National Unit specification

General information

Unit title: Ethical Hacking (SCQF level 4)

Unit code: H9HY 44

Superclass: CC

Publication date: July 2015

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this Unit is to provide **beginners** with the **basic** knowledge and understanding of the skills and techniques used by ethical and malicious hackers.

The Unit provides an overview of the current legislation enacted to combat computer crime and an opportunity of applying basic hacking methods (in a controlled environment).

A specific aim of this Unit is to raise learners' awareness of potential cyber threats. Additionally, learners will have an appreciation of the ethics and laws relating to computer crime.

On completion of this Unit, learners will gain **basic** knowledge of the current legislation in place relating to computer crime, and be able to distinguish between basic methods used by ethical and malicious hackers to compromise computer systems, as well as applying these skills in a controlled environment. Learners may progress to *Ethical Hacking* at SCQF level 5 or similar National Units.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF level 4.

Outcomes

On successful completion of the Unit the learner will be able to:

1 Identify current legislation relating to computer crime.
2 Describe the basic methods that ethical and malicious hackers use to compromise computer systems.
3 Apply basic hacking methods to compromise computer systems in a controlled environment.

National Unit specification: General information (cont)

Unit title: Ethical Hacking (SCQF level 4)

Credit points and level

1 National Unit credit at SCQF level 4: (6 SCQF credit points at SCQF level 4)

Recommended entry to the Unit

Whilst entry is at the discretion of the centre, it would be beneficial if learners have gained basic IT Skills. This may be evidenced by possession of:

H3LJ 09 *Computer Basics* (SCQF level 3)

or equivalent qualifications or experience.

It is recommended that learners sign an acceptable use policy before using ethical hacking tools.

Core Skills

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

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

Context for delivery

This Unit may be offered stand-alone or as part of the National Progression Award Ethical Hacking at SCQF level 4. If offered as part of this Group Award, there may be opportunities to combine and integrate teaching and learning across Units. There may also be opportunities to combine Evidence Requirements and integrate assessments.

The Assessment Support Pack (ASP) for this Unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

Equality and inclusion

This Unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

National Unit specification: Statement of standards

Unit title: Ethical Hacking (SCQF level 4)

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

Identify current legislation relating to computer crime.

Performance Criteria

(a) Basic computing terminology is used appropriately.
(b) Basic legal terminology is understood correctly.
(c) Current legislation relating to computer crime is identified.
(d) Real life examples of breaches of legislation relating to cybercrime are identified.

Outcome 2

Describe the basic methods that ethical and malicious hackers use to compromise computer systems.

Performance Criteria

(a) Describe current methods used to compromise computer systems.
(b) Describe the potential dangers of cyber-attacks to personal devices.
(c) Describe safety measures that can be taken to protect personal devices.
(d) Use basic hacking terminology correctly.

Outcome 3

Apply basic hacking methods to compromise computer systems in a controlled environment.

Performance Criteria

(a) Select basic features of software that could be used for hacking with guidance.
(b) Apply basic features of software that could be used for hacking with guidance.
(c) Use current methods to defend a computer system in a controlled environment.
(d) Use current methods to attack a computer system in a controlled environment.
(e) Practical activities are carried out in familiar contexts with guidance.

National Unit specification: Statement of standards (cont)

Unit title: Ethical Hacking (SCQF level 4)

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge and experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. Sampling may be used in certain circumstances (see below) where the sample is sufficiently random and robust to clearly infer competence in the complete domain.

The evidence for this Unit may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). Particular consideration should be given to digital formats and the use of multimedia.

Given the level of this Unit, the amount of evidence, and corresponding time spent on assessment, should be minimised but sufficient to satisfy the Performance Criteria. Whenever possible, evidence should be a naturally occurring by-product of teaching and learning. However, it must be produced by the learner. Authentication must be used where this is uncertain.

Evidence is required for two types of competence: **cognitive competence** (knowledge and understanding) and **practical competence** (practical abilities).

The evidence of cognitive competence must include Outcome 1 (all Performance Criteria) and Outcome 2 (all Performance Criteria).

Evidence of cognitive competence may be sampled across the knowledge domain defined by this Unit Specification, so long as the sample is unknown, and unpredictable, to the learner. Where sampling is used to assess the learner's knowledge and understanding, an appropriate pass mark should be set.

The practical evidence will demonstrate Outcome 3 (all Performance Criteria) and can take any appropriate form. At least **one** basic method to defend a computer system and **one** basic method to attack must be used in a controlled environment.

