# *CompTIA Security+ Outline*

Domain 1: Mitigating threats

- 1.1 Core system maintenance
- 1.2 Virus and spyware management
- 1.3 Browser security
- 1.4 Social engineering threats

Domain 2: Cryptography

- 2.1 Symmetric cryptography
- 2.2 Public key cryptography

Domain 3: Authentication systems

- 3.1 Authentication
- 3.2 Hashing
- 3.3 Authentication systems

Domain 4: Messaging security

- 4.1 E-mail security
- 4.2 Messaging and peer-to-peer security

Domain 5: User and role based security

- 5.1 Security policies
- 5.2 Securing file and print resources

Domain 6: Public key infrastructure

- 6.1 Key management and life cycle
- 6.2 Setting up a certificate server
- 6.3 Web server security with PKI

Domain 7: Access security

- 7.1 Biometric systems
- 7.2 Physical access security
- 7.3 Peripheral and component security
- 7.4 Storage device security

Domain 8: Ports and protocols

8.1 TCP/IP review
8.2 Protocol-based attacks

Domain 9: Network security

9.1 Common network devices
9.2 Secure network topologies
9.3 Browser-related network security
9.4 Virtualization

Domain 10: Wireless security

10.1 Wi-Fi network security
10.2 Non-PC wireless devices

Domain 11: Remote access security

11.1 Remote access
11.2 Virtual private networks

Domain 12: Auditing, logging, and monitoring

12.1 System logging
12.2 Server monitoring

Domain 13: Vulnerability testing

13.1 Risk and vulnerability assessment
13.2 IDS and IPS
13.3 Forensics

Domain 14: Organizational security

14.1 Organizational policies
14.2 Education and training
14.3 Disposal and destruction

Domain 15: Business continuity

15.1 Redundancy planning
15.2 Backups
15.3 Environmental controls

Review and Test Prep.