Offensive Security Intro - TryHackMe Lab Report

Name: Ashish Sawant

Email: aaashi0301@gmail.com

GitHub: https://github.com/aaashi03

TryHackMe Profile: https://tryhackme.com/p/ashish0301

Date: April 15, 2025

# 🧠 Lab Overview

The 'Offensive Security Intro' room on TryHackMe introduces the core concepts and mindset of offensive cybersecurity. It gives an overview of ethical hacking, penetration testing methodologies, and how attackers exploit system vulnerabilities.

# 🎯 Objective

To understand the offensive security approach, including reconnaissance, vulnerability identification, exploitation, and reporting. This knowledge is essential to strengthen defenses from a defender’s perspective.

# 📚 Key Topics Covered

- Introduction to the offensive security mindset

- Key stages of penetration testing

- Types of hackers: White, Black, and Grey hats

- Legal and ethical considerations of ethical hacking

- Overview of commonly used offensive tools (e.g., Nmap, Metasploit)

- Introduction to vulnerability scanning and basic exploitation

# 🔐 Relevance to SOC Analyst Role

- Helps understand attacker tactics, techniques, and procedures (TTPs)

- Aids in identifying true positive alerts by recognizing real attack patterns

- Improves defensive response by knowing offensive methodologies

# 🛠️ Hands-On Tasks Completed

- Explored phases of penetration testing including Recon, Scan, Exploit, Report

- Reviewed tools like Nmap for network discovery

- Understood how exploits work and how vulnerabilities are identified

# ✅ Conclusion

This lab built my foundational knowledge of offensive security techniques and how attackers think. It supports my development as a SOC Analyst by enhancing my ability to detect and respond to cyber threats based on offensive tactics.