Higher National Unit specification: general information

Unit title: Security Concepts

Unit code: H17V 34

Superclass: CB

Publication date: March 2012

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

This Unit is designed to introduce candidates to the issues involved in designing and constructing secure contemporary computer networks and is aimed at candidates undertaking an HN in Computing with Networking or Technical Support that require an understanding of the concepts underpinning network security.

On completion of the Unit the candidate should be able to:

1 Demonstrate network security, compliance and operational security
2 Identify and describe threats and vulnerabilities
3 Implement basic application, data, host security and access control mechanisms
4 Identify suitable methods of cryptography

Recommended prior knowledge and skills

Access to this Unit will be at the discretion of the Centre. There are no specific requirements but candidates would benefit from knowledge of PC hardware and software, as well as the basic concepts of computer networking.

Credit points and level

2 Higher National Unit credits at SCQF level 7: (16 SCQF credit points at SCQF level 7*)

**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.*

General information (cont)

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.

Context for delivery

If this Unit is delivered as part of a Group Award, it is recommended that it should be taught and assessed within the subject area of the Group Award to which it contributes.

Higher National Unit specification: statement of standards

Unit title: Security Concepts

Unit code: H17V 34

The sections of the Unit stating the Outcomes, Knowledge and/or Skills, and Evidence Requirements are mandatory.

Where evidence for Outcomes is assessed on a sample basis, the whole of the content listed in the Knowledge and/or Skills section must be taught and available for assessment. Candidates should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Demonstrate network security, compliance and operational security.

Knowledge and/or Skills

- Identify the function of security and the principles of secure network administration
- Differentiate between the elements of network design
- Identify and differentiate between network ports, protocols and wireless technologies
- Demonstrate the usage of network devices and associated technologies
- Identify risk concepts and mitigation strategies
- Identify incident response, disaster recovery and business continuity procedures
- Explain the impact of environmental controls

Evidence Requirements

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- show successful completion of a single multiple-choice final assessment of which 16 questions must relate to this Outcome and cover all the Knowledge and/or Skills listed above.
- demonstrate practical ability by implementing a secure wireless network within a secure network topology using a secure addressing scheme.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

Outcome 2

Identify and describe threats and vulnerabilities.

Knowledge and/or Skills

- Identify and differentiate between different types of Malware and Viruses
- Describe different types of network, social engineering and application attacks
- Identify mitigation and deterrent techniques
- Differentiate between penetration testing and vulnerability scanning
- Demonstrate usage of assessment tools and techniques for security threat avoidance

Evidence Requirements

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- show successful completion of a single multiple-choice final assessment of which 11 questions must relate to this Outcome and cover all of the Knowledge and/or Skills listed above.
- demonstrate practical ability by the use of assessment tools and techniques for security threat avoidance.

Outcome 3

Implement basic application, data, host security and access control mechanisms.

Knowledge and/or Skills

- Identify the importance of application and data security
- Describe the importance of authentication services
- Identify the concepts of authentication, authorization and access control
- Describe security control in relation to account management
- Implement appropriate procedures to establish host security

Evidence Requirements

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- show successful completion of a single multiple-choice final assessment of which 15 questions must relate to this Outcome with an even distribution across the above Knowledge and/or Skills list.
- demonstrate practical ability by manipulating operating system security and settings and the installation and configuration of anti-malware/virus software.

Higher National Unit specification: statement of standards (cont)

Unit title: Security Concepts

Outcome 4

Identify suitable methods of cryptography.

Knowledge and/or Skills

- Describe general cryptography concepts
- Identify appropriate cryptographic tools and concepts
- Describe the concepts of public key infrastructure and certificate management

Evidence Requirements

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- show successful completion of a single multiple-choice final assessment of which eight questions must relate to this Outcome and cover all of the Knowledge and/or Skills listed above.
- there are no practical elements to this Outcome.

Higher National Unit specification: support notes

Unit title: Security Concepts

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 80 hours.

Guidance on the content and context for this Unit

The content of this Unit is aimed at providing the candidate with a broad knowledge base in the concepts of computer and network security along with conceptual understanding of how many elements of modern security concepts operate.

The Unit design has aimed to incorporate practical deliverables. To allow candidates to perform these practical elements, centres will require suitable resources.

Although the Unit is expressed in generic terms, it should be related to a context that will be familiar to candidates, eg how secure wireless networks and topologies, along with addressing schemes and associated tools can be implemented.

