Unit 120: CompTIA Security+

Unit code: K/501/3599

QCF Level 3: BTEC in IT

Credit value: 9

Guided learning hours: 80

Aim and purpose

The Security+ certification is an internationally recognised validation of the technical knowledge required of foundation-level security practitioners. A Security+ certified individual has successfully proven holding a foundation-level of skill and knowledge in General Security Concepts, Communication Security, Infrastructure Security, Basics of Cryptography and Operational/Organizational Security. Candidates are recommended to have two years experience in a networking role with pre-existing knowledge of TCP/IP, experience in a security related role, Network+ or equivalent certification, and adequate training and self-study materials.

Unit introduction

This unit is a comprehensive introduction to the principles of systems security and enable a learner to explore the range of techniques used in applying security as well as attempting to subvert a system.

The unit explores network infrastructure security, how access control can be both physical and logical in the deployment of a secure systems solution, why regular audits of a systems security would enhance the security offered. Technologies used in cryptographic techniques are explored along with how an organisation would manage their security and overcome any social engineering techniques.

CompTIA link with a range of different partners to offer a range of learning resources, where learners and centres can access these through CompTIAs Academic learning programme. To attain a pass, learners must take the CompTIA Security+ certification exam.

This unit will prepare learners to sit the CompTIA Security+ certification exam, this unit is also assessed with BTEC merit and distinction criteria.

To view general information about CompTIA objectives please visit: www.comptia.org, where the detailed scope and sequence for all certifications are available for anyone to download.

Learning outcomes

On completion of this unit a learner should:

1 Understand general security concepts

2 Recognise and understand communication security

3 Understand and differentiate infrastructure security

4 Understand and apply the basics of cryptography

5 Understand operational & organisational security.

Unit content in relation to the Merit and Distinction Criteria

Security Solution: eg using cryptography, firewall based, user access control, passwords, usernames and levels, proxy control, VPN, network based, workstation based, server based, domain based, access control list

Implementation: on at least two devices on an interconnected network

Testing: eg penetration testing, black hat, white hat, using known vulnerability, range test, stress test, brute force

Assessment and grading criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria for a pass grade describe the level of achievement required to pass this unit.

Assessment and grading criteria		
To achieve a pass grade the evidence must show that the learner is able to:	**To achieve a merit grade the evidence must show that, in addition to the pass criteria, the learner is able to:**	**To achieve a distinction grade the evidence must show that, in addition to the pass and merit criteria, the learner is able to:**
Pass CompTIA Security+ Certification Exam The centre will evidence this with a copy of the learners results, the learner MUST PASS at the minimum set by CompTIA.	**M1** plan a security solution **[IE, CT]**	**D1** justify the security solution [IE, CT, SM]
	M2 implement the security solution [IE, SM]	**D2** critically test the security solution. [SM, IE]
	M3 manage and maintain the security solution. [TW, EP, SM]	

PLTS: This summary references where applicable in the pass criteria, in the square brackets, the elements of the personal, learning and thinking skills. It identifies opportunities for learners to demonstrate effective application of the referenced elements of the skills.

Key	IE – independent enquirers	RL – reflective learners	SM – self-managers
	CT – creative thinkers	TW – team workers	EP – effective participators

Essential guidance for tutors

Delivery

The CompTIA Security+ course and associated certifications are delivered as part of an academic programme available to centres in UK and Eire. Centres may only access this certification's associated discounts from within this programme are advised to seek guidance on what current courses comprise the study/delivery required for learners to access the certification.

More information on the programme, membership and delivery requirements can be found at www.comptia.org.

If learners are taking CompTIA study as part of their BTEC programme, it is recommended that both programmes of study are integrated. Practical and theory tasks for the CompTIA programme can be integrated into the study required for the merit and distinction criteria within this unit.

The outcomes of this unit are synergic with the other CompTIA units as well as those offered by Cisco, Microsoft and VMWare, where there are considerable differences. This unit may be delivered in parallel or in sequence. Units in security, systems support and networking, that are both BTEC specific as well as from other vendors may be taught in conjunction with the CompTIA units to enhance the learners experience.

