CompTIA Security+ Class Outline

Chapter 1: Security Fundamentals

- Module A: Security concepts
- Module B: Risk management
- Module C: Vulnerability assessment

Chapter 2: Understanding attacks

- Module A: Understanding attackers
- Module B: Social engineering
- Module C: Malware
- Module D: Network attacks
- Module E: Application attacks

Chapter 3: Cryptography

- Module A: Cryptography concepts
- Module B: Public key infrastructure

Chapter 4: Network fundamentals

- Module A: Network components
- Module B: Network addressing
- Module C: Network ports and applications

Chapter 5: Securing networks

- Module A: Network security components
- Module B: Transport encryption
- Module C: Hardening networks
- Module D: Monitoring and detection

Chapter 6: Securing hosts and data

- Module A: Securing hosts
- Module B: Securing data
- Module C: Mobile device security

Chapter 7: Securing network services

- Module A: Securing applications
- Module B: Virtual and cloud systems

Chapter 8: Authentication

- Module A: Authentication factors
- Module B: Authentication protocols

Chapter 9: Access control

- Module A: Access control principles
- Module B: Account management

Chapter 10: Organizational security

- Module A: Security policies
- Module B: User training
- Module C: Physical security and safety

Chapter 11: Disaster planning and recovery

- Module A: Business continuity
- Module B: Fault tolerance and recovery
- Module C: Incident response