Week 1: Introduction to Penetration Testing

- Overview of penetration testing
- Understanding the different types of penetration testing
- The penetration testing process
- Types of penetration testing tools

Week 2: Reconnaissance and Information Gathering

- Gathering information about the target
- Open source intelligence (OSINT) techniques
- Network scanning and port scanning
- Passive and active information gathering

Week 3: Vulnerability Assessment

- Identifying vulnerabilities in the target system
- Types of vulnerabilities: software, configuration, and human
- Using vulnerability scanners and other tools
- Analyzing and prioritizing vulnerabilities

Week 4: Exploitation and Privilege Escalation

- Exploiting vulnerabilities to gain access to the target system
- Understanding privilege escalation techniques
- Buffer overflow attacks
- Password cracking techniques

Week 5: Network Penetration Testing

- Testing network infrastructure security

- Understanding network architecture and protocols
- Conducting a penetration test of a network
- Techniques for gaining access to network devices

Week 6: Web Application Penetration Testing

- Testing web application security
- Understanding web application architecture and technologies
- Conducting a penetration test of a web application
- Techniques for exploiting web application vulnerabilities

Week 7: Social Engineering and Physical Penetration Testing

- Understanding social engineering techniques
- Conducting a social engineering penetration test
- Physical security assessment techniques
- Conducting a physical penetration test

Week 8: Wireless Penetration Testing

- Understanding wireless network security
- Conducting a wireless penetration test
- Exploiting wireless vulnerabilities
- Techniques for cracking Wi-Fi passwords

Week 9: Post-Exploitation Techniques

- Maintaining access to the target system
- Understanding privilege escalation techniques
- Covering tracks and maintaining stealth
- Using rootkits and backdoors

Week 10: Report Writing and Documentation

- Writing a penetration testing report
- Understanding the different types of reports
- Documenting findings and recommendations
- Communicating findings to stakeholders

Week 11: Ethical and Legal Considerations

- Understanding ethical and legal considerations in penetration testing
- Ethical hacking and the Code of Ethics
- Legal issues and the law
- Liability and risk management

Week 12: Advanced Penetration Testing Techniques

- Advanced penetration testing techniques and tools
- Understanding advanced attacks and exploits
- Conducting a comprehensive penetration test
- Staying up to date with new threats and vulnerabilities

Week 13: Cryptography and Steganography

- Understanding cryptography and steganography
- Types of cryptographic algorithms and their uses
- Detecting and hiding information in images and audio files
- Using steganography to hide data

Week 14: Cloud Security Testing

- Understanding cloud security
- Cloud service models and deployment models
- Cloud security testing techniques
- Penetration testing of cloud infrastructure and applications

Week 15: Mobile Security Testing

- Understanding mobile security
- Mobile operating systems and architectures
- Mobile application security testing techniques
- Penetration testing of mobile devices and applications

Week 16: IoT Security Testing

- Understanding IoT security

- IoT architecture and technologies
- IoT security testing techniques
- Penetration testing of IoT devices and systems

Week 17: Red Team vs. Blue Team Exercises

- Understanding red team vs. blue team exercises
- Types of exercises and their objectives
- Conducting red team exercises
- Conducting blue team exercises

Week 18: Network Traffic Analysis and Forensics

- Understanding network traffic analysis and forensics
- Tools and techniques for analyzing network traffic

Week 19: Application Security Testing

- Understanding the importance of application security
- Types of application security testing
- Manual and automated application security testing
- Common application security vulnerabilities and how to test for them

Week 20: Cloud Native Security Testing

- Understanding cloud-native security
- Security risks and considerations for cloud-native environments
- Penetration testing techniques specific to cloud-native applications and infrastructure
- Mitigating cloud-native security risks and vulnerabilities