Hacking Methodology: Course Outline

Course Description

This course provides an overview of common hacking methodologies used in ethical hacking and penetration testing. Students will learn the systematic approach hackers use to identify and exploit vulnerabilities in computer systems and networks.

Learning Objectives

By the end of this course, students will be able to:

1. Understand the phases of a typical hacking methodology
2. Identify common tools and techniques used in each phase
3. Recognize the importance of ethical considerations in hacking

Course Outline

Week 1: Introduction to Hacking Methodology

- Ethical hacking vs. malicious hacking
- Overview of the hacking process
- Legal and ethical considerations

Week 2-3: Reconnaissance and Information Gathering

- Passive vs. active reconnaissance
- OSINT techniques
- Network scanning and enumeration

Week 4-5: Vulnerability Assessment

- Identifying system and network vulnerabilities
- Common vulnerability types
- Vulnerability scanning tools

Week 6-7: Exploitation

- Exploitation techniques
- Password cracking
- Social engineering

Week 8-9: Post-Exploitation

- Privilege escalation
- Maintaining access
- Covering tracks

Week 10: Reporting and Remediation

- Documenting findings
- Risk assessment
- Recommending security improvements

Assessment

- Weekly lab exercises (40%)
- Midterm project: Vulnerability assessment report (25%)
- Final project: Simulated penetration test and presentation (35%)

Required Tools

- Kali Linux or similar penetration testing distribution
- Virtual machines for practice environments

Ethical Guidelines

Students must adhere to strict ethical guidelines throughout the course. All hacking activities will be performed only on authorized systems and networks provided for educational purposes.