Unit 32: Networked Systems Security

Unit code: J/601/7332

QCF Level 3: BTEC National

Credit value: 10

Guided learning hours: 60

Aim and purpose

The aim of this unit is to ensure learners know about the types and sources of network attacks and how to protect against them, and to develop the skills and understanding needed to plan for and protect a networked system.

Unit introduction

In this unit learners will build an understanding of the security issues that relate specifically to networked systems.

The need to ensure that all computer and networked systems are secure is vital to individuals and organisations. There are frequent news reports about IT security issues and virus scares. This unit ensures that learners know where and how security threats arise and how organisations can minimise their risks. They will research organisational policies and procedures to find out how they can help protect systems. Breaches in security may be caused by human actions, either accidentally or by malicious intent, negligence or through incorrect installation, configuration or operation.

Attacks against networked systems are commonplace and increasing and, therefore, the IT practitioner needs to develop specialist skills to be able to combat these threats. This unit enables learners to understand why security is necessary, what specific potential dangers exist and how to protect systems.

The unit introduces the hardware and software the IT technician can utilise to combat threats, looking at both wired and wireless network systems. Personal access controls such as biometrics will be investigated and cryptography techniques tried and compared. Intrusion detection systems such as firewalls and virus checkers will be used.

An important part of the unit is the practical work. Learners will have the opportunity to take a hands-on approach to learning and configure and test networked systems to improve security.

This unit complements the other network and security units in the qualification.

Learning outcomes

On completion of this unit a learner should:

1 Know the types and sources of network attacks

2 Know about security related hardware and software

3 Understand organisational aspects of network security

4 Be able to apply system security.

Unit content

1 Know the types and sources of network attacks

Attacks: types eg denial of service, back door, spoofing, mathematical, brute force, software exploitation, viruses, rootkits, worms, Trojans, spyware, adware

Sources of attacks: internal eg disaffected staff; external eg via internet connections or through unsecured wireless access point, viruses introduced by email

2 Know about security related hardware and software

Email systems: security features eg secure MIME, spam, hoaxing, relay agents

Wireless systems: security features eg site surveys, MAC association, WEP/WPA keys, TKIP

Networked devices: security features eg router, switch, wireless access point

Transmission media: issues eg use of shielding

Personal access control: devices eg biometrics, passwords, usernames, permissions, digital signatures

Security control at device level: access control eg protocols, log in, certificates

Encryption: eg encrypting files for confidentiality, encryption with application-specific tools, recovering encrypted data

Intrusion detection systems: devices eg firewalls, virus protection, spyware protection, file monitoring, folder monitoring, use of honeypots, alarms

3 Understand organisational aspects of network security

Policies and procedures: monitoring; education and training; backup and recovery schemes; configuring and upgrading software; setting up file and folder permissions

User responsibilities: adherence to specific guidelines eg strength of password, installation of new software

Education of IT professionals: maintenance of skills; knowledge of exploits; application of updates and patches

Physical security of system: lock and key; logging of entry; secure room environments; authentication of individual

Risk assessment and reduction: potential risks; penetration testing; security audits

4 Be able to apply system security

Administration: procedures eg implementing password policy, locking down user accounts, securing administrator's permissions, protecting against viruses, restricting access to critical services, installing or updating security software

Algorithms: types eg private/public key encryption, DES, 3DES, RSA, hashing

Transport: methods eg IPSEC, GRE, VPN

Application: eg certificates, trust memberships

Filtering: eg firewalls, access control lists

Test: test for functionality; test for performance eg does security measure slow down system functions

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:**
P1 describe how networks can be attacked		**D1** discuss recent network threats
P2 describe how networked systems can be protected [IE2]	**M1** explain the operation of different intruder detection systems	
P3 explain what an organisation can do to minimise security breaches in networked systems [SM4]	**M2** suggest how users can be authenticated to gain access to a networked system	**D2** compare the security benefits of different cryptography techniques.
P4 plan procedures to secure a network		
P5 configure a networked device or specialist software to improve the security of a network.	**M3** report on the similarities and differences between securing wireless and wired networked systems.	

