Certified Ethical Hacker
Course Book outline

Chapter 1: Introduction to Ethical Hacking, Ethics and Legality

Chapter 2: Footprinting and Social Engineering

Chapter 3: Scanning and Enumeration

Chapter 4: System Hacking, Password Cracking, Escalating Privileges, and Hiding Files

Chapter 5: Trojans, backdoors, viruses, and worms

Chapter 6: Sniffers

Chapter 7: Denial of Service and Session Hijacking

Chapter 8: Hacking Web Servers, Web Application Vulnerabilities, and Web-based password cracking techniques.

Chapter 9: SQL Injection and Buffer Overflows

Chapter 10: Wireless Hacking

Chapter 11: Physical Security

Chapter 12: Linux Hacking

Chapter 13: Evading IDSs, Honeypots and Firewalls

Chapter 14: Cryptography

Chapter 15: Penetration Testing Methodologies

Course review include question-and-answer session, review of Assessment Test questions, and/or other review practices.