Internship Final Report

**Student Name:** Bongoni Devendar Goud

**University:** SR University

**Major:** Computer Science

**Internship Duration:** Novembert 1st, 2024 - November 31st, 2024

**Company:** ShadowFox **Domain:** Cyber Security **Mentor:** Mr. Surendharan **Assistant Mentor:** Mr. Pranshu **Coordinator:** Mr. Aakash

# Objectives

My primary objectives for this internship were to:

1. Understand the foundational principles and techniques of penetration testing.
2. Perform hands-on exercises in identifying and exploiting vulnerabilities in a controlled environment.
3. Enhance skills in using tools and methodologies specific to penetration testing.

# Tasks and Responsibilities

During my internship, I was involved in the following key tasks:

1. **Information Gathering**:
   * Conducted enumeration of target systems to identify open ports and services using tools like **Nmap**.
   * Performed OS detection and service version enumeration.
2. **Vulnerability Assessment**:
   * Scanned the target for known vulnerabilities and verified potential exploits using **Nikto** and **Metasploit Framework**.
3. **Exploitation**:
   * Exploited identified vulnerabilities to gain unauthorized access to the target system.
   * Used a reverse shell to establish and maintain access.
4. **Privilege Escalation**:
   * Enumerated the compromised system to identify weaknesses.
   * Successfully escalated privileges to gain root/admin access using enumeration tools like **LinPEAS**.
5. **Post-Exploitation**:
   * Extracted sensitive information such as credentials, system logs, and configuration files from the compromised machine.
   * Documented steps to ensure reproducibility and evidence.

# Learning Outcomes

* **Technical Proficiency**:  
  Gained practical experience in penetration testing tools such as Nmap, Nikto, Metasploit, and LinPEAS.
* **Systematic Approach to Exploitation**:  
  Learned the structured methodology of penetration testing, from reconnaissance to post-exploitation.
* **Problem-Solving Skills**:  
  Improved ability to analyze and adapt to unexpected obstacles, such as failed exploits and misconfigurations.
* **Documentation**:  
  Enhanced proficiency in documenting findings, which is critical for professional penetration testing.

# Challenges and Solutions

 Initial unfamiliarity with specific tools and their configurations.  
 **Solution**: Reviewed official documentation, tutorials, and worked through TryHackMe labs to gain hands-on experience.

 Identifying the correct exploit for a given vulnerability.  
 **Solution**: Utilized vulnerability databases and cross-referenced CVEs to ensure appropriate exploit selection.

.

# Conclusion

This task provided a comprehensive introduction to penetration testing, allowing me to apply theoretical knowledge in a practical, hands-on environment. The structured approach to identifying and exploiting vulnerabilities has deepened my understanding of the cybersecurity domain. This experience motivates me to further explore advanced topics in penetration testing and security auditing.

# Acknowledgments

I express my gratitude to **Shadowfox** for providing an excellent platform for hands-on learning in cybersecurity. Additionally, I appreciate the resources and guidance that helped me successfully complete this task.

This report reflects my learning journey and the skills acquired during the task, emphasizing the importance of structured and practical cybersecurity training.

.