National Unit specification: general information

Unit title: Computing: Network Management and Security (SCQF level 6)

Unit code: FX1N 12

Superclass: CB

Publication date: October 2011

Source: Scottish Qualifications Authority

Version: 01

Summary

The purpose of this Unit is to introduce candidates to some of the fundamental issues and skills relating to securing a networked computer system. Candidates will develop an understanding of the main components and related terminology of a computer security policy and related technical vocabulary.

This Unit has been written as part of the National Certificate in Computing: Technical Support (SCQF level 6) and is also available as a standalone Unit.

Outcomes

1 Describe simple network security procedures.
2 Describe components of a simple computer network system.
3 Implement simple security on a computer network system.
4 Monitor activity and intrusion detection.

Recommended entry

While entry is at the discretion of the centre, candidates would normally be expected to have attained one of the following or equivalent:

- F1K2 11 Computing: Computer Hardware and Systems (SCQF level 5)
- F1FA 11 PC Passport: IT Systems (SCQF level 5)

National Unit specification: general information (cont)

Unit title: Computing: Network Management and Security (SCQF level 6)

Credit points and level

1 National Unit credit at SCQF level 6: (6 SCQF credit points at SCQF level 6*)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the Support Notes of this Unit specification.

There is no automatic certification of Core Skills or Core Skill components in this Unit.

National Unit specification: statement of standards

Unit title: Computing: Network Management and Security (SCQF level 6)

Acceptable performance in this Unit will be the satisfactory achievement of the standards set out in this part of the Unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Outcome 1

Describe simple network security procedures.

Performance Criteria

(a) Describe the assets to be secured.
(b) Describe the threats to network security.
(c) Describe the characteristics of a good security policy.

Outcome 2

Describe components of a simple computer network system.

Performance Criteria

(a) Describe network infrastructure devices.
(b) Describe network services.
(c) Describe end devices.

Outcome 3

Implement simple security on a computer network system.

Performance Criteria

(a) Implement security using a host based IDS.
(b) Implement security using a network based IDS.

Outcome 4

Monitor activity and intrusion detection.

Performance Criteria

(a) Monitor a computer network system.
(b) Detect and mitigate an attack on a host device.
(c) Detect and mitigate a network infrastructure attack.

National Unit specification: statement of standards (cont)

Unit title: Computing: Network Management and Security (SCQF level 6)

Evidence Requirements for this Unit

Evidence is required to demonstrate that candidates have achieved all Outcomes and Performance Criteria.

For Outcomes 1 and 2, written and/or oral recorded evidence is required which demonstrates that candidates can:

- describe the assets to be secured. These must include hardware, software, data and people
- describe a minimum of three threats to a network
- describe the characteristics of a good security policy
- describe a minimum of six network infrastructure devices
- describe a minimum of four network services
- describe a minimum of three end devices

The evidence for Outcomes 1 and 2 should be obtained under controlled, supervised conditions. The assessment will be open-book. Candidates will have access to notes and reference books.

For Outcomes 3 and 4, performance evidence is required which demonstrates that candidates can:

- implement simple security effectively using a host based IDS
- implement simple security effectively using a network based IDS
- monitor a computer network system effectively
- detect and mitigate an attack on a host device effectively
- detect and mitigate a network infrastructure attack effectively

The evidence for Outcomes 3 and 4 will be obtained under controlled, supervised, open-book conditions. Candidates will have access to notes and reference books.

National Unit specification: support notes

Unit title: Computing: Network Management and Security (SCQF level 6)

This part of the Unit specification is offered as guidance. The support notes are not mandatory.

While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this Unit

This Unit is aligned to the following e-Skills UK National Occupational Standards Level 3: IT/Technology Security Management.

Outcome 1

This Outcome relates to identifying key assets that need to be protected. The list of following categories is based on the RFC 2196 Site Security Handbook:

Hardware:	Workstations, servers, networking infrastructure devices (eg routers, switches), computer peripherals.
Software:	Operating systems, applications, services.
Data:	Databases, stored on-line, archived off-line, during execution, in transit over communications media.
People	Users, support staff.

