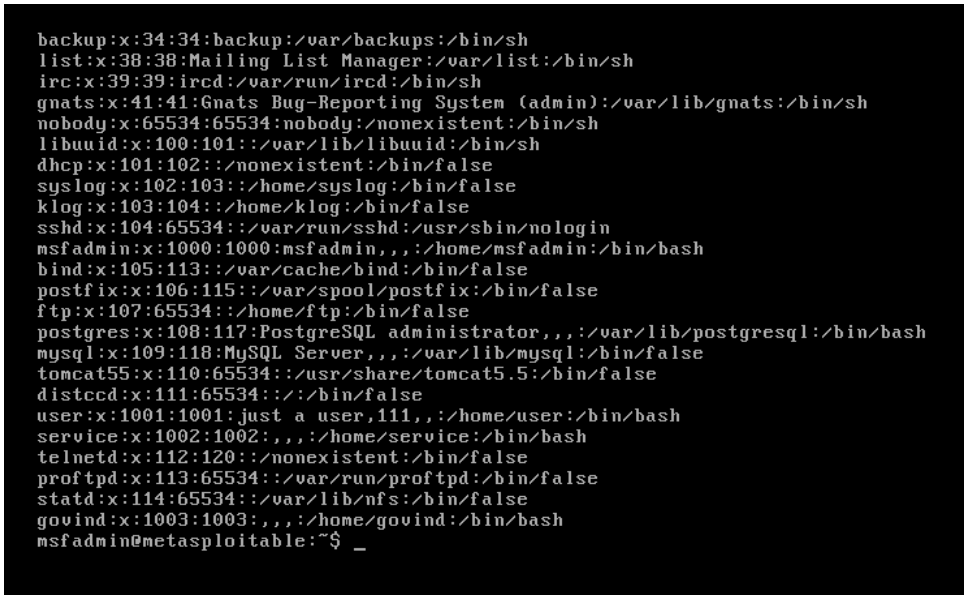
4. New User Creation

To meet project requirements, a new user named 'govind' was created using Linux user management commands. This demonstrates basic system administration skills.



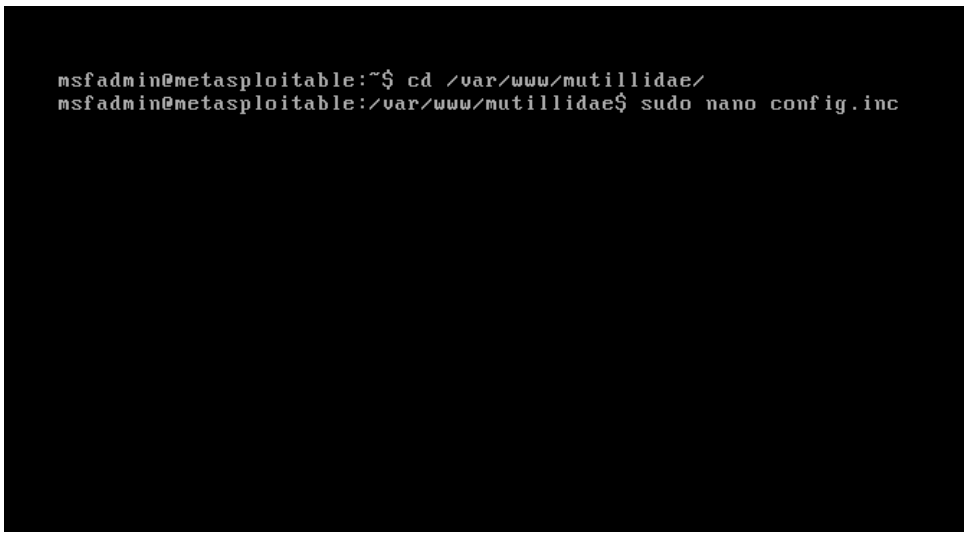
5. User Verification

The newly created user account was verified by checking the system password file. This ensures that the user was successfully added to the operating system.



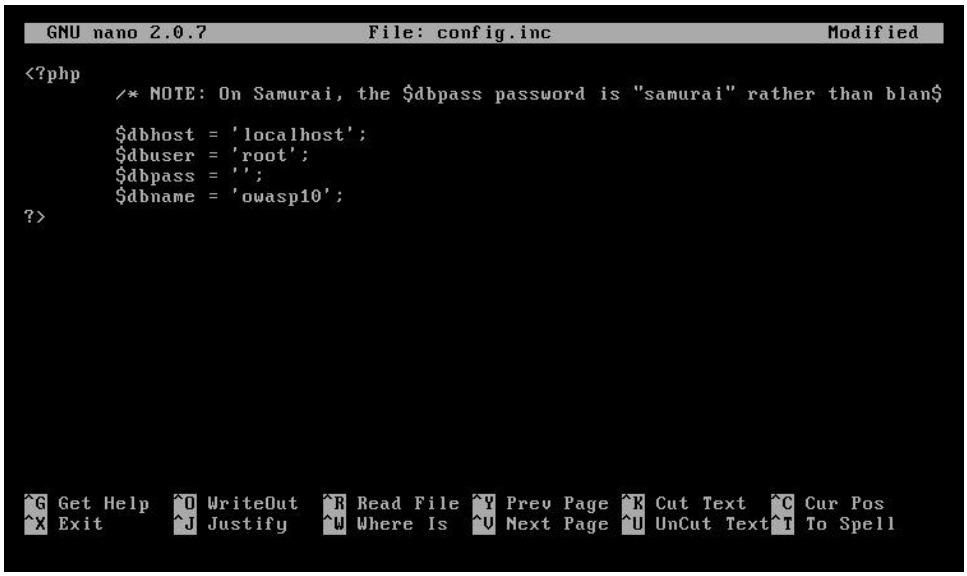
6. Mutillidae II Configuration Fix

Initially, Mutillidae II failed to load due to database configuration issues. The configuration file was edited to correct database credentials and database name.



This screenshot shows the modification of the config.inc file of Mutillidae II. The database name was changed from **metasploit** to **owasp10** to fix the database

connection error. After updating the correct database name, the application connected successfully to the database and loaded properly in the browser.



7. Successful Execution

After correcting the configuration, Mutillidae II loaded successfully in the browser without errors. This project provided hands-on experience with vulnerable systems, Linux commands, and web security labs.

8. Conclusion

This project successfully demonstrated the setup and configuration of the Metasploitable virtual machine for security testing purposes. System-level tasks such as user creation and verification were performed correctly. The Mutillidae II web application was configured by fixing the database connection issue, which allowed it to run without errors. Overall, the project provided practical knowledge of Linux administration, virtual machine usage, and basic web application security concepts in a controlled lab environment.