

COMPTIA SECURITY+ CERTIFICATION COURSE



Distance Learning Centre's **Security+ Certification Course** covers the Latest 2008 Security+ Certification syllabus.

The certification validates knowledge of communication security, infrastructure security, cryptography, operational security, and general security concepts. It is an international, vendor-neutral certification that is taught around the world. Although not a prerequisite, it is recommended that students have the CompTIA Network+ certification.

Security threats are increasing in number and severity, and the gap between the need for security professionals and qualified IT personnel is the largest of any IT specialty, according to a 2008 CompTIA study. Even in a troubled economy, most businesses plan to maintain or increase their investment in security.

Major organisations that employ CompTIA Security+ certified staff include Booz Allen Hamilton, Hewlett-Packard, IBM, Motorola, Symantec, Telstra, Hitachi, Ricoh, Lockheed Martin, Unisys, Hilton Hotels Corp., General Mills, the U.S. Navy, Army, Air Force and Marines.

There are more than 10,000 CompTIA Security+ certified professionals worldwide. CompTIA Security+ is an elective or prerequisite to advanced security certifications.

Course Objectives:

After completing this course, you will know how to:

- Mitigate threats to network security through core system maintenance, implement virus and spyware management tools, secure Web browsers, and identify social engineering threats.
- Identify cryptography concepts including algorithms, public keys, security certificates, and single- and dual-sided certificates.
- Implement authentication systems such as one-, two-, and three-factor authentication, prevent password cracking, and use authentication such as Kerberos and CHAP.
- Secure e-mail and messaging services.
- Create security policies to secure file and print resources.
- Install, enable, and configure public key infrastructure.
- Install and configure security systems including biometric systems, physical access controls, as well as access to peripherals, computer components, and storage devices.
- Assess vulnerability to security attacks against TCP/IP ports and protocols.
- Configure intranet and extranet security zones and use virtualization to protect network security, as well as identify common threats against network devices.
- Implement a secure wireless network.
- Create a secure remote access network using RADIUS, TACACS, LDAP, and VPNs.
- Use auditing, logging, and monitoring techniques to maintain a secure network.
- Conduct security risks and vulnerability assessment using IPS, IDS, MBSA, and OVAL tools.
- Establish organizational security through organizational policies, education and training, and the proper disposal and destruction of IT equipment.
- Create a business continuity plan that prepares the organization to deal with security threats and natural disasters.

Price:
£200.00

Instalment Options:

You can spread the payments for this course over 4 monthly payments. 1 initial payment of £80.00, followed by 3 monthly payments of £40.00.

Course Format:

Course Book with Online Practice Exams

Assessment:

CompTIA SY0-201 Security+ Examination

Approximate Study Time:
80 Hours of Self Study

The CompTIA Security+ Certification Course Consists of:

➤ **CompTIA Security+ Certification Course Card**

Access the most important information you need quickly and easily with four-color, tri-fold, six-sided Course Cards! This card can help you pass the test, as well as provide a handy reference for general networking information. A basic overview summarizes access methods, transport protocols, network services, wireless LANs, and security and authentication protocols.

Advanced topics cover network devices, network security, remote access protocols, and WAN technologies. The quick reference section will help you remember types of media, media connectors, and cables, as well as reference models, IP addressing, TCP/IP protocols and ports, networking technologies, and remote access connection technologies.

➤ **CompTIA Security+ SY0-201 Course Book:**

The Security+ Certification course teaches material that maps to all skill and knowledge objectives for the CompTIA Security+ certification exam (SY0-201).

After completing the course book, students will understand the field of network security and how it relates to other areas of information technology. This course also provides the broad-based knowledge necessary to prepare for further study in specialized security fields, or it can serve as a capstone course that gives a general introduction to the field.

The course book covers the following Units:

- **Unit 1: Migrating Threats**

The following topics are covered in this unit: Core system maintenance; Virus and spyware management; Browser security; and Social engineering threats.