Evidence of practical competence may be produced over an extended period of time; but where it is generated without supervision, some means of authentication must be carried out. The Guide to Assessment provides advice on methods of authentication.

The Guidelines on Approaches to Assessment (see the Support Notes section of this specification) provides specific examples of instruments of assessment.

National Unit Support Notes

Unit title: Ethical Hacking (SCQF level 4)

Unit Support Notes are offered as guidance and 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 will provide learners with the basic knowledge and understanding of the skills and techniques used by both ethical and malicious hackers. This Unit is intended for beginners and should be delivered in that context. At this level (SCQF level 4), treatment of every topic should be non-complex and foundational. It is anticipated that this Unit will prepare learners for the *Ethical Hacking* Unit at SCQF level 5.

This Unit is split into two main sections; the theory and legislation around ethical hacking in Outcomes 1 and 2 and the practical skills element in Outcomes 3.

With the increased advancements and developments in technology, cybercrime is becoming more prevalent. This Unit will raise awareness of the potential cyber threats individuals are at risk from while also gaining an appreciation of the ethics and laws relating to computer crime, which is covered in Outcome 1. It is imperative that learners have an awareness of a range of current Scottish and UK legislation relating to cybercrime and are fully aware of the consequences if they use any skills learnt from this Unit without approved supervision. Tutors may wish to get learners to consider recent high-profile cases where digital evidence has been crucial in making a conviction and consider the steps which will have been undertaken to gather the evidence for that conviction.

At the time of writing, current Scottish and UK legislation relating to cybercrime are:

- Data Protection Act (1998)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act
- Police and Justice Act (2006)

Increased exposure of malicious hackers and attacks in the media means there is a greater general public awareness of the presence of cybercrime. It is important that learners are exposed to methods used by malicious hackers to compromise computer systems, which is covered in Outcomes 2 and 3. This will help ensure a holistic understanding of basic methods ethical hackers used to defend computer systems from such attacks. This Unit will include practical elements to provide learners with an opportunity to apply basic hacking methods they have gained throughout this Unit. It is expected that on completion of this Unit learners will be able to identify and apply basic hacking methods in a controlled environment.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 4)

The focus of this Unit is **ethical** hacking and **all learning and teaching must be delivered in that context**. It is vital that learners appreciate the distinction between ethical and malicious hacking. Learner activities must also be carried out in that context. Ethics must be emphasised throughout this Unit **in every Outcome**. Learners must be made aware of the consequences of malicious hacking, and recognise their responsibilities when they carry out practical activities.

Given the ubiquity of computer networks, their basic operational principles should be known and understood, and the potential attacks and defences in a networked environment should be discussed.

Guidance on approaches to delivery of this Unit

A practical hands-on approach to learning should be adopted to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before learners commence these activities.

The actual distribution of time between Outcomes is at the discretion of the centre. However, one possible approach is to distribute the available time as follows, with emphasis on the practical tasks:

- Outcome 1: 10 hours
- Outcome 2: 12 hours
- Outcome 3: 18 hours

Guidance on approaches to assessment of this Unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

These Outcomes can be assessed in a variety of ways. A traditional approach would involve the testing of knowledge through a selected response instrument (such as a multiple-choice test). The test will sample the knowledge in Outcomes 1 and 2. The sample must be sufficiently random and robust to clearly infer competence in the whole knowledge domain. Every Performance Criterion must be covered in the test; the relative weighting of each one is left to the discretion of the assessor. An appropriate pass mark must be set. The pass mark will be influenced by the instrument of assessment. All of the associated Performance Criteria must be satisfied. It is recommended that if this approach is adopted then all of the knowledge and understanding in this Unit is combined into a single test that samples from the knowledge domain, with an appropriate pass mark. For example, multiple-choice test, comprising 25 questions, each with four options (A–D), could have a pass mark of 15.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 4)

The remaining practical competencies could be assessed through observation of candidate activity throughout the duration of the Unit (and recorded on an observation checklist). The observation checklist, in addition to specifying the prescribed Performance Criteria, should also include brief details of the candidate's practical task carried out (Outcome 3).

Another approach to assessment would be the creation and maintenance of a web log, which would record candidate activity throughout the Unit. This would log, on a daily or weekly basis, what candidates learn and what they do. The log would record all of the learning and practical activities carried out by the candidate. However, their posts would have to satisfy the relevant Performance Criteria. So, for example, the post(s) that relates to Outcome 1, Performance Criterion (d), would have to provide the identifications of examples with breach current Scottish and UK legislation that relate to cybercrime (or provide a link to such identifications with some narrative). Practical activities could also be recorded via the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post). Sampling is not appropriate when this approach is used. While all of the Performance Criteria must be satisfied, the evidence may be distributed across the entire journal. It is not necessary for a specific Performance Criterion to be satisfied entirely within a specific journal entry.