The practical elements may be done as individual tasks or carried out as part of a larger case study/project requirement.

This Unit may assist candidates in preparing for CompTIA examination SY0-301: Security+. Vendor certifications can change rapidly and candidates should be encouraged the check the current details at www.comptia.org to ensure that all objectives have been covered.

Guidance on the delivery of this Unit

During the delivery of this Unit it is important that every opportunity is taken to introduce real-world examples, opportunities for whole-class and group discussion and practical demonstrations wherever possible. Concepts and terminology should be presented in context throughout the Unit. Video presentations should be used where appropriate for providing an alternative explanation of a difficult topic, or as a focus for class discussion or group work. Wherever possible theoretical learning should be re-enforced using practical labs/demonstrations, for example to demonstrate the use of particular tools, the lecturer could capture relevant packets using a suitable packet sniffer tool.

Although not formally taught in this Unit, candidates should be aware of the Health and Safety risks to themselves and others that can arise when working with electrical equipment. Safe working practices should be explained and demonstrated.

Given the theoretical nature of this Unit, it is intended that a significant amount of time will be made available as a central part of the course for revision, tutorials and formative assessment exercises. Candidates should be strongly encouraged to undertake further reading, opportunities for individual or group research should be provided.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

When any practical work is carried out it is advisable, time permitting, that a fault finding element be added into the teaching, thus enabling deeper learning. While there are recognisable fault finding methodologies, the reality still exists that problem solving mainly stems from the thought processes that occur while investigations into the problem are beginning. These thought processes will normally be based upon previous experience and learning already gained. Due to the wide range of skill sets which may be available in a group of candidates, it could be seen as good practice to identify and use these situations to enhance the learning of the complete group of candidates, this will also enable substantial levels of peer learning.

The Unit broadly covers a lot of security concepts and fundamentals. It would be advisable to teach and assess this Unit alongside operating system; networking and server related Units as this would aid candidates in appreciating an understanding from differing perspectives.

The most important overall emphasis should be on the relevance and currency of content in such a rapidly-evolving field.

Guidance on the assessment of this Unit

Assessment will consist of a single multiple-choice assessment alongside a practical assessment.

The single multiple-choice assessment will be conducted in unseen closed-book supervised timed conditions. The assessment may be carried out using e-assessment or paper based. To pass candidates should answer 60% of the questions correctly.

If a candidate requires to be reassessed, a different selection of questions must be used. At least half the questions in the reassessment must be different from those used in the original test.

The suggested time allocation for a multiple-choice assessment is two minutes for each question plus five minutes starting-up time and five minutes finishing-off time, thus a total of 110 minutes should be allocated for a 50-question end-of-Unit test.

In the event that e-assessment is deployed, centres may also utilise other types of questioning, eg:

- Drag and Drop
- Mix and Match

The level of this Unit would prohibit the use of True/False type questions.

The practical elements may be done as individual tasks or carried out as part of a larger case study/project requirement the latter being advisable as it may lead to an enriched learner experience. These tasks will be open-book with time allocated, being at the discretion of the centre.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

Some of the practical tasks have a problem solving element. This will allow assessment of fuller understanding of network operation. The steps taken, by the candidate, to resolve, also requires to be recorded as evidence.

Assessment Guidelines

For each Outcome, candidates should be aware of the following:

Outcome 1

Describe network security, compliance and operational security.

Explain the function of security and the purpose of network devices and technologies:
- Firewalls, routers, switches, proxies, gateways, 802.11, VPN technology, protocol analysers/sniffers, filtering and packet inspection.

Identify the principles of secure network administration:
- Firewall rules, VLANs, router configurations, Access control lists, port security, network segmentation, log analysis.

Differentiate the elements of network design:
- DMZ, subnetting, VLANs, NAT, telephony, Virtualization/cloud computing.

Identify and differentiate between network ports, protocols and wireless technologies:
- IPSec, SSL, SSH, HTTPS, SFTP, SCP, SNMP, WPA, WPA2, WEP, MAC filtering, SSID broadcasts, TKIP, Channelling.

Identify risk concepts and mitigation strategies:
- Controlling, reduction: privacy/acceptable use/security/mandatory policies, risk calculation, change/incident management, user permission reviews, auditing.

Identify incident response, disaster recovery and business continuity procedures:
- Basic forensic procedures, damage/loss control, chain of custody, incident response, impact analysis, continuity planning, disaster recovery.

Explain the impact of environmental controls:
- Fire suppression, shielding, temperature control, CCTV monitoring.

