

## Security + Training

The Security + training course is designed to sharpen your knowledge of the foundational security concepts assessed in the CompTIA Security+™ exam. Thru the use of hands-on labs, instructor led demos and lecture you will gain real-world knowledge of how to protect your network from attack while preparing for your certification.

This course includes a Mike Myers Passport Security + book, TSI courseware, sample exam questions, hands-on labs and training led by the finest instructors in the security industry. All of TSI's instructors are also security practitioners, so you know you will be getting industry insights in addition to your exam preparation.

## Course Outline

1. Security Concepts
  - a. Access control models
  - b. Authentication methods
  - c. Attacker tools and methodology
  - d. Malicious code
2. Communication Security
  - a. Remote access administration
  - b. E-mail security
  - c. Internet security administration
  - d. Internet threats
  - e. Securing file transfer protocols
  - f. Wireless Security
3. Infrastructure Security
  - a. Network Security Devices
    - i. Firewalls
    - ii. Routers
    - iii. Switches
    - iv. IDS
  - b. Cabling Security concerns
  - c. Security Topology
  - d. IDS and establishing a security baseline
  - e. Application and network hardening
4. Cryptography
  - a. Goals of cryptography
  - b. Symmetric and asymmetric algorithms
  - c. Hashing for integrity
  - d. PKI and Key Management
5. Organizational Security
  - a. Physical Security
  - b. Business Continuity Planning and Disaster Recovery
  - c. Understanding Security Policy
  - d. Managing User Privileges
  - e. Forensics
  - f. Risk Identification and Management
  - g. Social Engineering