Security +

Description: *This is an introduction in basic computer and network security skills, which includes developing a comprehensive approach to information security that embraces both the human and technical dimensions. Security+ is a hands-on course designed to teach:*

- *Fundamental network defense and countermeasures*
- *Network auditing, vulnerability analyses and intrusion detection*
- *Incident reporting, viruses, user authentication and smart cards*
- *Privilege management, firewalls and remote access*
- *Operating system security and patch installation*
- *Virtual private networks, wireless network and wireless device security*
- *Public key infrastructure, digital certificates, and cryptography*
- *Biometrics, forensics, security policy and security law*

This training provides the student with the training necessary to succeed in the Security+ Certification exam. The Security+ Certification Exam by COMPTIA is an industry exam that is from authorized testing centers.

Session 1: Mitigating threats
- Core system maintenance
- Virus and spyware management
- Browser security
- Social engineering threats

Session 2: Cryptography
- Symmetric cryptography
- Public key cryptography

Session 3: Authentication systems
- Authentication
- Hashing
- Authentication Systems

Session 4: Messaging security
- E-mail security
- Messaging and peer-to-peer security

Session 5: User and role based security
- Security policies
- Securing file and print resources

Session 6: Public key infrastructure
- Key management and life cycle
- Setting up a certificate server
- Web server security with PKI

Session 7: Access security
- Biometric systems
- Physical access security
- Peripheral and component security
- Storage device security

Session 8: Ports and protocols
- TCP/IP review
- Protocol-based attacks

Session 9: Network security
- Common network devices
- Secure network topologies
- Browser-related network security
- Virtualization

Session 10: Wireless security
- Wi-Fi network security
- Non-PC wireless devices

Session 11: Remote access security
- Remote access
- Virtual private networks

Session 12: Auditing, logging, and monitoring
- System logging
- Server monitoring

Session 13: Vulnerability testing

- Risk and vulnerability assessment
- IDS and IPS
- Forensics

Session 14: Organizational security

- Organizational policies
- Education and training
- Disposal and destruction

Session 15: Business continuity

- Redundancy planning
- Backups
- Environmental controls


CORPORATION
LEARNING ALLIANCE