CONTENTS

CHAPTER 1: Introduction to Ethical Hacking **01-30**
1.1 Cybersecurity Fundamentals
1.2 Types of Hackers
1.3 Ethical Hacking Phases
1.4 Legal and Ethical Considerations
1.5 Security Standards and Frameworks

CHAPTER 2: Footprinting and Reconnaissance **31-57**
2.1. Information Gathering Techniques
2.2. Open-Source Intelligence (OSINT)
2.3. Domain and DNS Enumeration
2.4. Social Media Reconnaissance
2.5. Countermeasures

CHAPTER 3: Scanning Networks **58-80**
3.1. Network Scanning Concepts
3.2. Port Scanning Techniques
3.3. Service Enumeration
3.4. Vulnerability Identification
3.5. Scanning Tools

CHAPTER 4: System Hacking **81-101**
4.1 Password Attacks
4.2 Privilege Escalation
4.3 Maintaining Access
4. 4Covering Tracks
4.5 System Hardening

CHAPTER 5: Malware Threats **102-134**
5.1 Types of Malware
5.2 Trojans and Backdoors
5.3 Ransomware Analysis
5.4 Malware Detection Techniques
5.5 Malware Prevention

CHAPTER 6: Sniffing and Session Hijacking **135-158**
6.1. Packet Capture Fundamentals
6.2. Network Sniffing Tools
6.3. Session Hijacking Techniques
6.4. MITM Attacks
6.5. Defense Mechanisms

CHAPTER 7: Web Application Security **159-186**
7.1. Web Application Architecture
7.2. SQL Injection
7.3. Cross-Site Scripting (XSS)
7.4. Authentication Attacks
7.5. Web Security Testing

CHAPTER 8: Wireless Network Security **187-217**
8.1. Wireless Technologies
8.2. Wi-Fi Security Protocols
8.3. Wireless Attacks
8.4. Bluetooth Security
8.5. Wireless Defense Strategies

CHAPTER 9: Cloud and IoT Security **218-244**
9.1. Cloud Computing Risks
9.2. Cloud Security Assessment
9.3. IoT Vulnerabilities
9.4. IoT Attack Vectors
9.5. Security Best Practices

CHAPTER 10: Penetration Testing and Reporting **245-273**
10.1. Penetration Testing Methodology
10.2. Exploitation Frameworks
10.3. Post-Exploitation Activities
10.4. Report Writing
10.5. Professional Ethics and Career Development