PLTS: This summary references where applicable, in the square brackets, the elements of the personal, learning and thinking skills applicable in the pass criteria. 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 emphasis in this unit should be on practical experiences to underpin the theoretical principles. If necessary, individual or small group workshops can be arranged in parallel with other activities to maximise the use of limited resources.

It is likely that discussion and negotiation with the centre's IT services will be necessary to ensure that learners do not have access to key systems. An isolated network connected to the internet is preferred. Simulated systems such as the Cisco Systems Packet Tracer application post version 5.2, as well as virtualisation of operating systems using Virtual Box, QEMU and VM Ware, all provide ideal environments to practise these skills in a secure manner which will not compromise centre security.

Visits and talks by external staff are recommended. Access to relevant current magazines and journals would be valuable to keep the content and examples up to date.

Learners will be familiar with virus attacks and will probably have heard of many of the types of virus currently 'live', but may not be familiar with other ways in which networks can be attacked. Useful research about the threats can be carried out using the internet and trade magazines and newspapers. Threats can be discussed and categorised by type and severity.

There are many methods of protecting systems and the unit content gives examples. New devices and software are being produced constantly and it is suggested that a selection of the examples is chosen to concentrate on, ensuring that each of the sub-headings in the unit content is represented. Technical support staff from a local business may be able to give a talk about the security measures they use. Otherwise case studies can be used.

A visiting speaker would also be of value when considering the organisational aspects of security. Do they have policies in place may be a good opening question. Case studies can help provide alternative views on how to protect systems.

Practising the application of security methods will be limited to what is feasible within the constraints of the centre. Installing software and setting access controls should be possible, remembering this must be applied to a network and not a stand-alone machine. Learners should be made aware of all the methods outlined in the unit content even if they are unable to put them into practice themselves.

Outline learning plan

The outline learning plan has been included in this unit as guidance and can be used in conjunction with the programme of suggested assignments.

The outline learning plan demonstrates one way in planning the delivery and assessment of this unit.

Topic and suggested assignments/activities and/assessment
Introduction to the unit
Types and sources of network attacks: • whole-class exercise – tutor presentation on types of attacks, followed by directed research • whole-class exercise – tutor presentation on sources of attacks, followed by directed research • a mixture of research, discussion and case studies.

Topic and suggested assignments/activities and/assessment
Security-related hardware and software: • whole-class exercise – tutor presentation on email security, followed by directed research • whole-class exercise – tutor presentation on wireless security, followed by practical exercise • whole-class exercise – tutor presentation on security features of networked devices, followed by practical exercise • whole-class exercise – tutor presentation on transmission media issues, followed by directed research • whole-class exercise – tutor presentation on intrusion detection systems, followed by practical exercise • whole-class exercise – tutor presentation on personal access control, followed by practical exercise • whole-class exercise – tutor presentation on security control at device level, followed by practical exercise • whole-class exercise – tutor presentation on encryption, followed by directed research • a mixture of practical exploration of the technologies, learner exercises, case studies and detailed investigation.
Assignment 1 – Are We Safe?
Organisational aspects of network security: • whole-class exercise – tutor presentation on policies and procedures, followed by practical exercise • whole-class exercise – tutor presentation on user responsibilities, followed by discussion • individual exercise – learners research education of IT professionals • whole-class exercise – tutor presentation on physical security of systems, followed by directed research • whole-class exercise – tutor presentation on risk assessment and reduction, followed by individual exercise • a mixture of practical exploration of the technologies, learner exercises, case studies and detailed investigation.
Assignment 2 – What's Best?
System security: • whole-class exercise – tutor presentation on algorithms, followed by individual exercise • whole-class exercise – tutor presentation on transport, followed by individual exercise • whole-class exercise – tutor presentation on application, followed by individual exercise • whole-class exercise – tutor presentation on filtering, followed by individual exercise • whole-class exercise – tutor presentation on testing, followed by individual exercise • a mixture of practical exploration of the technologies, learner exercises, case studies and detailed investigation. Learners will need access to practical resources and suitable technology, they can also use simulators or multimedia tools to gain prior experience before handling live resources.
Assignment 3 – Start Installing!

Assessment

It is suggested that this unit is assessed using the three assignments summarised in the *Programme of suggested assignments* (PSA) table. However, there are a number of options for splitting the assessment and tutors may develop different approaches as appropriate to their learners and centre constraints.