Higher National Unit specification: support notes (cont)

Unit title: Security Concepts

Outcome 2

Identify and describe threats and vulnerabilities.

Identify and differentiate between different types of Malware and Viruses:
- Adware, Viruses, Worms, Spyware, Trojans, Rootkits, Backdoors, Botnets.

Describe and differentiate between different types of network, social engineering and application attacks:
- Man-in-the-Middle, DDoS, Smurf, spoofing, spamming, phishing, DNS poisoning, shoulder surfing, tailgating, hoaxes, impersonation, packet sniffing, war chalking, war driving, cross site scripting, SQL injections, LDAP injections, buffer overflows, cookies, session hijacks.

Identify mitigation and deterrent techniques:
- Electronic bypassing, system/security/access logs, physical security, hardening, intrusion detection, risk/threat/vulnerability assessing, baseline reporting.

Differentiate between penetration testing and vulnerability scanning
- Threat verification, exploiting vulnerabilities, passive testing, white/black/gray box testing

Implement assessment tools and techniques for security threat avoidance:
- Protocol analysers, sniffers, port scanners, honeypots

Outcome 3

Implement basic application, data, host security and access control mechanisms.

Identify the importance of application and data security:
- Hardening, patch management, secure coding, data loss prevention, encryption

Describe the importance of authentication services
- RADIUS, TACACS, LDAP, Kerberos

Identify the concepts of authentication, authorization and access control:
- Identification/authentication, Biometrics, Tokens, Smartcards, SSO, ACLs, Mandatory/discretionary access control

Describe security control in relation to account management:
- Password complexity, recovery, length, lockout, privileges.

Implement appropriate procedures to establish host security:
- Operating system security settings, anti-malware/virus, patch management, baselining, mobile devices, physical hardware security

Outcome 4

Identify suitable methods of cryptography.

Describe general cryptography concepts:

- Symmetric/asymmetric, transport encryption, hashing, steganography, Digital signatures,

Identify appropriate cryptographic tools and concepts:

- Wireless technology, MD5, SHA, AES, DES, 3DES, RSA, PAP/CHAP, Blowfish, transport encryption

Describe the concepts of public key infrastructure and certificate management:

- PKI, Public key, private keys, recovery agents, Certificate authorities

Online and Distance Learning

If this Unit is delivered by open or distance learning methods, additional planning and resources may be required for candidate support, assessment and quality assurance. A combination of new and traditional authentication tools may have to be devised for assessment and re-assessment purposes.

Opportunities for the use of e-assessment

E-assessment may be appropriate for some assessments in this Unit and is detailed within the section 'Guidance of Assessment for 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).*

Opportunities for developing Core Skills

This Unit would not normally develop Core Skills. This would be dependent on specific teaching and or assessment methods and as methods used on this Unit are not prescriptive this Unit could not guarantee inclusion of Core Skills.

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

General information for candidates

Unit title: Security Concepts

This is a two credit Unit at SCQF level 7 and is aimed at providing you with fundamental skills in the concepts of network security and associated tools and is aimed at candidates undertaking and HNC or HND in Computing with Networking or Technical Support that require an understanding of the concepts underpinning network security.

On completion of this Unit you should be able to:

- describe network security, compliance and operational security.
- identify and describe threats and vulnerabilities.
- identify basic application, data, host security and access control mechanisms.
- identify suitable methods of cryptography.

Outcome 1 focuses on the fundamentals of network security and design, devices, ports, protocols, risk management concepts disaster recovery and environmental controls.

Outcome 2 focuses on threats and vulnerabilities such as malware, spyware, social engineering techniques, penetration testing and the tools that can be used for security threat avoidance and ethical hacking techniques.

Outcome 3 focuses on application, data, host and access control mechanisms along with authentication services, operating system security controls account and password management.

Outcome 4 focuses on cryptographic methodologies such as cryptographic tools public key/private key infrastructure, digital signatures, certificate management and data encryption tools and techniques.

There will be one closed-book restricted-response assessment covering all Outcomes. You will be presented with a total of 50 questions and expected to answer 60% of these correctly. You will also be expected to keep a log book, or equivalent, recording the practical tasks you have carried out during the Unit. You must satisfy the requirements for these assessments in order to achieve the Unit.

This Unit may assist candidates in preparing for CompTIA examination SY0-301: Security+. Vendor certifications can change rapidly and candidates should be encouraged the check the current details at www.comptia.org to ensure that all objectives have been covered.