

Week	Date	Topics
Week 1	13-Jan	Introduction: Security Overview, Defense Planning, Using the simulator
Week 2	20-Jan	Threats, Attacks, and Vulnerabilities: Understanding Attacks, Malware, Social Engineering, Vulnerability Concerns
Week 3	27-Jan	Physical Threats: Device and Network Protection, Environmental Controls
Week 4	3-Feb	Networks and Hosts Design and Diagnosis: Manageable Network Plan, Windows System Hardening, File Server Security, Linux Host Security
Week 5	10-Feb	Devices and Infrastructure: Security Appliances, DMZs, Firewalls, NAT, VPNs, Web Threat Protection, Network Access Control, Threats
Week 6	17-Feb	Identity, Access, and Account Management: Access Control Models, Authentication, Authorization, Windows and Linux User Management
Week 7	24-Feb	Cryptography and PKI: Cryptography Implementations, Hashing, File Encryption, PKI
Week 8	3-Mar	Wireless Threats: Wireless Overview, Attacks, Defenses
Week 9	10-Mar	Virtualization, Cloud Security, and Securing Mobile Devices: Virtual Networking, Cloud Services, Mobile Device Management
Week 10	17-Mar	Securing Data and Applications: Data Transmission Security, DLP, Web App Attacks, Application Security
Week 11	24-Mar	Security Assessments: Penetration Testing, Intrusion Detection, Security Assessment Techniques
Week 12	31-Mar	Incident Response, Forensics, and Recovery: Incident Response, Digital Forensics, Backup and Restore
Week 13	7-Apr	Risk Management: Organizational Security Policies, Risk Management, Email
Week 14	14-Apr	Governance and Compliance: Audits, Controls, Privacy
Week 15	21-Apr	Practice Exams
Week 16	28-Apr	Practice Exams
Week 17	5-May	
Week 18	12-May	Take CompTIA Exam