Given that the journal will be completed over an extended period of time, perhaps in a number of locations, the completed log must be authenticated. Professional judgement should be exercised when a Performance Criterion is evidenced across several entries. Not every practical task would require authentication; at this level it is acceptable for some posts to be a simple description of appropriate practical activities. When necessary, separate authentication (such as oral questioning) could be used for verification purposes. Authentication may take various forms including, but not limited to, oral questioning and plagiarism checks. A statement of authenticity should be provided by the candidate to verify the work as their own, and also state any necessary sources and permissions (if any).

The critical aspect is that the blog is an overall accurate reflection of the practical activities (and, therefore, the associated skills) carried out by the learner during the life of the Unit.

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the statements, identifications, descriptions and selections necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, etc that collectively evidence candidates' competencies. Some form of authentication would be required. This could be as simple as a statement of originality, signed by the candidate and the assessor.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 4)

Opportunities for 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 learner evidence and that conditions of assessment as specified in the Evidence Requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

This Unit provides opportunities to deliver some of the following Core Skills:

Information and Communication Technology (ICT) (SCQF level 4)
Communication (SCQF level 4)
Problem Solving (SCQF level 4)
Working with Others (SCQF level 4)

Several of the Core Skill components in *Information and Communication Technology (ICT)* can be addressed in this Unit. There are opportunities to select and start application software, use tools, enter and edit data, locate information, use search techniques, select information, and recognise security risks and act accordingly.

Some of the Core Skill components in *Communication* can be addressed in this Unit. There are opportunities to pick out important ideas and key points, choose a format, include information or ideas, present information and use spelling, grammar and punctuation to make your writing clear. Additionally, there are opportunities to express ideas or opinions clearly and in a logical way whilst listening to other and respond accordingly.

Some of the Core Skill components in *Problem Solving* can be addressed in this Unit. There are ample opportunities to recognise the main factors affecting a simple situation, decide on an appropriate course of action to solve the problem, work out an action plan to deal with the problem, choose what you need to carry out the action plan, carry out the action plan, checking it is complete and decide how effective your action plan was.

One or more of the Core Skill components in *Working with Others* can be addressed in this Unit. There are opportunities to carry out a role in a co-operative activity, and seek and offer support.

In addition to Core Skills, this Unit provides opportunities to develop digital citizenship skills.

History of changes to Unit

Version	Description of change	Date

General information for learners

Unit title: Ethical Hacking (SCQF level 4)

This section will help you decide whether this is the Unit for you by explaining what the Unit is about, what you should know or be able to do before you start, what you will need to do during the Unit and opportunities for further learning and employment.

This Unit aims to provide you with the fundamental knowledge and skills of ethical hacking. It will also help you gain respect for current legislation surrounding computer crime.

This Unit is an introduction of the knowledge and skills used by ethical and malicious hackers. There will be an emphasis in this Unit to gain as much practical skills throughout this course. Providing the opportunities to put into practice the theory you learn. This will give you a greater understanding into the approaches used to attack and protect computer systems from computer crime. You will also explore current legislation in order to provide you with an understanding of the risks and consequences relating to all methods you will learn in this course.

The Unit is designed for **beginners.** It covers a wide range of knowledge and skills including:

- The difference between ethical and malicious hackers.
- Identify current breaches of legislation.
- Describe the dangers of cyber-attacks to personal devices.
- Describe ways to protect personal devices from cyber-attacks.
- Use current methods to attack and defend a computer system from cyber-attacks in a controlled environment.
- Use methods learnt responsibly.

No previous knowledge or experience of computers is presumed. It is designed for the beginner who wants to gain a basic understanding of the current methods used to attack and defend a computer system from malicious hackers.

The assessment may take different forms. It will be straight-forward and not take much time away from your learning. It may involve a short test of your knowledge and some practical tasks, or it may simply be a record of your activities during the Unit. The focus of the Unit is on learning — not assessing.

This Unit is part of a series of Units on ethical hacking. You may progress to the next Unit in the series (the *Ethical Hacking* Unit at SCQF level 5) on completion of this Unit if you wish to improve your knowledge and skills in this area.