Candidates will be required to identify these assets and describe the potential threats to them. The threats can be categorized as:

- unauthorised access to resources and/or information
- unintended and/or unauthorized disclosure of information
- denial of service

Candidates will be required to identify and describe contemporary sources of these types of threats. Typical sources could include:

- back door attacks
- spoofing attacks
- man in the middle attacks
- replay attacks
- password-guessing attacks
- privilege escalation
- viruses
- logic bombs
- trojan horses
- worms

Candidates should be introduced to real life examples of the effects of some of these threats on commercial organizations, government and individuals. Web sites and organisations sharing security information such as CERT, CIAC, Security Focus, MITRE and Whitehats should be explored and publications such as the Cybersecurity Watch Survey and CIRC bulletins should be examined.

Candidates will be required to identify and describe the characteristics of a good security policy. The general characteristics defined in RFC 2196 could be used as a basis for this. Exposure to real life examples of security policies such as IT policies within the delivering centre would be suitable documentation to review.

Outcome 2

This Outcome relates to the identification and description of a computer network system. Candidates will be required to identify and describe network infrastructure devices such as:

- router
- switch
- wap
- firewall
- remote access service
- vpn
- proxy

Candidates will be required to identify and describe network services such as:

- DNS
- WWW
- FTP
- Email
- NFS

Candidates will be required to identify and describe end devices such as:

- clients
- servers
- peripherals

National Unit specification: support notes (cont)

Unit title: Computing: Network Management and Security (SCQF level 6)

Outcome 3

This Outcome relates to the implementation of simple security features of a host based intrusion detection system (or host based intrusion protection system) and a network based intrusion detection system (or network based intrusion protection system).

Candidates will be exposed to the features of IDS systems that allow components of a security policy to be implemented. These features may include stateful firewalls, behavioural rules and signature analysis. Emphasis will be placed on the requirement for clearly stated security goals which will allow appropriate security tools to be selected and appropriate conditions to be checked and restrictions to be imposed.

Outcome 4

This Outcome relates to the monitoring and detection of a simulated attack on a host and a simulated attack on a network infrastructure. Candidates should be introduced to open source or proprietary IDS systems. A host based attack can be introduced by use of the EICAR (European Institute of Computer Antivirus Research) test. A network infrastructure based attack such as a Denial of Service attack can be simulated through use of tools such as BreakingPoint or Ddosim.

Guidance on learning and teaching approaches for this Unit

A practical hands-on approach to learning should be adopted to engage learners and exemplify key concepts. It is recommended that candidates gain hands-on configuration experience of a host based IDS/IPS and a network based IDS/IPS.

It is important that candidates develop an appropriate technical vocabulary. The main components and related terminology of a computer security policy should be introduced throughout the Unit.

The actual distribution of time between Outcomes is at the discretion of the centre but is expected that Outcome 2 will require more learning time than the others.

The use of simulation and/or virtual machines could be used for teaching and assessment of parts of this Unit.

Guidance on approaches to assessment for this Unit

Outcome 1

This Outcome can be assessed using a set of 10 restricted response questions. The evidence for this Outcome should be obtained under open-book supervised conditions. Where re-assessment is required, a different instrument of assessment should be used.

Outcome 2

This Outcome can be assessed using a set of 10 restricted response questions. The evidence for this outcome should be obtained under open-book supervised conditions. Where re-assessment is required, a different instrument of assessment should be used.

National Unit specification: support notes (cont)

Unit title: Computing: Network Management and Security (SCQF level 6)

Outcomes 3 and 4

These Outcomes can be assessed using practical exercises, evidenced by a checklist or logbook.

Outcomes 4

This Outcome can be assessed using a practical exercise. Candidates will monitor a computer network system and mitigate two simple attacks. This assessment can be evidenced by a checklist or logbook.

Opportunities for the use of e-assessment

E-assessment may be appropriate for some assessments in this Unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all candidate evidence and that conditions of assessment as specified in the Evidence Requirements are met, regardless of the mode of gathering evidence. Further advice is available in *SQA Guidelines on Online Assessment for Further Education (AA1641, March 2003), SQA Guidelines on e-assessment for Schools (BD2625, June 2005)*.

Opportunities for developing Core Skills

In this Unit candidates will:

- identify key assets that need to be protected including hardware, software, data and people identify and describe potential threats to the key assets
- identify and describe the characteristics of a good security policy
- identify and describe network infrastructure devices, services and end devices
- select appropriate security tools to meet specific security goals
- implement simple security features
- monitor activity to detect and mitigate against attack

This means that as candidates are doing this Unit they will be developing aspects of the Core Skills of *Problem Solving*, *Communication* and *Information and Communication Technology*.

Disabled candidates and/or those with additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering whether any reasonable adjustments may be required. Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**

History of changes to Unit

Version	Description of change	Date