Outline learning plan

CompTIA as part of the their academy programme, provide learning plans and study guidance for their courses. CompTIA recommend an estimated 75 hours of delivery to attain the pass criteria, in line with QCF credit and notional learning hours. The notional hours for managed learning is set at 40 for learners to attempt the merit and distinction

Assessment

To achieve a pass grade, learners must pass the CompTIA Security+ examination.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the merit and distinction criteria in the assessment and grading grid. This is for guidance and it is recommended that centres either write their own assignments or adapt any Edexcel assignments to meet local needs and resources.

Criteria covered	Assignment title	Scenario	Assessment method
M1, D1	The security solution	Learners are asked to recommend and evaluate a security proposal based on currently available technology, the assessment could be enhanced by encouraging learners to explore the different types of attacks in common use.	Presentation, poster, oral, report, video.
M2, M3, D2	Secure the system	Learners will secure a system ensuring it is operational, secure capable of disaster recovery and providing a network service.	Presentation, poster, oral, report, video, practical observation.

Links to National Occupational Standards, other BTEC units, other BTEC qualifications and other relevant units and qualifications

To be completed, links to 6.1 of the NOS and may be co-presented with all other CompTIA modules

Essential resources

As members of the CompTIA academic programme, centres may choose to access a range of teaching and assessment practice resources. The technological requirement for this unit does not demand any more than the 'average' centre is already providing for a computer systems session, old computers, spare components, replacement parts will enhance the learning experience. If a centre is restricted by the cost of licensing, many Linux distributions exist, that are easy to install in both desktop and server versions and now comparable in support and management terms to other popular operating systems.

To ensure system 'integrity' this unit may be best delivered in a separate sandboxed environment, away from the main campus network.

Employer engagement and vocational contexts

CompTIA certification is internationally recognized by a diverse range of employers (from SME's to large corporations) as one of the principal certifications in systems support and maintenance.

Indicative reading for learners

For access to the CompTIA academic programme resources and more information on joining the programme, please visit www.comptia.org

Delivery of personal, learning and thinking skills

The table below identifies the opportunities for personal, learning and thinking skills (PLTS) that have been included within the pass assessment criteria of this unit.

Skill	When learners are ...
Independent enquirers	The pass criteria is set by an examination, the PLTS of self management and reflective learning is supported by the learner, taking personal study and revision in advance of the Examination.
Creative thinkers	
Reflective learners	
Team workers	
Self-managers	
Effective participators	

Although PLTS are identified within this unit as an inherent part of the assessment criteria, there are further opportunities to develop a range of PLTS through various approaches to teaching and learning.

Skill	When learners are ...
Independent enquirers	investigating current security issues and presenting a proposed solution
Creative thinkers	investigating current security issues and presenting a proposed solution
Reflective learners	investigating current security issues and presenting a proposed solution
Self-managers	implementing and testing the security solution proposed.

Functional Skills – Level 2

Skill	When learners are ...
ICT – Use ICT systems	
Select, interact with and use ICT systems independently for a complex task to meet a variety of needs	Implementing and testing the proposed security solution
Use ICT to effectively plan work and evaluate the effectiveness of the ICT system they have used	Implementing and testing the proposed security solution
Manage information storage to enable efficient retrieval	Implementing and testing the proposed security solution
Follow and understand the need for safety and security practices	Implementing and testing the proposed security solution
Troubleshoot	Implementing and testing the proposed security solution
ICT – Find and select information	
Select and use a variety of sources of information independently for a complex task	Developing the security system proposal
Access, search for, select and use ICT-based information and evaluate its fitness for purpose	Developing the security system proposal
Mathematics	
Understand routine and non-routine problems in a wide range of familiar and unfamiliar contexts and situations	All cryptographic techniques employ a range of complex mathematical techniques
English	
Speaking and listening – make a range of contributions to discussions and make effective presentations in a wide range of contexts	Presenting the justification of the proposal.