The suggested overall scenario for the assignments is that learners are employed by the IT support department of an organisation and have been asked to review and upgrade the organisation's network security systems.

Suggested Assignment 1 – Are We Safe?

Phase 1: an overview of current network security threats and how to protect against them.

P1, P2 and M1, are straightforward and can be presented in any format, for example rather than a written report, developed as a wiki. In explaining intruder detection systems, learners should include a comparison of the systems to achieve M1.

For D2, a more in-depth analysis of recent threats is expected, where 'recent' in this case means no more than two years ago.

Suggested Assignment 2 – What's Best?

Phase 2: how to minimise risks.

The work for this assignment could be included with that for the first assignment but this would be a bulky piece of largely theoretical work and learners may find it hard to maintain their motivation.

To distinguish it from the first assignment, it is suggested this is evidenced through a presentation. The requirement for P3 is 'explain', which should be more than a simple description of the elements outlined in the unit content.

For M2, a variety of authentication methods should be explained and one or more recommended for use by the organisation.

D2 will require some in-depth research into cryptography techniques and a discussion of the relative benefits.

Suggested Assignment 3 – Start Installing!

Phase 3: configure and test network security hardware/software.

This is the practical element of the assessment and will require access to suitable equipment.

For P4 a written plan or checklist of procedures to be completed could be used as evidence

For P5 observation records and witness statements can be used as evidence that the work was carried out and appropriate testing completed.

For M3, learners could write up a report (any format), which may be supported by work they have completed with both wired and wireless systems.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the pass, 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
P1, P2, M1, D1	Are We Safe?	You work for the IT support department of an organisation. The managers have asked for a review of their network security procedures, starting with an overview of current threats and how to protect against them.	Report Presentation Wiki
P3, M2, D2	What's Best?	Following your report on threats, the organisation would now like a presentation on how best to minimise risks.	Report Presentation
P4, P5, M3	Start Installing!	The organisation has reviewed their needs and asked you to configure their system appropriately.	Security plan Observation record Witness statement Report

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

This unit forms part of the BTEC in IT sector suite. This unit has particular links with the following unit titles in the IT suite:

Level 2	Level 3	Level 4
Unit 11: IT Security	Unit 5: Managing Networks	Unit 56: Network Security
	Unit 7: Organisational Systems Security	Unit 48: IT Security Management

This unit maps to some of the underpinning knowledge from the following areas of competence in the Level 3 National Occupational Standards for IT (ProCom):

- 6.2 IT Security Management.

Essential resources

Learners will need access to practical resources and suitable technology. They can also use simulators or multimedia tools to gain experience before handling live resources. This unit *must* be delivered in a managed environment with no connection to a live system.

Employer engagement and vocational contexts

Learners will gain most by researching a real organisation either by visiting or using visiting speakers.

The Information Commissioner's Office produces excellent teaching and learning materials which highlight the need for control over data. These can provide a useful introduction to the need for privacy, a subjects rights, and an organisations obligations under the Data Protection Act 1998.

Indicative reading for learners

Textbooks

McClure S, Scambray J and Kurtz G – *Hacking Exposed: Network Security Secrets and Solutions, 6th Edition* (McGraw-Hill Osborne, 2009) ISBN-10: 0071613749, ISBN-13: 978-0071613743

Harris S, Harper A, Eagle C and Ness J – *Gray Hat Hacking, 2nd Edition* (McGraw-Hill Osborne, 2008) ISBN-10: 0071495681, ISBN-13: 978-0071495684

Website

www.hackingalert.com/hacking-articles/hotmail-hacking-guide.php

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	describing how networked systems can be protected
Self-managers	explaining what an organisation can do to minimise security breaches in networked systems.

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	discussing recent network threats comparing the security benefits of different cryptography techniques.

Functional Skills – Level 2

Skill	When learners are ...
ICT – Using ICT	
Plan solutions to complex tasks by analysing the necessary stages	testing network security following configuration
Select, interact with and use ICT systems safely and securely for a complex task in non-routine and unfamiliar contexts	configuring a networked device or specialist software to improve the security of a network.