- **Unit 2: Cryptography**

The following topics are covered in this unit: Symmetric cryptography; and Public key cryptography.

- **Unit 3: Authentication systems**

The following topics are covered in this unit: Authentication; Hashing; and Authentication systems.

- **Unit 4: Messaging security**

The following topics are covered in this unit: E-mail security; and Messaging and peer-to-peer security.

- **Unit 5: User and role based security**

The following topics are covered in this unit: Security policies; and Securing file and print resources.

- **Unit 6: Public key infrastructure**

The following topics are covered in this unit: Key management and life cycle; Setting up a certificate server; and Web server security with PKI.

- **Unit 7: Access security**

The following topics are covered in this unit: Biometric systems; Physical access security; Peripheral and component security; and Storage device security.

- **Unit 8: Ports and protocols**

The following topics are covered in this unit: TCP/IP review; and Protocol-based attacks.

- **Unit 9: Network security**

The following topics are covered in this unit: Common network devices; Secure network topologies; Browser-related network security; and Virtualization.

- **Unit 10: Wireless security**

The following topics are covered in this unit: Wi-Fi network security; and Non-PC wireless devices.

- **Unit 11: Remote access security**

The following topics are covered in this unit: Remote access; and Virtual private networks.

- **Unit 12 : Auditing, logging, and monitoring**

The following topics are covered in this unit: System logging; and Server monitoring.

- **Unit 13 : Vulnerability testing**

The following topics are covered in this unit: Risk and vulnerability assessment; IDS and IPS; and Forensics.

- **Unit 14: Organizational security**

The following topics are covered in this unit: Organizational policies; Education and training; and Disposal and destruction.

- **Unit 15: Business continuity**

The following topics are covered in this unit: Redundancy planning; Backups; and Environmental controls.

PLEASE NOTE: The Security+ Certification Course is designed as a theory-based course but does contain all relevant information on how to complete practical exercises.

The course books that we use are Official CompTIA Press Course materials.



➤ **CertBlaster Online Exam Preparation Software**

The course comes with DTI Publishing's Online CertBlaster exam preparation software absolutely free.

CertBlaster® is a powerful certification preparation tool that simulates the conditions of the exams students prepare for. **CertBlaster®** offers four practice modes and all the different question types required to simulate all the exams.

CertBlaster covers mock examination questions in multiple choice or multiple answer formats. This software is the perfect addition to help prepare for your exam.

Pre-Requirements:

There are no particular entry requirements for the course but we advise that all students have a good general knowledge of using PCs, the Windows operating system and Windows-based software. It is also advisable that students have completed the CompTIA A+ and Network+ Certification syllabus.

The course is designed for theory purposes but to complete the practical elements of this course, students would require access to multiple PC's as well as networking equipment & toolkit.

Students also would also require Windows Vista Ultimate Edition and Windows Server 2008 Standard Edition software as well as the following hardware items: Network card; Fingerprint scanner; A Trusted Platform Module (TPM) chip or a USB flash drive.

Course Duration & Support:

Students may register at any time. The courses are designed as self-study courses but if you have any problems you can email our email support.

As the course is self study you can complete in as little or as long a time as you prefer, and we do not impose a cut-off date for study.

Assessment:

Assessment is from the Security+ Certification SY0-201 Examination. Examinations are 90 minutes in length each and have 100 questions in multiple choice/multiple answer format. The Exam is graded on a scale of 100 - 900 with a minimum passing score of 720.

Qualification:

On Completion of the Security+ Certification Course, you can apply for your **internationally recognised Security+ SY0-201 Examination**.

Examinations must be sat at a registered Prometric or Pearson VUE testing centre and are currently £191.00 + VAT each.

You can locate testing centres and schedule appointments on their Websites:



Prometric website – <http://www.prometric.com/>

Pearson VUE - <http://pearsonvue.com/>